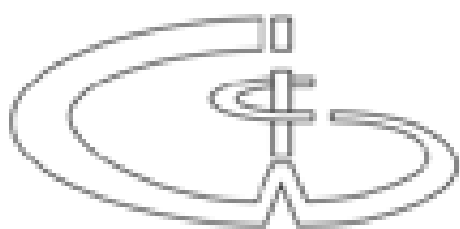




Pre-Proceedings of the
2022 Symposium on Information Theory and Signal
Processing in the Benelux

Université catholique de Louvain
Louvain-la-Neuve, Belgium
June 1–2, 2022



Previous symposia

1. 1980 Zoetermeer, The Netherlands, Delft University of Technology
2. 1981 Zoetermeer, The Netherlands, Delft University of Technology
3. 1982 Zoetermeer, The Netherlands, Delft University of Technology
4. 1983 Haasrode, Belgium ISBN 90-334-0690-X
5. 1984 Aalten, The Netherlands ISBN 90-71048-01-2
6. 1985 Mierlo, The Netherlands ISBN 90-71048-02-0
7. 1986 Noordwijkerhout, The Netherlands ISBN 90-6275-272-1
8. 1987 Deventer, The Netherlands ISBN 90-71048-03-9
9. 1988 Mierlo, The Netherlands ISBN 90-71048-04-7
10. 1989 Houthalen, Belgium ISBN 90-71048-05-5
11. 1990 Noordwijkerhout, The Netherlands ISBN 90-71048-06-3
12. 1991 Veldhoven, The Netherlands ISBN 90-71048-07-1
13. 1992 Enschede, The Netherlands ISBN 90-71048-08-X
14. 1993 Veldhoven, The Netherlands ISBN 90-71048-09-8
15. 1994 Louvain-la-Neuve, Belgium ISBN 90-71048-10-1
16. 1995 Nieuwekerk a/d IJssel, The Netherlands ISBN 90-71048-11-X
17. 1996 Enschede, The Netherlands ISBN 90-365-0812-6
18. 1997 Veldhoven, The Netherlands ISBN 90-71048-12-8
19. 1998 Veldhoven, The Netherlands ISBN 90-71048-13-6
20. 1999 Haasrode, Belgium ISBN 90-71048-14-4
21. 2000 Wassenaar, The Netherlands ISBN 90-71048-15-2
22. 2001 Enschede, The Netherlands ISBN 90-365-1598-X
23. 2002 Louvain-la-Neuve, Belgium ISBN 90-71048-16-0
24. 2003 Veldhoven, The Netherlands ISBN 90-71048-18-7
25. 2004 Kerkrade, The Netherlands ISBN 90-71048-20-9
26. 2005 Brussels, Belgium ISBN 90-71048-21-7
27. 2006 Noordwijk, The Netherlands ISBN 90-71048-22-7
28. 2007 Enschede, The Netherlands ISBN 978-90-365-2509-1
29. 2008 Leuven, Belgium ISBN 978-90-9023135-8
30. 2009 Eindhoven, The Netherlands ISBN 978-90-386-1852-4
31. 2010 Rotterdam, The Netherlands ISBN 978-90-710-4823-4
32. 2011 Brussels, Belgium ISBN 978-90-817-2190-5
33. 2012 Enschede, The Netherlands ISBN 978-90-365-3383-6
34. 2013 Leuven, Belgium ISBN 978-90-365-0000-5
35. 2014 Eindhoven, The Netherlands ISBN 978-90-386-3646-7
36. 2015 Brussels, Belgium ISBN 978-2-8052-0277-3
37. 2016 Louvain-la-Neuve, Belgium ISBN 978-2-9601884-0-0
38. 2017 Delft, The Netherlands ISBN 978-94-6186-811-4
39. 2018 Enschede, The Netherlands ISBN 978-90-365-4570-9
40. 2019 Ghent, Belgium ISBN 978-94-918-5703-4
41. 2021 Eindhoven (online), The Netherlands ISBN

The 42nd Symposium on Information Theory in the Benelux has been organized by

Université catholique de Louvain and Université Libre de Bruxelles

<https://sites.uclouvain.be/sitb2022>

on behalf of the

Werkgemeenschap voor Informatie- en Communicatietheorie (WIC),
and the IEEE Benelux Signal Processing Chapter.

Financial support from the IEEE Benelux Signal Processing Chapter, the IEEE Benelux Information Theory Chapter and the Werkgemeenschap voor Informatie- en Communicatietheorie (WIC) is gratefully acknowledged.

Organizing committee:
Jérôme Louveaux (UCL)
François Quitin (ULB)

Proceedings

Proceedings of the 42nd Symposium on Information Theory and Signal Processing in the Benelux. Edited by Jérôme Louveaux and François Quitin.
ISBN: Pending.

Table of contents

<i>Probabilistic Constellation Shaping Algorithms: Performance vs. Complexity Trade-offs</i> Yunus C. Gültekin, Alex Alvarado	1
<i>RF fingerprinting for wireless localization networks using Bayesian techniques</i> Amélia Struyf, Cédric Hannotier, François Quitin	3
<i>Linear Precoder Design in Massive MIMO under Realistic Power Amplifier Consumption Constraint</i> Emanuele Peschiera, François Rottenberg	10
<i>Observability analysis of Direction-of-Arrival estimation using dual-antenna receivers</i> Youssef Agram, Jianqiao Cheng, François Quitin	15
<i>Unsupervised neural decoding of auditory attention using a Binary Quadratic Program</i> Nicolas Heintz, Tom Francart, Alexander Bertrand	20
<i>Unraveling Finger Veins: An Improvement to Unsupervised Finger Vein Recognition with a Convolutional Autoencoder</i> Tugce Arican, Raymond Veldhuis, Luuk Spreeuwers	21
<i>Biometric testing: aligning standards and practice</i> Florens de Wit, Chris Zeinstra, Luuk Spreeuwers	26
<i>A Diffraction Aware Alternative to Image Method in Ray Tracing</i> Jérôme Eertmans, Claude Oestges, Laurent Jacques	33
<i>Hardware-Friendly Iterative Projection Aggregation Decoder for Reed-Muller Codes</i> Marzieh Hashemipour-Nazari, Kees Goossens, Alexios Balatsoukas-Stimming	35
<i>Strategies for Increasing Longevity of IoT Devices</i> Jona Cappelle, Jarne Van Mulders, Sarah Goossens, Guus Leenders, Liesbet Van der Perre	36
<i>Distributed Gaussian Process for Multi-agent Systems</i> Peiyuan Zhai, Raj Thilak Rajan	37
<i>Exploring the GANformer for Face Generation: Investigating the segmentation and smile augmentation potential</i> Romano Ferla, Chris Zeinstra, Luuk Spreeuwers	38
<i>Grant-Free Random Access in Massive MIMO for Static Low-Power IoT Nodes</i> Gilles Callebaut, Liesbet Van der Perre, François Rottenberg	46
<i>Epileptic Seizure Detection using a Tensor-Network Kalman Filter for LS-SVMs</i> Seline de Rooij, Borbála Hunyadi	52
<i>Decoder-only transformers for passive human activity recognition</i> Shervin Mehryar, Lin Fei Kang, Yue Fei, Shahrokh Valaee	53

<i>Object Detection and Person Tracking in CathLab with Automatically Calibrated Cameras</i>	
Yingfeng Jiang, Renjie Dai, Jincheng Zeng, Rick Butler, Teddy Vijfvinkel, Yanbo Wang, John van den Dobbelsteen, Maarten van der Elst, Justin Dauwels	57
<i>Reliability of wireless intra-aircraft networks: A comparative analysis of IEEE 802.15.4 protocols</i>	
Berna Eraslan, Sonia Heemstra de Groot, Georgios Exarchakos, Ignas Niemegeers	58
<i>Relative Affine Localization for Robust Distributed Formation Control</i>	
Zhonggang Li, Raj Thilak Rajan	64
<i>Tracking Rental Bikes in Smart Cities: a Multi-RAT Approach</i>	
Guus Leenders, Gilles Callebaut, Liesbet Van der Perre, Lieven De Strycker .	66
<i>Embedded AI Enabled Air-Writing for a Post-COVID World</i>	
Koen Goedemondt, Jie Yang, Qing Wang	67
<i>Tensor-based Hemodynamic Response Estimation in Functional Ultrasound Data</i>	
Sofia-Eirini Kotti, Borbála Hunyadi	69
<i>Relative Kinematics Estimation Using Accelerometer Measurements</i>	
Anurodh Mishra, Raj Thilak Rajan	70
<i>On the Integration of Acoustics and LiDAR: a Multi-Modal Approach to Acoustic Reflector Estimation</i>	
Ellen Riemens, Pablo Martínez-Nuevo, Jorge Martinez, Martin Møller, Richard C. Hendriks	72
<i>Extreme Precipitation Nowcasting using Deep Generative Models</i>	
Haoran Bi, Maksym Kyryliuk, Zhiyi Wang, Cristian Meo, Yanbo Wang, Ruben Imhoff, Remko Uijlenhoet, Justin Dauwels	73
<i>Approximate quantum encryption with faster key expansion</i>	
Mehmet Hüseyin Temel, Boris Škorić	74
<i>Multi-Objective Game Theory for Multi-User OFDM Integrated Radar Waveform Design</i>	
Guillaume Thiran, Ivan Stupia, Luc Vandendorpe	81
<i>Unconditional tamper evidence from short keys</i>	
Bart van der Vecht, Xavier Coiteux-Roy, Boris Škorić	82
<i>Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Standardization Process Finalists</i>	
Corentin Verhamme, Gaëtan Cassiers, François-Xavier Standaert	85
<i>Adaptation of Simultaneous Orthogonal Matching Pursuit for Cooperative Spectrum Sensing</i>	
Adelin Roty, Jean-François Determe	87
<i>Adaptive Optimizer Design for Constrained Variational Inference</i>	
Alp Sarı, Semih Akbayrak, Ismail Senöz, Bert de Vries	88

<i>Collusion-resistant fingerprinting of parallel content channels</i>	
Basheer Joudeh, Boris Škorić	94
<i>A Distributed Adaptive Signal Fusion Framework for Spatial Filtering within a Wireless Sensor Network</i>	
Cem Ates Musluoglu, Charles Hovine, Alexander Bertrand	104
<i>Compressed Sensing in Wireless Acoustic Sensor Networks</i>	
Chesney Buyle, Bert Cox, Tuur Baele, Laura Monteyne, Lieven De Strycker .	105
<i>Convergence of Stochastic PDMM</i>	
Sebastian Jordan, Richard Heusdens	111
<i>Spatial Diversity Effects for Multi-node Ultrasonic Indoor Positioning</i>	
Daan Delabie, Liesbet Van der Perre, Lieven De Strycker	112
<i>Aircraft Trajectory Prediction using ADS-B Data</i>	
Xuzhou Yang, Junzi Sun, Raj Thilak Rajan	113
<i>Temporal synchronization of radar and lidar streams</i>	
David Aledo, Tanmay Manjunath, Raj Thilak Rajan, Darek Maksimiuk, Rene van Leuken	123
<i>Distributed Detect-and-Avoid with Non-Stationary Obstacles</i>	
Ellen Riemens, Raj Thilak Rajan	133
<i>Image Search Engine by Deep Neural Networks</i>	
Yuanyuan Yao, Qi Zhang, Yanan Hu, Cristian Meo, Yanbo Wang, Andrea Nanetti, Justin Dauwels	134
<i>Dramco Uno: A Low-Entry IoT Learning Platform for STE(A)M-Oriented Education</i>	
Guus Leenders , Geoffrey Ottoy , Gilles Callebaut	135
<i>Surface Electrocardiogram Reconstruction Using Intra-operative Electrograms</i>	
Hanie Moghaddasi, Borbála Hunyadi, Alle-Jan van der Veen, Natasja M.S. de Groot, Richard C. Hendriks	136
<i>Feasibility of CSMA/NDA protocol for wireless systems using On-Off Keying</i>	
Mehmet Fatih AYTEN, François Quitin	137
Papers not appearing in the proceedings	142
<i>Joint Estimation of Parameters in a Cardiac Tissue Model Using Confirmatory Factor Analysis</i>	
Miao Sun, Natasja M.S. de Groot, Richard C. Hendriks	
<i>Estimation of Atrial Fibre Direction Based on Activation Maps</i>	
Johannes W. de Vries, Richard C. Hendriks and Miao Sun	
<i>Finite Impulse Response Filters for Simplicial Complexes</i>	
Maosheng Yang, Elvin Isufi, Michael T. Schaub, Geert Leus	
<i>Wi-Fi-based passive radars for crowd monitoring</i>	
Martin Willame, Jérôme Louveaux, François Horlin	
<i>Adaptive Map Matching Based on Dynamic Word Embeddings for Indoor Positioning</i>	
Xinyue Lan, Lijia Zhang, Zhuoling Xiao, Bo Yan	

<i>Dynamic Bi-Colored Graph Partitioning</i>	
Yanbin He, Mario Coutino, Elvin Isufi, Geert Leus	
<i>Characterisation and Cancellation of Interference with Multiple Phase-coded FMCW Dual-Function RADAR Communication Systems</i>	
François De Saint Moulin, Claude Oestges, Luc Vandendorpe	
<i>Single-Pulse Estimation of Target Velocity on Planar Arrays</i>	
Costas A. Kokke, Mario Coutiño, Richard Heusdens, Geert Leus, Laura Anitori	
<i>Learning Time-Varying Graphs from Online Data</i>	
Alberto Natali, Elvin Isufi, Mario Coutino, Geert Leus	
<i>Sensor-to-cell height estimation for conductivity estimation in cardiac cells</i>	
Cees H. Kos, Miao Sun, Richard C. Hendriks	
<i>Node Attachment and Filtering on Expanding Graphs</i>	
Bishwadeep Das, Elvin Isufi	

Probabilistic Constellation Shaping Algorithms: Performance vs. Complexity Trade-offs

Yunus Can Gültekin and Alex Alvarado
 Information and Communication Theory Lab
 Eindhoven University of Technology
 Eindhoven, The Netherlands
 {y.c.g.gultekin, a.alvarado}@tue.nl

Abstract—We review the recent advances in the design of probabilistic shaping algorithms. We investigate the implementation complexity of these algorithms in terms of required storage and computational power. We show that (1) the optimum performance can be achieved via different algorithms creating a trade-off between storage and computational complexities, and (2) a significant reduction in complexity can be achieved via the recently-proposed *shift-based band-trellis enumerative sphere shaping* if a slight degradation in performance is tolerated.

Index Terms—Probabilistic Amplitude Shaping, Enumerative Coding, Implementation Complexity.

I. EXTENDED ABSTRACT

Probabilistic amplitude shaping (PAS) [1] combines an amplitude shaper with a forward error correction (FEC) code, and achieves the capacity of the additive white Gaussian noise (AWGN) channel [2], [3]. The function of the amplitude shaping block is to generate the amplitudes of the channel inputs while a systematic FEC encoder determines their signs as shown in Fig. 1. Popular amplitude shaping algorithms which are optimum for the AWGN channel include constant composition distribution matching (CCDM) [4], enumerative sphere shaping (ESS) [5], multiset-partition distribution matching (MPDM) [6], shell mapping (SM) [7], etc. This optimality is in the sense that the resulting channel input distribution approaches the Gaussian distribution for large shaping blocklength N and large constellation cardinality M .

The objective when designing an amplitude shaper is to obtain a certain characteristic (e.g., fixed composition, small average energy, small energy variation, low kurtosis, etc.) for the channel input sequences with (1) low storage complexity, and (2) low computational complexity. For the AWGN channel, this objective is to obtain a (sampled) Gaussian-like channel input distribution, i.e., the Maxwell–Boltzmann (MB) distribution. CCDM, for instance, generates amplitude sequences with a fixed composition which is obtained by quantizing the MB distribution. On the other hand, ESS and SM, both sphere shaping algorithms, generate amplitude sequences such that the resulting signal space has an N -spherical shape, which in turn indirectly induces an MB-like distribution.

The work of Y.C. Gültekin and A. Alvarado has received funding from the ERC under the EU’s H2020 programme via the Starting grant FUN-NOTCH (ID: 757791) and via the Proof of Concept grant SHY-FEC (ID: 963945).

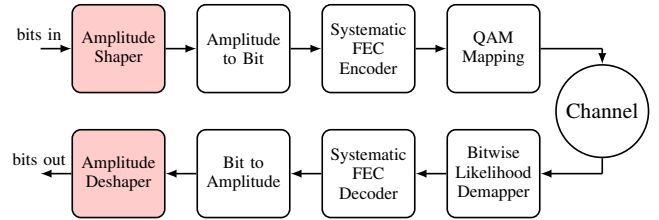


Fig. 1. PAS block diagram. Red blocks are the focus of this paper.

For other types of communication channels, different input distributions or signal space structures may be more advantageous to improve performance. As an example, the nonlinear interference generated during the propagation of the channel input waveform over the nonlinear fiber channels has been shown to depend on the fourth-order standardized moment of the input distribution (i.e., kurtosis) [8], [9], or on the energy variations in the input waveform [10], [11]. Accordingly, we have recently proposed a modified version of ESS, kurtosis-limited ESS (K-ESS), to generate shaped input sequences with low kurtosis [12]. Then in [13], we have proposed another modified version of ESS, band-trellis ESS (B-ESS), to generate sequences with small energy variations. We have demonstrated that K-ESS and B-ESS provide higher signal-to-noise ratios (SNRs) and increased achievable rates concerning uniform signaling and AWGN-optimal shaping.

On the practical side, a bounded-precision (BP) implementation method was proposed for ESS and SM in [14] to decrease their high storage and computational full-precision (FP) complexities, resp. This method can be applied to ESS, K-ESS, B-ESS, and in fact, to any enumerative-coding-based shaping algorithm. In [15], a finite-precision (FiP) implementation was proposed for arithmetic-coding-based DM algorithms. This technique can be applied to CCDM, MPDM, and in fact, to any DM algorithm that has an underlying arithmetic encoder. Then in [16], an on-the-fly (OtF) computation method was proposed for ESS, creating a trade-off between its storage and computational complexities. In [17], a logarithmic-domain implementation was introduced for arithmetic-coding-based CCDM such that high-precision multiplications and divisions required in the algorithm are replaced with low-precision addi-

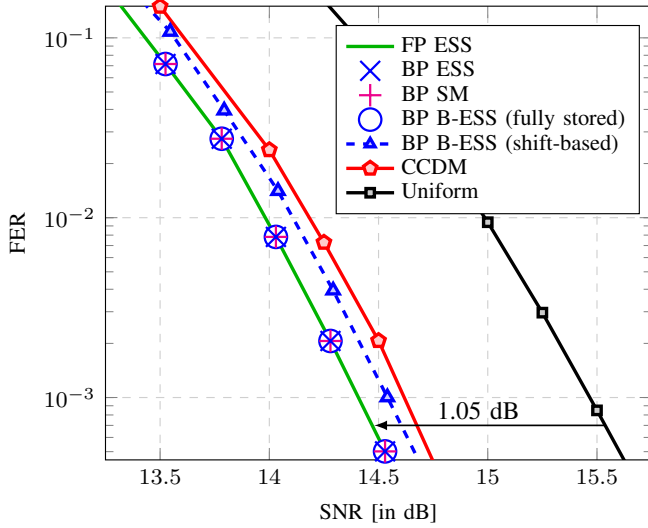


Fig. 2. FER vs. SNR for 64-QAM at the PAS transmission rate of 4 bit/2-D. All shaping schemes use a blocklength of $N = 216$. FEC is based on IEEE 802.11's LDPC codes.

tions and subtractions. Finally, in [18], the implementation of B-ESS was discussed and an OtF computation technique was provided based on binary shifts such that the required storage is independent of the shaping blocklength. The theses [19], [20] provide a good overview of the implementation of DM algorithms, while [21] provides a discussion on the complexity of various shaping algorithms.

In this work, we investigate the performance vs. complexity trade-offs of some of the above-mentioned shaping algorithms. We show in Fig. 2 that the optimum performance can be obtained with different algorithms from different parts of the storage vs. computational complexity spectrum as shown in Fig. 3. We also show that if a slight performance loss is tolerated, our shift-based B-ESS has significantly-reduced complexity concerning other enumerative algorithms.

REFERENCES

- [1] G. Böcherer, F. Steiner, and P. Schulte, "Bandwidth efficient and rate-matched low-density parity-check coded modulation," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 4651–4665, Dec. 2015.
- [2] G. Böcherer, "Probabilistic signal shaping for bit-metric decoding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, June 2014, pp. 431–435.
- [3] Y. C. Gültekin, A. Alvarado, and F. M. J. Willems, "Achievable information rates for probabilistic amplitude shaping: An alternative approach via random sign-coding arguments," *Entropy*, vol. 22, no. 7: 762, July 2020.
- [4] P. Schulte and G. Böcherer, "Constant composition distribution matching," *IEEE Trans. Inf. Theory*, vol. 62, no. 1, pp. 430–434, Jan. 2016.
- [5] Y. C. Gültekin, W. J. van Houtum, A. Koppelaar, and F. M. J. Willems, "Enumerative sphere shaping for wireless communications with short packets," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 1098–1112, Feb. 2020.
- [6] T. Fehenberger, D. S. Millar, T. Koike-Akino, K. Kojima, and K. Parsons, "Multiset-partition distribution matching," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1885–1893, Mar. 2019.
- [7] P. Schulte and F. Steiner, "Divergence-optimal fixed-to-fixed length distribution matching with shell mapping," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 620–623, Apr. 2019.

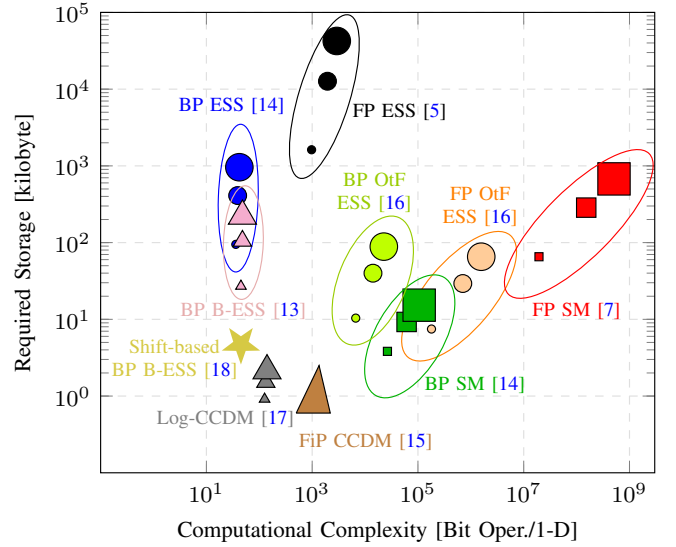


Fig. 3. Maximum computational complexity vs. maximum required storage of amplitude shaping, modified and extended from [21, Fig. 12]. Size of the markers are proportional to the corresponding blocklength $N \in \{216, 432, 648\}$.

- [8] R. Dar, M. Feder, A. Mecozzi, and M. Shtaif, "Properties of nonlinear noise in long, dispersion-uncompensated fiber links," *Opt. Express*, vol. 21, no. 22, pp. 25 685–25 699, Nov. 2013.
- [9] T. Fehenberger, A. Alvarado, G. Böcherer, and N. Hanik, "On probabilistic shaping of quadrature amplitude modulation for the nonlinear fiber channel," *J. Lightw. Technol.*, vol. 34, no. 21, pp. 5063–5073, Nov. 2016.
- [10] O. Geller, R. Dar, M. Feder, and M. Shtaif, "A shaping algorithm for mitigating inter-channel nonlinear phase-noise in nonlinear fiber systems," *J. Lightw. Technol.*, vol. 34, no. 16, pp. 3884–3889, Aug. 2016.
- [11] J. Cho, X. Chen, G. Raybon, D. Che, E. Burrows, S. Olsson, and R. Tkach, "Shaping lightwaves in time and frequency for optical fiber communication," *Nature Commun.* **13**, 785, Feb. 2022.
- [12] Y. C. Gültekin *et al.*, "Kurtosis-limited sphere shaping for nonlinear interference noise reduction in optical channels," *J. Lightw. Technol.*, vol. 40, no. 1, pp. 101–112, Jan. 2022.
- [13] —, "Mitigating nonlinear interference by limiting energy variations in sphere shaping," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, San Diego, CA, USA, Mar. 2022.
- [14] Y. C. Gültekin, F. M. J. Willems, W. J. van Houtum, and S. Şerbetli, "Approximate enumerative sphere shaping," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, June 2018, pp. 676–680.
- [15] M. Pikus, W. Xu, and G. Kramer, "Finite-precision implementation of arithmetic coding based distribution matchers," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019.
- [16] Y. C. Gültekin, W. J. van Houtum, A. G. C. Koppelaar, and F. M. J. Willems, "Low-complexity enumerative coding techniques with applications to amplitude shaping," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 33–37, Jan. 2021.
- [17] Y. C. Gültekin, F. M. J. Willems, and A. Alvarado, "Log-CCDM: distribution matching via multiplication-free arithmetic coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, June-July 2022.
- [18] —, "Band-ESS: Streaming enumerative coding with applications to probabilistic shaping," June 2022, (preprint).
- [19] P. Schulte, "Algorithms for distribution matching," Ph.D. dissertation, Tech. Uni. of Munich, Germany, Apr. 2020.
- [20] M. Pikus, "Finite-precision and multi-stream distribution matching," Ph.D. dissertation, Tech. Uni. of Munich, Germany, Sep. 2019.
- [21] Y. C. Gültekin, T. Fehenberger, A. Alvarado, and F. M. J. Willems, "Probabilistic shaping for finite blocklengths: Distribution matching and sphere shaping," *Entropy*, vol. 19, no. 5: 581, May 2020.

RF fingerprinting for wireless localization networks using Bayesian techniques

Amélia Struyf
Brussels School of Engineering
Université Libre de Bruxelles
Brussels, Belgium
amelia.struyf@ulb.be

Cédric Hannotier
Brussels School of Engineering
Université Libre de Bruxelles
Brussels, Belgium
cedric.hannotier@ulb.be

François Quitin
Brussels School of Engineering
Université Libre de Bruxelles
Brussels, Belgium
francois.quitin@ulb.be

Abstract—One major problem of wireless localization network is to identify the nodes that transmit data packets, especially when the localization system does not decode MAC addresses. In this paper, the performances of multi-target tracking techniques for RF fingerprinting are evaluated. The targets periodically transmit 802.11 Wi-Fi packets to a single receiver. The fingerprinting feature considered is the Carrier Frequency Offset (CFO). The local oscillator (LO) dynamics is included in the system model which allows to take into account the CFO drift. Multi-target tracking is performed by the Joint Probabilistic Data Association Filter (JPDAF) and the Exact Neighbourhood version of the JPDAF (EN-NPDA) associated with a Kalman filter. Different tracking scenarios are simulated to test the performance of the algorithms and highlight their limits. An experiment using Universal software-defined radios is performed to validate the algorithms.

Index Terms—RF fingerprinting, Wi-Fi, CFO drift, JPDAF, Kalman filter

I. INTRODUCTION

Uniquely identifying and tracking radio-frequency (RF) devices is a key feature for wireless localisation networks. MAC or higher layers-based device identification is widely developed but creates problems from a user anonymization perspective and is software-hackable [1], [2]. This motivates the use of RF fingerprinting, which relies on inherent transceivers imperfections caused by chip manufacturing tolerances, to uniquely identify RF devices.

PHY-layer fingerprinting is mostly separated in two categories [1]: white-list fingerprinting, and unsupervised learning strategies, which tend to lock on the data packet containing the MAC ID, leading to limited performances [3]. RF fingerprinting algorithms that use the wireless protocols common packet header rely on a few typical features, such as the carrier frequency offset (CFO). In these algorithms, the CFO is frequently assumed to be a static [4], [5] or random Gaussian-distributed feature [6]. In reality, phase noise and random walk frequency noise affect real local oscillators (LO), causing a random drift of CFO over time [7]. One of the challenges of using CFO for device fingerprinting is to handle the CFO drift and the large noise that is typical of CFO estimates. When multiple devices are emitting packets, the large CFO noise makes it difficult to associate each packet to a given target uniquely. One of the interesting aspects from a user

anonymization perspective of using CFO for fingerprinting lies in the fact that it allows short-term device tracking while preventing long-term identification.

In this paper, we study the performances of bayesian multi-target tracking (MTT) algorithms for RF fingerprinting using the CFO as a feature, as shown in Figure 1. Using MTT algorithms allows to uniquely associate the CFO of a data packet to a given device, while also taking into account the dynamics of the CFO.

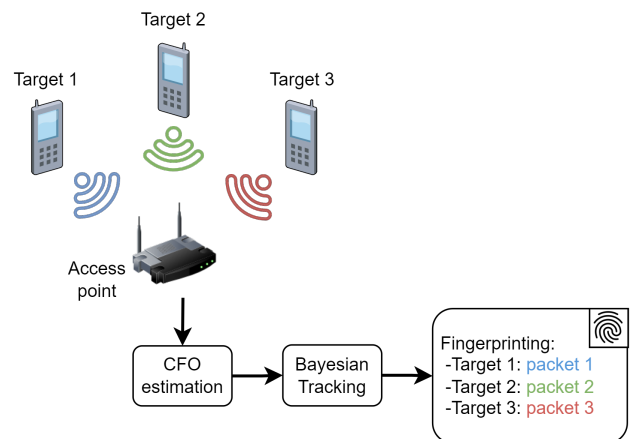


Fig. 1. RF fingerprinting using Bayesian techniques

Contributions : The contributions of this paper are summarised as follows :

- we evaluate the performances of well known MTT algorithms on various simulated tracking scenarios.
- an experiment is performed in order to validate the MTT algorithms on data generated using Universal Software Radio Peripheral (USRP) software-defined radios (SDRs).

The main innovation of our work compared to the existing literature lies in the inclusion of the LO dynamics into the CFO-based fingerprinting framework.

The remainder of this paper is organized as follows. Section II explains the CFO estimation and multi-target tracking algorithms. The simulation results are discussed in Section III.

Section IV presents the experimental results. Finally, section V concludes this paper and presents future work.

II. ALGORITHM

A. System model

We consider a system with 1 to 10 targets transmitting data packets to a single receiver, as shown in Figure 1. Targets can appear and disappear from the tracking scene over time. All targets transmit packets at the same time interval comprised between 100 ms and 10 s. The received packets are "scanned" every 100ms - 10s corresponding to the target packet transmission interval. It is assumed that during each scan at most one packet from each target is received. Without loss of generality, we consider 802.11 Wi-Fi packets, which are composed of the legacy preamble followed by the payload. A very small fraction of sent packets can be undetected and there are no false-alarm data packets.

In the remainder of this section, the different parts of the algorithm used to track the different targets will be presented as follows. In section II-B, the CFO estimation method from the legacy preamble is presented. Section II-C and II-D explain the used tracking algorithms. Lastly, section II-E shows how to deal with targets appearing and disappearing from the tracking scene.

B. CFO estimation

The CFO $\Delta\omega$ is estimated from the L-LTF field of the legacy preamble. The L-LTF is composed of a 64 samples sequence, which has good correlation properties, repeated twice and preceded by a 32 samples cyclic prefix (CP). Using the L-LTF, a fine CFO estimation in the range $[-156,25 \text{ kHz}, 156,25 \text{ kHz}]$ can be performed based on an auto correlation process, which allows to detect repeated patterns in the received signal r [8]. The auto-correlation AC is computed as follows:

$$AC(n) = \sum_{m=0}^{T_{L-LTF}-1} r(n+m+T_{L-LTF})r^*(n+m) \quad (1)$$

where T_{L-LTF} is the L-LTF period equal to 64 samples. Figure 2 shows the profile of the auto-correlation obtained using the above equation. The second plateau that can be observed, indicated as AC_{max} in Figure 2, corresponds to the correlation between two L-LTF sequences.

The CFO can then be determined from this plateau as follows:

$$\Delta\omega = \frac{\angle(\sum_{l=0}^L AC_{max}(l))}{2\pi T_{L-LTF} T_s} \quad (2)$$

where T_s is the sampling period and L is the length of the plateau equal to 32 samples.

C. Joint Probabilistic Data Association Filter and Kalman filtering

1) *Kalman filter system model:* In order to track the CFO of multiple targets simultaneously, the Joint Probabilistic Data Association Filter (JPDAF) and the Exact Neighbour Neighbour version of the JPDAF (EN-NPDA) are used, both

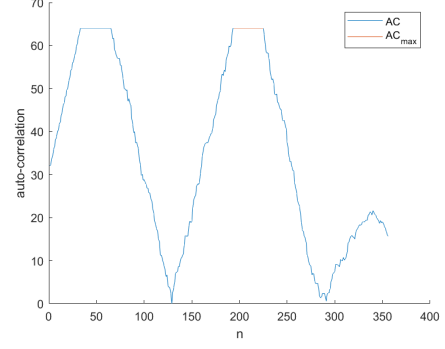


Fig. 2. Auto-correlation profile between the 802.11 legacy preamble and a copy of the preamble delayed of the L-LTF period.

associated with Kalman filtering. Accordingly, the evolution of the CFO of each target is modelled by the classical Kalman filter process and measurement equations (4) and (7) given hereafter [9].

The state vector x comprises the CFO and the CFO drift $\Delta\dot{\omega}$:

$$x = [\Delta\omega \quad \Delta\dot{\omega}] \quad (3)$$

Its evolution from time $k-1$ to time k is given by the following equation:

$$x_k = Fx_{k-1} + w \quad (4)$$

where:

- F is the state transition matrix given by the following expression:

$$F = \begin{bmatrix} 1 & dt \\ 0 & 1 \end{bmatrix} \quad (5)$$

with dt being the sampling interval.

- w is the process noise vector assumed to be Gaussian with zero-mean and covariance Q defined as:

$$Q = f_c^2 \begin{bmatrix} \sigma_2^2 dt + \sigma_3^2 \frac{dt^3}{3} & \sigma_3^2 \frac{dt^2}{2} \\ \sigma_3^2 \frac{dt^2}{2} & \sigma_3^2 dt \end{bmatrix} \quad (6)$$

with f_c being the carrier frequency, $\sigma_2 = 5.51 \cdot 10^{-18}$ and $\sigma_3 = 8.3 \cdot 10^{-25}$. This expression comes from the LO clock model given in [7] which includes the LO drift. The measurement vector z is linked to the state vector as follows:

$$z_k = Hx_k + v \quad (7)$$

where:

- H is the measurement matrix given by:

$$H = [1 \quad 0]^T \quad (8)$$

- v is the measurement noise vector assumed to be Gaussian with zero-mean and covariance R . The value of R has been set experimentally, by calculating the average variance of the estimated CFO of 100 successive Wi-Fi packets received every 100 ms.

2) *JPDAF*: The JPDAF is an algorithm that allows to perform soft decision tracking. It assumes that the number of targets to track N_T is known. It comprises 3 main stages described hereafter [10].

a) Prediction: In the JPDAF algorithm, all past information about each target until time $k - 1$ is condensed in the state estimate and in the estimated uncertainty covariance at time $k - 1$ respectively denoted as $\hat{x}_{k-1|k-1}$ and $P_{k-1|k-1}$. The estimated state vector, uncertainty covariance and the innovation covariance S at time k are predicted using the same equations as in the case of an ordinary Kalman filter:

$$\hat{x}_{k|k-1} = F\hat{x}_{k-1|k-1} \quad (9)$$

$$P_{k|k-1} = FP_{k-1|k-1}F^T + Q \quad (10)$$

$$S_k = HP_{k|k-1}H^T + R \quad (11)$$

The estimated state vector and the estimated uncertainty covariance are respectively initialised as:

$$\hat{x}_{0|0} = [z_0 \ 0]^T \quad P_{0|0} = \begin{bmatrix} R & 0 \\ 0 & 0 \end{bmatrix} \quad (12)$$

b) Determination of association probabilities: The second stage of the JPDAF consists in computing the probabilities that a measurement is associated to a given target. In order to determine these association probabilities, all possible joint association events are determined. This consists in all the possible combinations of track-measurement associations such that each measurement originates from at most one target and each target is responsible for at most one measurement. The probability of each joint association event A_k given the set of measurements Z_k is computed at time k as:

$$P(A_k|Z_k) = \frac{1}{c} \prod_j f_{k,t_j}(z_{k_j})^{\tau_j} \prod_t (P_D)^{\delta_t} (1 - P_D)^{1-\delta_t} \quad (13)$$

where z_{k_j} is the j^{th} measurement, P_D is the probability of detection set to $P_D = 0.99999$, τ_j is the measurement association indicator equal to 1 if the measurement is associated with a track in the considered joint association event and 0 otherwise, δ_t is the track association indicator equal to 1 if the track is associated to a measurement and 0 otherwise, c is a normalisation constant and $f_{k,t_j}(z_{k_j})$ is the likelihood that measurement j is associated to track t_j given by:

$$f_{k,t_j}(z_{k_j}) = \frac{e\left(-\frac{1}{2} \frac{(z_{k_j} - \hat{z}_{k|k-1}^{t_j})^2}{S_k^{t_j}}\right)}{\sqrt{2\pi S_k^{t_j}}} \quad (14)$$

where $\hat{z}_{k|k-1}^{t_j}$ is the predicted measurement corresponding to the target t associated with measurement j .

By summing all feasible association events where a given track is associated to a given measurement A_{jt_k} , the associations probabilities are determined:

$$\beta_{jt_k} = \sum_{A_k: A_{jt_k} \in A_k} P(A_k|Z_k) \quad (15)$$

where β_{jt_k} is the probability of the target t - measurement j association.

c) Update: for each track, the state is updated by weighting the innovations corresponding to each of the M measurements Z_k , denoted as v_{j_k} , according to the determined association probabilities:

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + W_k v_k \quad (16)$$

where v_k is the weighted innovation given by

$$v_k = \sum_j^M \beta_{j_k} v_{j_k} \quad (17)$$

and W_k is the Kalman gain computed as

$$W_k = P_{k|k-1} H^T S_k^{-1} \quad (18)$$

Finally, the estimated uncertainty covariance is updated as:

$$P_{k|k} = \beta_{0_k} P_{k|k-1} + (1 - \beta_{0_k}) P_{k|k}^c + \tilde{P}_k \quad (19)$$

where β_{0_k} is the probability that none of the measurements are associated with the target,

$$P_{k|k}^c = P_{k|k-1} - W_k S_k W_k^T \quad (20)$$

which is the covariance of the state updated with the correct measurement and

$$\tilde{P}_k = W_k \left(\sum_{j=1}^M \beta_{j_k} v_{j_k} v_{j_k}^T - v_k v_k^T \right) W_k^T \quad (21)$$

which represents the increase of the covariance due to uncertainty of association.

D. EN-NPDA associated with Kalman filter

One well known undesirable effect of the JPDAF is that track coalescence can occur when two or more track are close to each other. This "track merging" can lead to a high error in state estimation and make fingerprinting difficult. In order to avoid this problem, the EN-NPDA can be used.

The EN-NPDA is a variant on the JPDAF. The only change introduced consist in setting the probability of all feasible joint association events to zero except the highest one before computing the association probabilities [11]. The EN-NPDA is therefore a hard decision algorithm. Since RF fingerprinting requires to uniquely associate each packet to a given track, using a hard decision algorithm is suitable in this framework.

E. Track initiation and deletion

In the original JPDAF and EN-NPDA tracking algorithms, the number of targets to track is assumed to be known and constant. To deal with a variable number RF transmitters which can appear and disappear from the tracking scene, track management logic can be applied [12].

1) *Track initiation logic*: At each tracking instant k , measurements not associated to a track in the joint association event with the highest probability are send to the track initiation logic. Each of these measurements are considered to originate from a tentative track. An EN-NPDA algorithm determines which of these measurements are associated with current tentative tracks. Measurements which are not associated with any tentative tracks are considered as starting points of new tentative tracks. When a tentative track is associated to a measurement for $N_i = 3$ successive tracking time instants, the track is confirmed and is send to the main tracking algorithm.

2) *Track deletion logic*: When a confirmed track is not associated with a measurement for $N_d = 5$ successive tracking time instants, it is deleted.

A flowchart summarising the complete algorithm described in section II is shown in Figure 3.

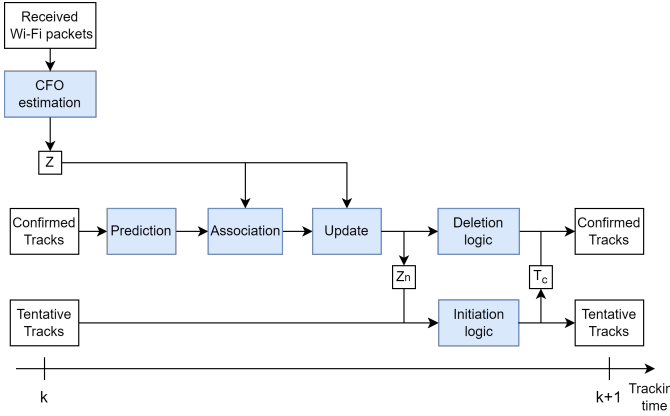


Fig. 3. Algorithm flowchart where Z are the measurements at time k , Z_n are the measurements not associated with a track and T_c are confirmed tracks.

III. SIMULATION

A. Simulation setup

Simulations have been performed in order to evaluate the performances of the JPDAF and EN-NPDA algorithms. The corresponding ground truth CFO are generated according to the system model equations (4) and (7). The values of different tracking parameters can be selected in a given range, as shown in Table I, in order to simulate different tracking scenarios described in the next section.

B. Simulations results

Three different scenarios have been simulated in order to evaluate the performances of the tracking algorithms and their limits. For each scenario, the performances have been evaluated graphically by comparing the measured CFO, the ground truth CFO and the CFO estimated by the JPDAF and EN-NPDA algorithms. They also have been evaluated

TABLE I
SIMULATION PARAMETERS AND THEIR RANGE

Symbol	Meaning	Range
N_{tracks}	Number of tracks	1 - 10
L_{simu}	Duration of the simulation	0 - 36000 s
$\Delta\omega_0$	Each track initial CFO	-20 - 20 kHz
$\Delta\dot{\omega}_0$	Each track initial CFO drift	-10 - 10 Hz/s
$N_{samples}$	Each track number of samples	0 - 50000
dt	Each track sampling interval	0.1 - 10 s
t_0	Each track appearing time	0 - L_{simu} s

numerically by two different metrics: 1) the association accuracy which corresponds to the fraction of sent packets correctly associated to a track in the feasible joint association event with the highest probability; 2) the root-mean square error (RSME) between the predicted CFOs and the ground truth CFO.

1) *Tracks appearing and disappearing from the tracking scene*: For this first scenario, a simulation comprising 4 tracks with different slopes was performed for a duration of 600 s with a sampling interval of 100 ms. As seen in Figure 4, showing the obtained graphical results, tracks 2 and 4 exist during the whole simulation while track 3 appears after 100 s and track 4 is deleted after 400 s.

Several observations can be made from Figure 4 and Table II, which presents the numerical results obtained for the different scenarios : 1) track 3 was correctly detected at 100 s and track 4 was correctly deleted after 400 s; 2) both JPDAF and EN-NPDA give similar CFO estimation which is close to the ground truth and has a low RMSE; 3) the obtained association accuracy is high with both algorithms. The very small fraction of packets that are not correctly associated correspond to occasional outliers that are not associated to any track.

TABLE II
SIMULATION NUMERICAL RESULTS

Track number	Association accuracy		RMSE (Hz)	
	JPDAF	EN-NPDA	JPDAF	EN-NPDA
Scenario 1				
1	0.998	0.998	19.785	19.799
2	0.997	0.997	35.766	35.175
3	0.998	0.998	18.507	18.389
4	0.998	0.998	48.128	47.632
Scenario 2				
1	0.929	0.929	77.317	77.317
2	0.929	0.929	246.014	249.035
3	0.913	0.913	52.764	52.575
4	0.838	0.838	262.215	286.590
Scenario 3				
1	0.580	0.587	111.761	77.076
2	0.447	0.447	39.978	42.262
3	0.473	0.477	49.49	28.964
4	0.615	0.620	124.675	69.799

2) *Increasing the sampling interval*: In this second scenario, all parameters are the same as in the first one, except the sampling interval which is increased to 10 s, which cor-

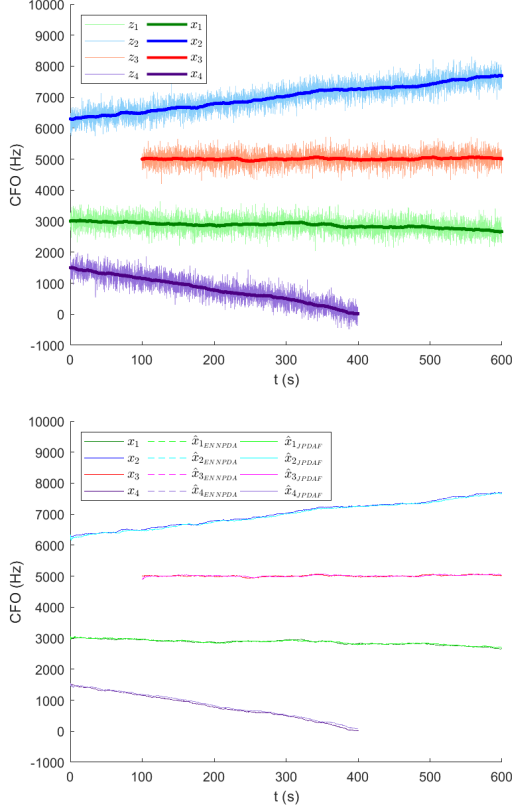


Fig. 4. Scenario 1: simulated tracks and simulation results where z_i is the i^{th} track measured CFO, x_i is the corresponding i^{th} track ground truth CFO, \hat{x}_{iJPDAF} and $\hat{x}_{iENNPDA}$ are the corresponding i^{th} track CFOs respectively estimated by the JPDAF and EN-NPDA.

responds to the maximal time interval between sent broadcast packets in the Wi-Fi standard. As observed in Figure 5 and in Table II, the RSMEs for both algorithms are larger than in scenario 1 as both the algorithm have trouble to converge, especially in the case of tracks with higher slopes. This leads to smaller association accuracies than in scenario 1.

3) *Tracks close to each other*: In this last scenario, 4 tracks that are initially very close to each other and then diverge are considered. The simulation lasts 100 s with a sampling time of 100 ms. Several observations and conclusions can be drawn from the results presented in Figure 6 and Table II : 1) Track coalescence can be observed for approximately 40 s in the estimation made by the JPDAF; 2) Using EN-NPDA allows to avoid track coalescence but introduces repulsion between the estimations of different tracks; 3) The RMSEs are globally higher than in scenarios with more distant tracks, especially with the JPDAF algorithm; 4) Although the EN-NPDA allows to improve the RMSE compare to the JPDAF, the association accuracies obtained with both algorithms are very similar and much lower than is the case of more distant tracks. This shows that one of the main limits of the implemented algorithms is that it does not perform well when the distance between tracks becomes too small.

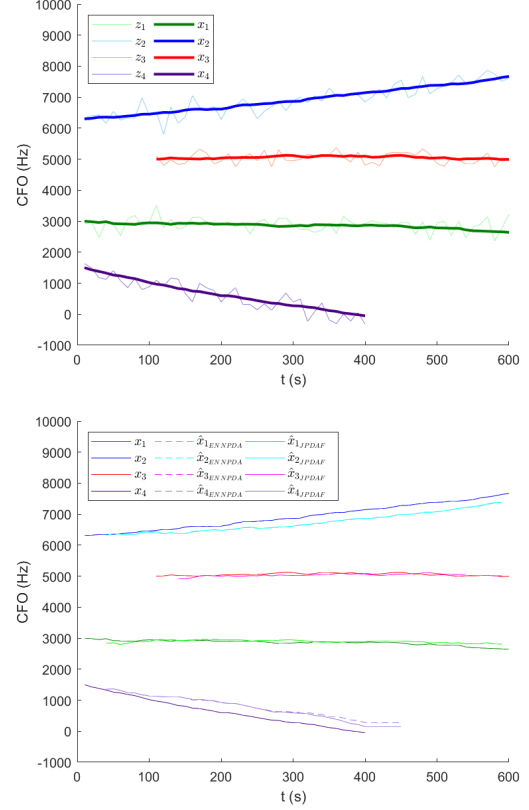


Fig. 5. Scenario 2: simulated tracks and simulation results

IV. EXPERIMENTAL SETUP AND RESULTS

A. Experimental setup

Our experimental setup is composed of 4 transmitters and one receiver, all of which are Ettus USRP X310. As shown in Figure 7, each transmitter is cable-connected to a RF adder, which is connected to the receiver. All the emitters transmit a data packet every 100 ms, at a rate of 20 MSamples/s and at a carrier frequency f_c of 2.55GHz, which corresponds to the parameters of the WiFi standard. The host PC records packets received by the receiver at f_c at a rate of 100 MSamples/s, for a duration of 10 min. The TCXO of the USRP are used as LOs. To be able to only record actual data packets and not the zeros received in between, an auto-correlator is implemented directly in the FPGA image of the receiver. In order to identify the sender of each received packet for ground-truth purposes, the packets from each transmitter have a unique payload.

B. Results

The raw experimental results and the results obtained when applying the JPDAF and EN-NPDA algorithms associated to Kalman filtering are shown in Figure 8. The numerical results are presented in Table III. A few observations can be made: 1) the high CFO noise causes the CFO estimations of different targets to overlap; 2) the CFO is not constant with time, but

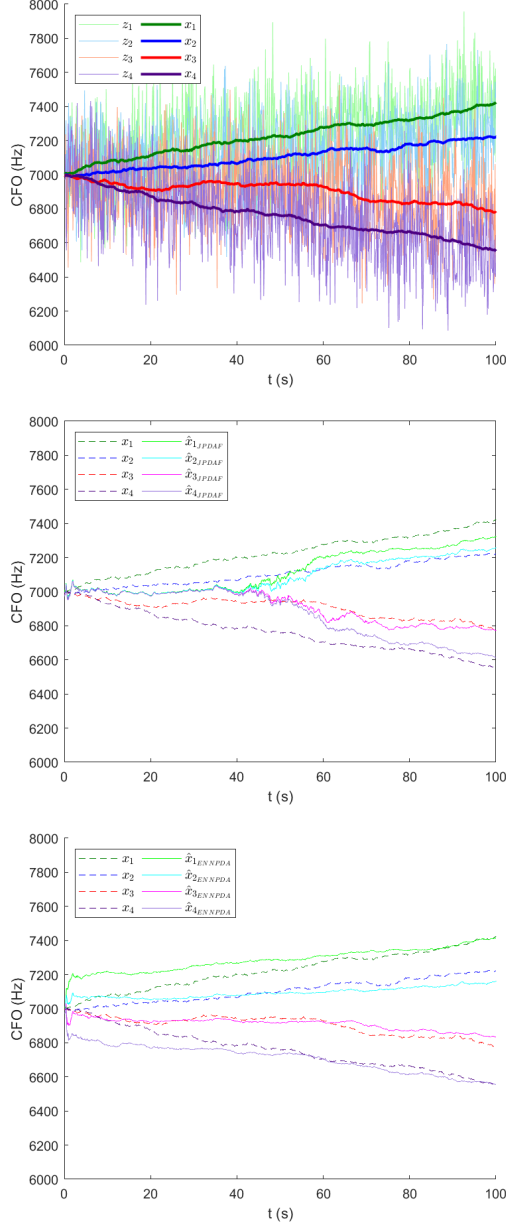


Fig. 6. Scenario 3: simulated tracks and simulation results

drifts at speeds of tens of Hz per minute; 3) the JPDAF and EN-NPDA allows to track the CFOs from different targets and associate each received packet to a given target with a high accuracy. However, no significant difference is observed between the JPDAF and the EN-NPDA in terms of association accuracy.

V. CONCLUSION

This paper describes an RF multi-target tracking and fingerprinting algorithm which uses the CFO, assumed to be drifting, as a feature. Simulation results show that the JPDAF and EN-NPDA algorithms present very good performances when the

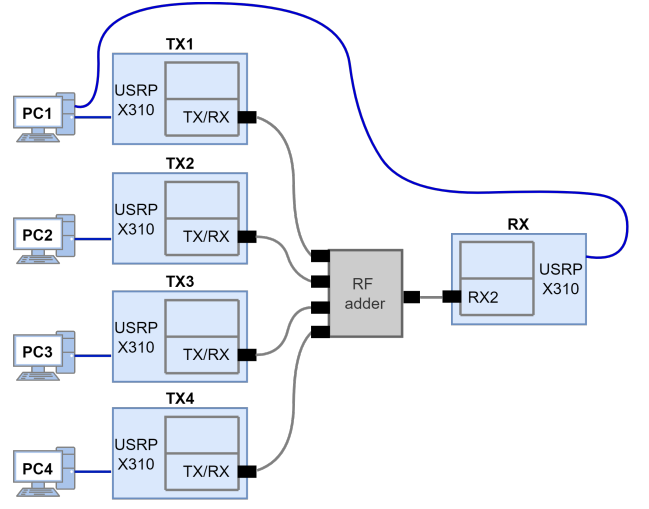


Fig. 7. Block-diagram of the experimental setup.

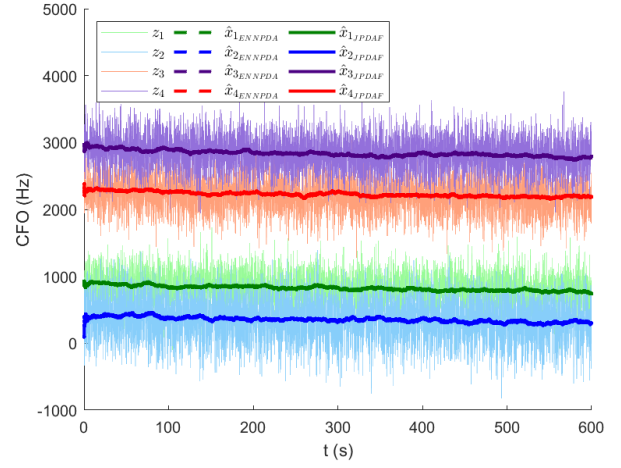


Fig. 8. Results where z_i is the raw estimated CFO of the i^{th} transmitter, \hat{x}_{i_JPDAF} and $\hat{x}_{i_EN-NPDA}$ are the corresponding CFO estimation obtained with respectively with JPDAF and EN-NPDA associated with Kalman filtering

different tracks are well separated and packets are available every 100 ms. The performances of the algorithm are strongly degraded when tracks are close to each other. Increasing the sampling interval causes slower convergence of the algorithm, which decreases its overall performance. The algorithms are evaluated on a experimental dataset, confirming the previous

TABLE III
EXPERIMENTAL NUMERICAL RESULTS

Track number	Association accuracy	
	JPDAF	EN-NPDA
1	0.873	0.873
2	0.861	0.862
3	0.952	0.951
4	0.953	0.952

tendencies. As future work, we would like to consider multi-target tracking algorithms such as multi-hypothesis tracking in which a tree considering all track-target associations for several tracking instants is constructed which allows to make the track-target association decision after several tracking instants.

REFERENCES

- [1] Q. Xu, R. Zheng, W. Saad and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," in *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 94-104, Firstquarter 2016
- [2] O. Gungor and C. E. Koksul, "On the Basic Limits of RF-Fingerprint-Based Authentication," in *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4523-4543, Aug. 2016
- [3] M. Cekic, S. Gopalakrishnan, U. Madhow, "Wireless fingerprinting via Deep Learning: The Impact of Confounding Factors", arXiv, 2021
- [4] C. G. Wheeler and D. R. Reising, "Assessment of the impact of CFO on RF-DNA fingerprint classification performance," 2017 International Conference on Computing, Networking and Communications (ICNC), 2017
- [5] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu and Y. Yan, "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," in *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 349-360, Feb. 2019
- [6] A. Ali and G. Fischer, "The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection," 2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON), 2019, pp. 1-6
- [7] C. Zucca and P. Tavella, "The clock model and its relationship with the Allan and related variances," in *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 52, no. 2, pp. 289-296, Feb. 2005
- [8] Horlin Francois and Bourdoux Andre, "Digital compensation for analog front-ends : a new approach to wireless transceiver design". John Wiley Sons Incorporated, 2008
- [9] M. Rhudy, R. Salguero and K. Holappa, "A Kalman Filtering Tutorial for Undergraduate Students", *International Journal of Computer Science Engineering Survey*, vol. 08, no. 01, pp. 01-18, 2017
- [10] Y. Bar-Shalom, F. Daum and J. Huang, "The probabilistic data association filter," in *IEEE Control Systems Magazine*, vol. 29, no. 6, pp. 82-100, Dec. 2009
- [11] H. L. Kennedy, "Controlling track coalescence with scaled Joint Probabilistic Data Association," 2008 International Conference on Radar, pp. 440-445, 2008
- [12] L. Storrer et al., "Indoor Tracking of Multiple Individuals With an 802.11ax Wi-Fi-Based Multi-Antenna Passive Radar," in *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20462-20474, 15 Sept.15, 2021

Linear Precoder Design in Massive MIMO under Realistic Power Amplifier Consumption Constraint

Emanuele Peschiera 

ESAT-DRAMCO

KU Leuven, Technology Campus Ghent

9000 Ghent, Belgium

emanuele.peschiera@kuleuven.be

François Rottenberg 

ESAT-DRAMCO

KU Leuven, Technology Campus Ghent

9000 Ghent, Belgium

françois.rottenberg@kuleuven.be

Abstract—The energy consumption of wireless networks is a growing concern. In massive MIMO systems, which are being increasingly deployed as part of the 5G roll-out, the power amplifiers in the base stations have a large impact in terms of power demands. Most of the current massive MIMO precoders are designed to minimize the transmit power. However, the efficiency of the power amplifiers depend on their operating regime with respect to their saturation regime, and the consumed power proves to be non-linearly related to the transmit power. Power consumption-based equivalents of maximum ratio transmission, zero-forcing, and regularized zero-forcing precoders are therefore proposed. We show how the structure of the solutions radically changes. While all antennas should be active in order to minimize the transmit power, we find on the contrary that a smaller number of antennas should be activated if the objective is the power consumed by the power amplifiers.

Index Terms—massive MIMO linear precoders, power consumption model, power amplifier efficiency.

I. INTRODUCTION

Information and communication technologies consumed approximately 100 TWh of electricity in 2021, which represents the 6-7% of the world electricity demand [1]. About two thirds of energy consumption come from the mobile networks, where base stations (BSs) are accountable for the 80% of the total consumption on average [2]. Therefore, it is important to include realistic power consumption criteria into the design of communication systems.

The current state of the art linear massive MIMO precoders, e.g., maximum ratio transmission (MRT), zero-forcing (ZF) and regularized zero-forcing (RZF) [4], are obtained under a total transmit power constraint and not a total consumed power constraint. Indeed, these precoders minimize the total transmit power given that certain user requirements are satisfied. Implicitly, the consumed power p_{cons} is assumed to be linearly proportional to the transmit power p_{tx} , i.e.,

$$p_{\text{cons}} = p_{\text{tx}}/\eta, \quad (1)$$

η being the power amplifier (PA) efficiency, which is assumed to be constant. However, it is known that the actual PA efficiency is not constant but depends on the ratio between the output power and the maximum output power, i.e., the back-off [5]. It is generally agreed that the PA causes most

losses in the transmitter [3], therefore its realistic behavior needs to be taken into account. Given a BS equipped with M antennas, and defining p_m as the output power at the PA m , the total transmit power is $p_{\text{tx}} = \sum_{m=0}^{M-1} p_m$. A more realistic model of the efficiency of the PA of antenna m is given by [6]

$$\eta_m = \eta_{\text{max}} \sqrt{\frac{p_m}{p_{\text{max}}}}, \quad (2)$$

where p_{max} is the maximal PA output power and η_{max} is the maximal PA efficiency, obtained for $p_m = p_{\text{max}}$, which is, e.g., around 78.5% for class B amplifiers. The model in (2) has been shown to be accurate for many classes of amplifiers when the output power is low [5]. The total consumed power becomes

$$p_{\text{cons}} = \sum_{m=0}^{M-1} p_m/\eta_m = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \sum_{m=0}^{M-1} \sqrt{p_m}. \quad (3)$$

Therefore, p_{cons} presents a square root dependence on p_m . As a result, common designs that minimize the total transmit power do not minimize the total consumed power. To the best of our knowledge, few works have taken this more advanced model into account for design precoders. The MISO case has been studied in [6]. In [7], the problem was analyzed in detail from the capacity point of view in point-to-point MIMO, but only formulated for multi-user MIMO. No results and interpretations were proposed in the latter case.

In this work, we study novel precoders that minimize the consumed power subject to user performance criteria and a maximal per-antenna output power constraint. Our contribution can be summarized as follows:

- We first show the expression of the consumed power in terms of the precoding coefficients. In the multi-user case, p_{cons} corresponds to the $L_{2,1}$ norm of the precoding matrix. In the single-user case, it simplifies to the L_1 norm of the precoding vector. These norms preserve convexity, which allows to obtain efficient solutions, and promote sparsity, which radically changes the structure of the solution compared to the conventional precoders.
- We then derive the power consumption-efficient equivalent of MRT precoder in the single-user scenario. The closed-form solution, which was previously obtained in [6], consequently saturates the antennas with the strongest

channel gains until the required SNR is achieved. The gain in power consumption is evaluated varying the number of BS antennas.

- Last, we investigate the power consumption-efficient equivalents of ZF and RZF precoders in the multi-user scenario. In this case, convex optimization solvers allow to obtain the precoding coefficients. Compared to conventional precoders, a smaller number of antennas are activated. As the number of users grows, more antennas are utilized, and the gain in power consumption decreases.

A. Notations

Vectors and matrices are denoted by bold lowercase and uppercase letters, respectively. Superscripts $*$, T and \dagger stand for complex conjugate, transpose, and conjugate transpose operators. The symbols $\text{tr}[\cdot]$ and $\mathbb{E}[\cdot]$ denote the trace and the expectation operators, while j is the imaginary unit. The notation $\text{diag}(\mathbf{a})$ refers to a diagonal matrix whose k -th diagonal entry is equal to the k -th entry of the vector \mathbf{a} . A zero-mean complex Gaussian random variable with variance σ^2 is represented by $\mathcal{CN}(0, \sigma^2)$. A $K \times 1$ all-zero vector is $\mathbf{0}_K$, while \mathbf{I}_K is an identity matrix of size K . The (i, j) -th element of \mathbf{A} is indicated by $[\mathbf{A}]_{i,j}$. Last, $\mathbf{A}^{1/2} = \mathbf{B} \iff \mathbf{A} = \mathbf{B}\mathbf{B}$, $\mathbf{A}^n = \underbrace{\mathbf{A}\mathbf{A} \dots \mathbf{A}}_{n \text{ times}}$, and $\mathbf{A}^{-n} = \underbrace{\mathbf{A}^{-1}\mathbf{A}^{-1} \dots \mathbf{A}^{-1}}_{n \text{ times}}$ for $n \in \mathbb{N}^+$.

II. SYSTEM MODEL

A. Signal Model

We consider a massive MIMO system with M antennas and K users. The symbol of user k is denoted by s_k , it has unitary power and different user symbols are assumed uncorrelated. The symbols are linearly precoded so that the transmitted signal $\mathbf{x} \in \mathbb{C}^{M \times 1}$ is

$$\mathbf{x} = \mathbf{W}^T \mathbf{s}, \quad (4)$$

where $\mathbf{W} \in \mathbb{C}^{K \times M}$ is the precoding matrix and $\mathbf{s} \in \mathbb{C}^{K \times 1}$ contains the transmitted symbols. The coefficient $[\mathbf{W}]_{k,m} = w_{k,m}$ represents the precoding weight for user k at antenna m . The received signal $\mathbf{r} \in \mathbb{C}^{K \times 1}$ is

$$\mathbf{r} = \mathbf{H}\mathbf{x} + \boldsymbol{\nu}, \quad (5)$$

where $\mathbf{H} \in \mathbb{C}^{K \times M}$ is the channel matrix, $[\mathbf{H}]_{k,m} = h_{k,m}$ being the channel between user k and antenna m , and $\boldsymbol{\nu} \sim \mathcal{CN}(\mathbf{0}_K, \sigma_\nu^2 \mathbf{I}_K)$ represents the thermal noise.

B. Consumed Power Model

Being the symbols uncorrelated and with unit power, the transmit power at antenna m is

$$p_m = \mathbb{E}[|x_m|^2] = \sum_{k=0}^{K-1} |w_{k,m}|^2, \quad (6)$$

and the total transmit power becomes

$$p_{\text{tx}} = \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} |w_{k,m}|^2 = \|\mathbf{W}\|_F^2, \quad (7)$$

where $\|\cdot\|_F$ is the Frobenius norm. Using the model in (3), the total consumed power by the PAs can be expressed as

$$p_{\text{cons}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \sum_{m=0}^{M-1} \sqrt{\sum_{k=0}^{K-1} |w_{k,m}|^2} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \|\mathbf{W}\|_{2,1}, \quad (8)$$

where $\|\cdot\|_{2,1}$ is the $L_{2,1}$ norm.

C. Channel Model

As channel models, we consider pure line-of-sight (LOS) and independent and identically distributed (i.i.d.) Rayleigh fading, which corresponds to non-line-of-sight (NLOS) scenarios¹. For LOS channels, and assuming a uniform linear array (ULA) with inter-antenna spacing of half a wavelength,

$$[\mathbf{H}]_{k,m} = e^{-j\pi \cos \theta_k m}, \quad (9)$$

where θ_k is the user angle with respect to the array axis. In NLOS channels,

$$[\mathbf{H}]_{k,m} = h_{k,m}, \quad (10)$$

where $h_{k,m} \sim \mathcal{CN}(0, 1)$ is the small-scale fading coefficient, which is assumed uncorrelated to the other coefficients in \mathbf{H} .

III. SINGLE-USER SCENARIO

When $K = 1$, the precoding matrix becomes a vector $\mathbf{w} \in \mathbb{C}^{1 \times M}$. Accordingly, the Frobenius norm simplifies to the squared L_2 norm, i.e., $p_{\text{tx}} = \|\mathbf{w}\|_2^2$, while the $L_{2,1}$ norm becomes the L_1 norm, i.e., $p_{\text{cons}} = \|\mathbf{w}\|_1$. In the following, the index k is omitted for clarity. Since no inter-user interference is present, the main parameter is the signal-to-noise ratio (SNR), defined as

$$\text{SNR} = \frac{\left| \sum_{m=0}^{M-1} h_m w_m \right|^2}{\sigma_\nu^2}. \quad (11)$$

The conventional MRT can be found by minimizing the total transmit power under a received SNR constraint γ

$$\begin{aligned} & \underset{\{w_m\}}{\text{minimize}} && p_{\text{tx}} = \|\mathbf{w}\|_2^2 \\ & \text{subject to} && \frac{\left| \sum_{m=0}^{M-1} h_m w_m \right|^2}{\sigma_\nu^2} \geq \gamma. \end{aligned} \quad (12)$$

While the objective function is convex, the constraint is not convex. Anyway, we can consider $\sum_{m=0}^{M-1} h_m w_m$ to be purely real and positive as this would imply the multiplication by a constant phasor (done at the receiver to perform coherent combining) and would not change both the objective function and the constraint. The problem becomes

$$\begin{aligned} & \underset{\{w_m\}}{\text{minimize}} && p_{\text{tx}} = \|\mathbf{w}\|_2^2 \\ & \text{subject to} && \sum_{m=0}^{M-1} h_m w_m \geq \gamma^{1/2} \sigma_\nu, \end{aligned} \quad (13)$$

¹We did not include the large-scale fading as we make a first comparison between conventional and power consumption-efficient precoders, and we consider low output powers compared to the PA saturation power.

which is a convex problem and can be solved, e.g., exploiting the Karush–Kuhn–Tucker (KKT) conditions. The well-known MRT precoder is thus obtained, i.e., $\mathbf{w}^{\text{MRT}} = \sqrt{p_{\text{tx}}} \mathbf{h}^* / \|\mathbf{h}\|_2$, which achieves $\text{SNR}^{\text{MRT}} = p_{\text{tx}} \|\mathbf{h}\|_2^2 / \sigma_\nu^2$, where $\mathbf{h} \in \mathbb{C}^{1 \times M}$ is the channel vector.

The power consumption-efficient version of the previous precoder, together with a maximal per-antenna power constraint (i.e., the PA output saturation power constraint), is

$$\begin{aligned} & \underset{\{w_m\}}{\text{minimize}} && p_{\text{cons}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \|\mathbf{w}\|_1 \\ & \text{subject to} && \sum_{m=0}^{M-1} h_m w_m \geq \gamma^{1/2} \sigma_\nu, \\ & && |w_m|^2 \leq p_{\text{max}} \quad \forall m. \end{aligned} \quad (14)$$

The problem is convex, and therefore can be efficiently solved numerically [8], [9]. Moreover, a closed-form solution can be found through the KKT conditions by considering real non-negative precoding coefficients. Indeed, when the optimization variable is $\{g_m = w_m e^{j\angle h_m} \in \mathbb{R}, g_m \geq 0\}$, (14) becomes differentiable. The optimal solution corresponds to pouring power in the antenna with strongest channel gain $|h_m|$ until saturation, then the second one, and so on until the target SNR is achieved². A similar result has been obtained in [6]. Defining \mathcal{K}_- and \mathcal{K}_+ as the sets of the antennas with the $L-1$ and L strongest channel gains, we denote $\tilde{m} = \arg \min_{m \in \mathcal{K}_+} |h_m|$. The precoding coefficients are then given by

$$w_m^{\text{MRT-eff.}} = e^{-j\angle h_m} \begin{cases} \sqrt{p_{\text{max}}} & \text{if } m \in \mathcal{K}_- \\ \frac{\gamma^{1/2} \sigma_\nu - \zeta}{|h_{\tilde{m}}|} & \text{if } m = \tilde{m} \\ 0 & \text{otherwise,} \end{cases} \quad (15)$$

where $\zeta = \sqrt{p_{\text{max}}} \sum_{m' \in \mathcal{K}_-} |h_{m'}|$. Therefore, the antennas associated with the $M-L-1$ channel gains remain inactive. This represents a major difference with respect to the conventional MRT, in which all the antennas are active provided that their channel gain is greater than zero. The transmit power required by the MRT is $p_{\text{tx}}^{\text{MRT}} = \gamma \sigma_\nu^2 / \|\mathbf{h}\|_2^2$, hence, using (8),

$$p_{\text{cons}}^{\text{MRT}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \gamma^{1/2} \sigma_\nu \frac{\|\mathbf{h}\|_1}{\|\mathbf{h}\|_2^2}. \quad (16)$$

In the power consumption-efficient MRT, when no maximal per-antenna power constraint is considered, all the power is allocated to antenna $\hat{m} = \arg \max_m |h_m|$. The transmit power becomes $p_{\text{tx}}^{\text{MRT-eff.}} = \gamma \sigma_\nu^2 / |h_{\hat{m}}|^2$, and the consumed power is

$$p_{\text{cons}}^{\text{MRT-eff.}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \gamma^{1/2} \sigma_\nu \frac{1}{\|\mathbf{h}\|_\infty}. \quad (17)$$

where $\|\mathbf{h}\|_\infty = |h_{\hat{m}}|$ is the ∞ -norm of \mathbf{h} . The power consumption gain (PCG) is therefore

$$\text{PCG} = \frac{p_{\text{cons}}^{\text{MRT}}}{p_{\text{cons}}^{\text{MRT-eff.}}} = \|\mathbf{h}\|_\infty \frac{\|\mathbf{h}\|_1}{\|\mathbf{h}\|_2^2}. \quad (18)$$

²Note that the problem can be unfeasible if the target SNR is not achieved by setting all antennas to saturation.

For a pure LOS channel, $|h_m| = 1 \quad \forall m$, hence $\text{PCG} = 1$. If γ is achieved, any power allocation gives the same result (the first constraint in (14) reduces to $\sum_{m=0}^{M-1} g_m = \gamma^{1/2} \sigma_\nu$, which directly fixes the value of the cost function). When $|h_m|$ varies among the antennas, there is a gain in p_{cons} .

IV. MULTI-USER SCENARIO

Let us define the SINR of user k as

$$\text{SINR}_k = \frac{\left| \sum_{m=0}^{M-1} h_{k,m} w_{k,m} \right|^2}{\sum_{k'=0, k' \neq k}^{K-1} \left| \sum_{m=0}^{M-1} h_{k',m} w_{k',m} \right|^2 + \sigma_\nu^2}. \quad (19)$$

Given a target SINR γ_k for each user, the conventional precoders can be found as a solution to

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{tx}} = \|\mathbf{W}\|_F^2 \\ & \text{subject to} && \text{SINR}_k \geq \gamma_k \quad \forall k. \end{aligned} \quad (20)$$

The SINR constraints are not convex, but can be reformulated as convex [10], and the problem can be solved numerically. The power consumption-efficient precoders, together with a maximal per-antenna power constraint, are designed by solving

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{cons}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \|\mathbf{W}\|_{2,1} \\ & \text{subject to} && \text{SINR}_k \geq \gamma_k \quad \forall k, \\ & && \sum_{k=0}^{K-1} |w_{k,m}|^2 \leq p_{\text{max}} \quad \forall m. \end{aligned} \quad (21)$$

It is known how the $L_{2,1}$ norm promotes sparsity. Therefore, similarly to what happens in the single-user scenario, one can expect only a subset of BS antennas will be activated. However, it is important to remark how, to be able to spatially multiplex the K users, at least K antennas should be active. More in general, a decrease in the PCG is expected when the ratio M/K decreases.

A. Zero-Forcing

The ZF precoder is found by imposing zero inter-user interference. Defining $\mathbf{D}_\gamma = \text{diag}(\gamma_0, \dots, \gamma_{K-1})$ as the diagonal matrix containing the required SNRs of the users, the conventional ZF is found by solving

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{tx}} = \|\mathbf{W}\|_F^2 \\ & \text{subject to} && \mathbf{H}\mathbf{W}^T = \mathbf{D}_\gamma^{1/2} \sigma_\nu. \end{aligned} \quad (22)$$

The above problem is convex and can be solved, e.g., using the Lagrange multipliers method, obtaining

$$(\mathbf{W}^{\text{ZF}})^T = \mathbf{H}^\dagger (\mathbf{H}\mathbf{H}^\dagger)^{-1} \mathbf{D}_\gamma^{1/2} \sigma_\nu. \quad (23)$$

The power consumption-efficient ZF precoder, whose solution is denoted by $\mathbf{W}^{\text{ZF-eff.}}$, corresponds to

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{cons}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \|\mathbf{W}\|_{2,1} \\ & \text{subject to} && \mathbf{H}\mathbf{W}^T = \mathbf{D}_\gamma^{1/2} \sigma_\nu, \\ & && \sum_{k=0}^{K-1} |w_{k,m}|^2 \leq p_{\text{max}} \quad \forall m. \end{aligned} \quad (24)$$

This problem also has a convex formulation. However, it is difficult to find a closed form solution, but it can be easily solved numerically. To compare the two precoders, the PCG is computed as

$$\text{PCG} = \|\mathbf{W}^{\text{ZF}}\|_{2,1} / \|\mathbf{W}^{\text{ZF-eff.}}\|_{2,1}. \quad (25)$$

B. Regularized Zero-Forcing

The conventional RZF precoder design problem is³

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{tx}} = \|\mathbf{W}\|_F^2 \\ & \text{subject to} && \|\mathbf{H}\mathbf{W}^T - \mathbf{D}_\gamma^{1/2}\sigma_\nu\|_F^2 \leq \xi, \end{aligned} \quad (26)$$

where $\xi = \sigma_\nu^2 \text{tr} \left[\mathbf{D}_\gamma \left(\frac{1}{\sigma_\nu^2} \mathbf{A} + \mathbf{I}_K \right)^{-2} \right]$ and the square matrix $\mathbf{A} = \text{diag}(\lambda_0, \dots, \lambda_{K-1})$ contains the eigenvalues of $\mathbf{H}\mathbf{H}^\dagger$. Using the matrix eigendecomposition, \mathbf{A} can be computed by solving $\mathbf{H}\mathbf{H}^\dagger = \mathbf{U}\mathbf{A}\mathbf{U}^*$, \mathbf{U} being the matrix having the eigenvectors of $\mathbf{H}\mathbf{H}^\dagger$ on its columns. The problem at hand is convex and its well-known solution is

$$\left(\mathbf{W}^{\text{RZF}} \right)^T = \mathbf{H}^\dagger \left(\mathbf{H}\mathbf{H}^\dagger + \sigma_\nu^2 \mathbf{I}_K \right)^{-1} \mathbf{D}_\gamma^{1/2} \sigma_\nu. \quad (27)$$

The power consumption-efficient RZF is then given by

$$\begin{aligned} & \underset{\{w_{k,m}\}}{\text{minimize}} && p_{\text{cons}} = \frac{\sqrt{p_{\text{max}}}}{\eta_{\text{max}}} \|\mathbf{W}\|_{2,1} \\ & \text{subject to} && \|\mathbf{H}\mathbf{W}^T - \mathbf{D}_\gamma^{1/2}\sigma_\nu\|_F^2 \leq \xi, \\ & && \sum_{k=0}^{K-1} |w_{k,m}|^2 \leq p_{\text{max}} \quad \forall m. \end{aligned} \quad (28)$$

As for the ZF precoder, the problem is difficult to be solved analytically, despite having a convex formulation. However, numerical solvers can efficiently solve it. The obtained precoder can be compared to the one in (27) using (25).

V. NUMERICAL RESULTS

The numerical experiments have been carried out using as target SNR $\gamma_k = \gamma = 10$ dB, $\sigma_\nu = 1$ and no maximal per-antenna power constraint. The constraint on p_{max} has been removed for comparison purposes, as standard precoders do not consider it. In the single-user scenario, only NLOS channels has been simulated, as in LOS channels eq. (18) loses significance. Instead, in the multi-user scenario, both NLOS and LOS channels have been investigated.

In case of single-user systems, the results in terms of PCG are shown in Fig. 1. The PCG increases with M , as expected. Indeed, having no constraint on p_{max} , only one antenna will be active in the power consumption-efficient precoder, regardless of M . Note that having a large M is still important to increase spatial diversity in the selection of the antenna with the best channel gain. In the conventional MRT, instead, every additional antenna will be used, and therefore the gain in

p_{cons} will be greater for larger numbers of BS antennas. For $M = 100$ the PCG equals 2, corresponding to the 50% of power saving. Considering the constraint on p_{max} , the PCG is expected to decrease when p_{max} is comparable to γ . More antennas will be saturated to achieve the SNR requirement, and this will reduce the gap between the two precoders.

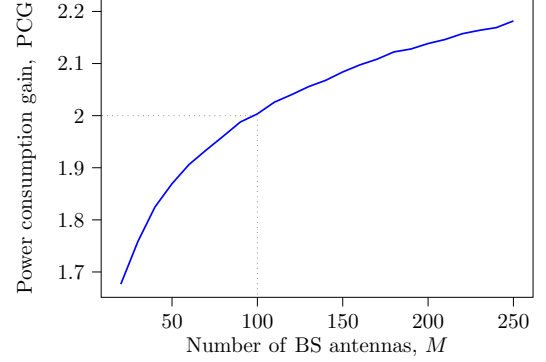


Fig. 1. Power consumption gain as a function of BS antennas for single-user case in NLOS channel, based on eq. (18). PCG was averaged over 10^4 channel realizations.

For multi-user systems, the power consumption-efficient precoders also select a subset of the M antennas. Fig. 2 shows how, for a ZF precoder with $M = 64$ and two users in a NLOS channel, only few antennas will have a non-zero power. When eight users are present (Fig. 3), more antennas will be activated in order to meet the SINR requirements of the users and mitigate inter-user interference. Nonetheless, the power distribution among the antennas varies significantly with respect to the conventional ZF scheme. About half of the antennas have $p_m \neq 0$ in the p_{cons} -efficient ZF, while all the antennas are utilized in the conventional ZF. Figure 4 illustrates the PCG as a function of M in NLOS channels. For $K = 2$, the PCG is still significant, e.g., it is equal to the 35% when $M = 64$. For eight users, instead, the PCG decreases and, when $M = 64$, the power saving is around the 11%. Differently from the single-user scenario, the introduction of the constraint on p_{max} is here expected to have less impact (especially for large values of K). Indeed, multiple antennas have to be used in order to multiplex different users, thus their power will less likely be set closer to saturation. In general, in LOS channels the PCG values are lower and close to one, i.e., no gain in power consumption. Similarly to the single-user case, in which the L_1 norm and the squared L_2 norm are equivalent for unitary channel gains, the optimization on the $L_{2,1}$ norm and on the squared Frobenius norm gives similar results.

VI. CONCLUSION

In this work, we conducted a first study on power consumption-efficient equivalents of the common massive MIMO linear precoders. A realistic expression of the power consumption, which is proportional to the square root of the transmit power, is first presented. The precoder design

³We fixed the value of ξ by using the KKT conditions for problem (26) such that to obtain the precoding matrix in (27). The proof is omitted for space reasons.

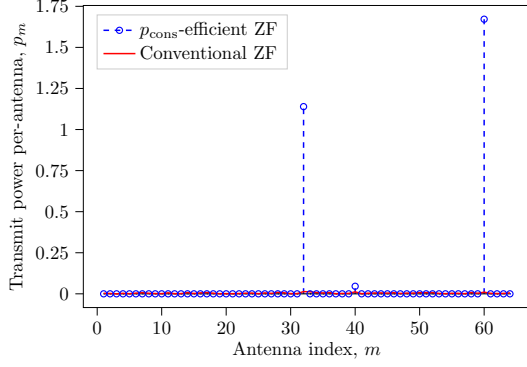


Fig. 2. Transmit power per-antenna for multi-user case with $K = 2$ in NLOS channel. Conventional ZF (in red) and power consumption-efficient ZF (in blue) are shown.

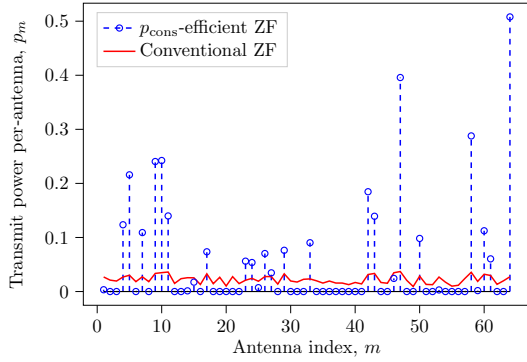


Fig. 3. Transmit power per-antenna for multi-user case with $K = 8$ in NLOS channel. Conventional ZF (in red) and power consumption-efficient ZF (in blue) are shown.

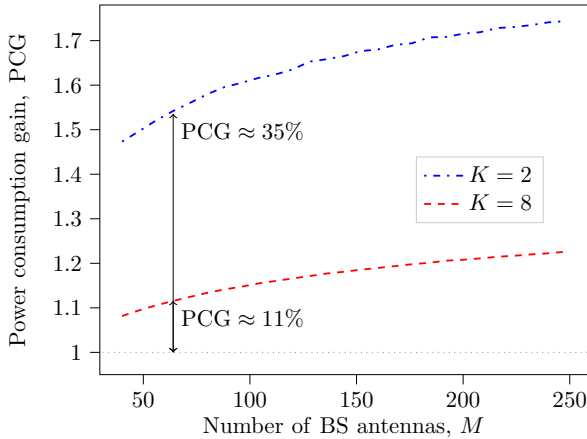


Fig. 4. Power consumption gain as a function of BS antennas for ZF precoder in NLOS channel, $K = 2$ (in blue) and $K = 8$ (in red). PCG was averaged over 10^3 channel realizations.

problems preserve convexity and can be easily solved numerically. In NLOS channels for both single-user and multi-user systems, the proposed precoders tend to activate few antennas compared to the conventional precoders. In LOS channels, given the same channel gains across both the antennas and the users, there are no significant differences. For the single-user scenario, a closed-form expression of the p_{cons} -efficient precoder is illustrated, and the gain in power consumption is equal to 1.92 for $M = 64$. Moving to the multi-user systems, the precoders design problem are first formulated and then solved numerically for a fixed SNR. For $M = 64$, the gain in power consumption varies from 1.54 when $K = 2$ to 1.12 when $K = 8$. The gap between the p_{cons} -efficient precoders and the transmit power-based precoders is not significant when several users are present. However, the structure of the retrieved solutions (e.g., Fig. 3) can provide further insights. Indeed, the entire RF chain of the non-active antennas can be turned off, and this will likely be associated with a higher PCG. More advanced models, e.g., including the circuit power consumption of each antenna, should be employed to have a complete characterization of the problem [11]. Future works also include numerical experiments considering the maximal per-antenna power constraint for both conventional and power consumption-efficient precoders. Non-linear distortion terms caused by the PA can also be included in the precoder design, similarly to [12]. The analysis of multi-carrier systems would be of interest too, and cell-free deployments certainly need to be investigated.

REFERENCES

- [1] D. Bol, T. Pirson, and R. Dekimpe, "Moore's law and ICT innovation in the anthropocene," in IEEE Des. Test Eur. Conf. 2021, 2021.
- [2] M. Yan, C. A. Chan, A. F. Gyga et al., "Modeling the total energy consumption of mobile network services and applications," *Energies*, vol. 12, no. 1, 2019.
- [3] J. N. Murdock and T. S. Rappaport, "Consumption factor and power-efficiency factor: a theory for evaluating the energy efficiency of cascaded communication systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 2, pp. 221-236, 2014.
- [4] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: spectral, energy, and hardware efficiency," *Found. Trends Signal Process.*, vol. 11, no. 3-4, pp. 154-655, 2017.
- [5] A. Grebennikov, "RF and microwave power amplifier design," 1st ed., New York, NY, USA: McGraw-Hill, 2005.
- [6] D. Persson, T. Eriksson, and E. G. Larsson, "Amplifier-aware multiple-input multiple-output power allocation," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1112-1115, 2013.
- [7] H. V. Cheng, D. Persson, and E. G. Larsson, "Optimal MIMO precoding under a constraint on the amplifier power consumption," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 218-229, 2019.
- [8] S. Diamond and S. Boyd, "CVXPY: A Python-embedded modeling language for convex optimization," *J. Mach. Learn. Res.*, vol. 17, no. 83, pp. 1-5, 2016.
- [9] A. Agrawal, R. Verschuere, S. Diamond, and S. Boyd, "A rewriting system for convex optimization problems," *J. Control. Decis.*, vol. 5, no. 1, pp. 42-60, 2018.
- [10] M. Bengtsson and B. Ottersten, "Optimal and suboptimal transmit beamforming," in *Handbook of Antennas in Wireless Communications*, Boca Raton, FL, USA: CRC Press, 2001, pp. 568-600.
- [11] O. T. Demir, M. Masoudi, E. Björnson, and C. Cavdar, "Cell-Free massive MIMO in virtualized CRAN: how to minimize the total network power?," in *ICC 2022 - IEEE Int. Conf. Commun.*, 2022.
- [12] F. Rottenberg, G. Callebaut, and L. Van Der Perre, "Z3RO precoder canceling nonlinear power amplifier distortion in large array systems," in *ICC 2022 - IEEE Int. Conf. Commun.*, 2022.

Observability analysis of Direction-of-Arrival estimation using dual-antenna receivers

Youssef Agram
Brussels School of Engineering
Université Libre de Bruxelles (ULB)
Brussels, Belgium
Youssef.Agram@ulb.be

Jianqiao Cheng
Brussels School of Engineering
Université Libre de Bruxelles (ULB)
Brussels, Belgium
Jianqiao.Cheng@ulb.be

François Quitin
Brussels School of Engineering
Université Libre de Bruxelles (ULB)
Brussels, Belgium
Francois.Quitin@ulb.be

Abstract—Direction-of-Arrival (DoA) estimation of radio-frequency (RF) transmitters can be achieved using virtual multi-antenna arrays. The method relies on a mobile, single- or multi-antenna receiver that captures successive messages from a transmitter, thereby emulating a larger multi-antenna array. However, two main challenges emerge from this technique: 1) Successive positions and orientations of antennas have to be determined, meeting spatial Nyquist criterion; 2) the local oscillator (LO) frequency offset between transmitter and receiver adds a drifting phase component to the received signal on each antenna of the array. In this paper, we focus on the observability analysis of a dual-antenna system i.e. the ability to resolving the direction-of-arrival (DoA) of a RF transmitter based on received data with a moving dual-antenna system. We study the impact of the LO frequency drift on DoA estimation, provide limiting scenarios when observability could be lost and how dual-antenna systems provide solution where single-antenna system cannot.

Index Terms—Direction of arrival, Observability, Virtual Multi-antenna array, RF transmitter localization.

I. INTRODUCTION

Localization of transmitters and receivers using radio frequencies (RF) is a key element in wireless communication [1], [2]. In this context, direction-of-arrival (DoA) can be used as metric to deduce a transmitter's location. This can be achieved through triangulation if multiple anchor nodes perform DoA estimation [3]. Previous papers have investigated the concept of *virtual* antenna arrays and how this can replace classical multi-antenna arrays [4] [5].

As a starting point, single antenna systems have been considered, showing limitations and performances achievable with current mobile smartphones. In [4], the performance of single-antenna system in DoA estimation was shown with semi-circular trajectories. It also presented the compromising Stop-and-Start (SaS) approach used to remove the contribution of constant local oscillator (LO) frequency offset in the drifting phase before AoA estimation.

Paper [6] addressed the problem of observability for a single-antenna system with constant LO frequency offset. It has shown that DoA could not be retrieved when the receiver performs a uniform linear movement. This constitute a significant restriction in our estimation algorithm for such common trajectories. The research was then extended in [5] to dual-antenna systems and proved the benefits of adding a second antenna on such device for localization purposes.

In this paper, results of the observability analysis of a single-antenna system from [6] are extended to dual-antenna systems. This will allow to also consider lower-quality LOs, whose LO frequency offset suffer from a linear drift. The contributions of this paper are the following:

- Identify system configurations where the DoA is not observable, both for single- and dual-antenna systems.
- Determine if the dual-antenna system can make a system observable when a single-antenna system cannot.
- Provide simulation results that highlight the (non-)observability of single- and dual-antenna systems.

Section II will define the mathematical background required to perform an observability analysis. We will then illustrate cases where some of the states can become hidden in a measured signal and thus become indistinguishable. Some of these scenarios will be simulated in Section III in order to confirm our theoretical results. Finally, Section IV draws conclusions on both systems in terms of observability.

II. OBSERVABILITY ANALYSIS

A. Concept of observability

Control system formalism describes the evolution of physical systems by a set of differential equations [7]. The model dynamics may have different levels of complexity from e.g. non-linearities, noise, time-variance, etc. The state of a noiseless system is supposed to be entirely determined by its state variables which can be identified using measured data [8]. This raises the notion of observability. It describes the ability to infer states from measured signals [9] [10]. In a DoA estimation system, this amounts to determine if the system provides all necessary information to perform DoA estimation.

B. Case 1 : SISO with constant LO frequency offset

Without loss of generality, let us consider a single-antenna 'A' moving in a 2D space along x-direction as shown in Figure (1). It receives successive packets from the transmitter at different time instants. Without loss of generality, we assume the transmitter sends packets at regular time intervals with period T_0 .

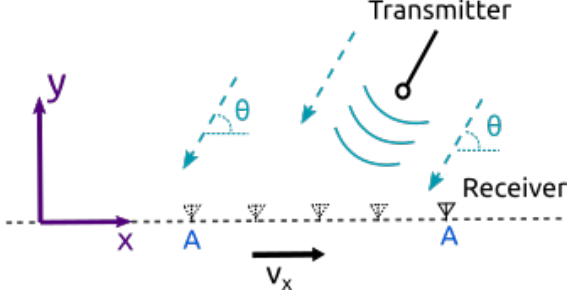


Fig. 1. Single-antenna moving in a x-y plane at constant speed (Case 1).

The phase of the received packets will then change during motion following the following discrete-time expression:

$$\phi_{k+1}^A = \phi_k + 2\pi \left(f_{0,k} + \frac{\cos(\theta_k)}{\lambda} v_{x,k} \right) T_0 + \frac{2\pi}{\lambda} \cos(\theta_k) \frac{a_{x,k}}{2} T_0^2 \quad (1)$$

where $k = 1, 2, \dots, N$ denotes the index of received packet (N in total), T_0 is the transmitting period, f_0 is the LO frequency offset between the transmitter and the receiver and θ is the azimuth angle-of-arrival (AoA). Two contributions can be distinguished, from frequency offset and motion. The expression immediately shows that both speed v_x and f_0 induce a linear drift on received phase while acceleration a_x has a quadratic contribution.

Observability analyses can be performed on nonlinear systems such as those in control affine forms [10]:

$$\sum_{NL,a} : \begin{cases} \dot{x}(t) = \sum_{i=1}^r f_i[x(t)] u_i \\ y(t) = h[x(t)] \end{cases} \quad (2)$$

If we consider that the LO frequency offset in 1 is constant, the following continuous-time system is obtained:

$$\begin{cases} \dot{\phi}^A(\mathbf{x}) = \frac{2\pi}{\lambda} v_x \cos(\theta) + 2\pi f_0 := \dot{\mathbf{x}}_1 \\ \dot{f}_0(\mathbf{x}) = 0 := \dot{\mathbf{x}}_2 \\ \dot{\theta}(\mathbf{x}) = 0 := \dot{\mathbf{x}}_3 \\ \dot{x}(\mathbf{x}) = v_x := \dot{\mathbf{x}}_4 \\ \dot{v}_x(\mathbf{x}) = a_x := \dot{\mathbf{x}}_5 \\ \dot{a}_x(\mathbf{x}) = 0 := \dot{\mathbf{x}}_6 \end{cases} \quad (3)$$

$$\begin{cases} h_1(\mathbf{x}) = \phi^A \\ h_2(\mathbf{x}) = x \end{cases}$$

where h_1 and h_2 denote measured quantities, namely ϕ^A and x (we assume here that the receiver is able to estimate the phase of the received signal ϕ^A and its relative position x). The observability analysis can be performed using the nonlinear observability matrix \mathcal{O} which is computed based on Lie derivatives of measured data [10].

The 0th- order Lie derivative of the measurement function is the function itself:

$$\begin{cases} \mathcal{L}_f^0 h_1(x) = h_1(x) = \mathbf{x}_1 \\ \mathcal{L}_f^0 h_2(x) = h_2(x) = \mathbf{x}_4 \end{cases} \quad (4)$$

The 1st- order Lie derivative of the measurement function with respect to f_i is defined as

$$\begin{cases} \mathcal{L}_f^1 h_1(x) = \sum_{i=1}^{n=6} \frac{\partial h_1(x)}{\partial \mathbf{x}_i} \cdot f_i(x) = 2\pi \left(\mathbf{x}_2 + \frac{\cos(\mathbf{x}_3)}{\lambda} \mathbf{x}_5 \right) \\ \mathcal{L}_f^1 h_2(x) = \sum_{i=1}^{n=6} \frac{\partial h_2(x)}{\partial \mathbf{x}_i} \cdot f_i(x) = \mathbf{x}_5 \end{cases} \quad (5)$$

Lie derivatives capture orthogonality between system vector field (3) and gradient of measured signals. Higher order Lie derivatives are computed by accumulating first-order derivatives. The next step is to construct the G matrix by stacking the Lie derivatives until the $(n-1)$ -th order:

$$G \triangleq \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_4 \\ \mathbf{x}_2 + 2\pi \left(\mathbf{x}_2 + \frac{\cos(\mathbf{x}_3)}{\lambda} \mathbf{x}_5 \right) \\ \mathbf{x}_5 \\ 2\pi \frac{\cos(\mathbf{x}_3)}{\lambda} \mathbf{x}_6 \\ \mathbf{x}_6 \\ O_{6 \times 1} \end{bmatrix} \quad (6)$$

Finally, we compute the gradient of G to obtain the nonlinear observability matrix \mathcal{O} :

$$\mathcal{O}_{NL_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2\pi & -2\pi \frac{\sin(\mathbf{x}_3)}{\lambda} \mathbf{x}_5 & 0 & 2\pi \frac{\cos(\mathbf{x}_3)}{\lambda} & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -2\pi \frac{\sin(\mathbf{x}_3)}{\lambda} \mathbf{x}_6 & 0 & 0 & 2\pi \frac{\cos(\mathbf{x}_3)}{\lambda} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{O_{6 \times 6}}$$

More specifically, the system is locally weakly observable if \mathcal{O} is full-rank. Here, \mathcal{O}_{NL_1} is full-rank and $\det(\mathcal{O}_{NL_1}) = -4\pi^2 \frac{\sin(\mathbf{x}_3)}{\lambda} \mathbf{x}_6$. It shows observability loss only when $a_x = 0$. This result can also be observed from equation (1) where f_0 and θ are confounded in the linear term, meaning that θ cannot be recovered from ϕ^A measurement when $a_x = 0$. This will be illustrated in Section III.

C. Case 2 : SISO with linear LO frequency drift

The previous case is extended by assuming a linear drift of the LO frequency offset over time i.e. $f_0 = \beta_0 + \beta_1 t$ with $\beta_0, \beta_1 \in \mathbb{R}$. In discrete-time, the expression becomes $f_{0,k+1} = f_{0,k} + \dot{f}_{0,k} T_0$ and the system can be derived as follows:

$$\begin{cases}
\phi_{k+1}^A = \phi_k + 2\pi \left(f_{0,k} + \frac{\cos(\theta_k)}{\lambda} v_{x,k} \right) T_0 \\
\quad + 2\pi \left(\frac{\dot{f}_{0,k}}{2} + \frac{\cos(\theta_k)}{\lambda} \frac{a_{x,k}}{2} \right) T_0^2 \\
f_{0,k+1} = f_{0,k} + \dot{f}_{0,k} T_0 \\
\dot{f}_{0,k+1} = \dot{f}_{0,k} = \beta_1 \\
\theta_{k+1} = \theta_k \\
x_{k+1} = x_k + \dot{x}_k T_0 + \frac{\ddot{x}_k}{2} T_0^2 \\
\dot{x}_{k+1} = \dot{x}_k + \ddot{x}_k T_0 \\
\ddot{x}_{k+1} = \ddot{x}_k
\end{cases} \quad (7)$$

with $\beta_1 \in \mathbb{R}$. Only one additional state has been added. In this case, the LO frequency offset also has a quadratic contribution on ϕ^A . The state-space model in time domain is then easily derived:

$$\begin{cases}
\dot{\phi}^A(\mathbf{x}) = \frac{2\pi}{\lambda} v_x \cos(\theta) + 2\pi f_0 := \dot{\mathbf{x}}_1 \\
\dot{f}_0(\mathbf{x}) = \beta_1 := \dot{\mathbf{x}}_2 \\
\ddot{f}_0(\mathbf{x}) = 0 := \dot{\mathbf{x}}_3 \\
\dot{\theta}(\mathbf{x}) = 0 := \dot{\mathbf{x}}_4 \\
\dot{x}(\mathbf{x}) = v_x := \dot{\mathbf{x}}_5 \\
\dot{v}_x(\mathbf{x}) = a_x := \dot{\mathbf{x}}_6 \\
\dot{a}_x(\mathbf{x}) = 0 := \dot{\mathbf{x}}_7
\end{cases} \quad (8)$$

$$\begin{cases}
h_1(\mathbf{x}) = \phi^A \\
h_2(\mathbf{x}) = x
\end{cases}$$

The previous equation again assumes that the receiver is able to estimate the phase of the received packets ϕ^A and it's relative position x . By applying identical rules as in previous case, we obtain the following observability matrix:

$$\mathcal{O}_{NL_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2\pi & 0 & -2\pi \frac{\sin(\mathbf{x}_4)}{\lambda} \mathbf{x}_6 & 0 & 2\pi \frac{\cos(\mathbf{x}_4)}{\lambda} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2\pi & -2\pi \frac{\sin(\mathbf{x}_4)}{\lambda} \mathbf{x}_7 & 0 & 0 & 2\pi \frac{\cos(\mathbf{x}_4)}{\lambda} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad O_{8 \times 7}$$

In this case, the system is no longer observable since $\text{rank}(\mathcal{O}_{NL_2}) = 6$. The rank deficiency of \mathcal{O}_{NL_2} is equal to the dimension of the nullspace \mathcal{NO} whose basis vectors indicate the non-observable states [11] [12]. More precisely, non-zero components in vectors correspond to states that spans the non-observable subspace. In this case, it provides only one basis vector q_1 :

$$q_1 = \begin{bmatrix} 0 & \frac{\sin(\mathbf{x}_4)}{\lambda} \mathbf{x}_6 & \frac{\sin(\mathbf{x}_4)}{\lambda} \mathbf{x}_7 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (9)$$

It means that \mathbf{x}_2 , \mathbf{x}_3 and \mathbf{x}_4 (f_0, \dot{f}_0, θ) lie within the non-observable subspace i.e. these states are hidden together in the measured signals and are therefore non-observable. To support this result, let us consider 2 different scenarios with the same dynamics i.e. identical x , v_x and a_x but different AoA and frequency offset profile i.e. θ and f_0 , as shown in Figure 2.

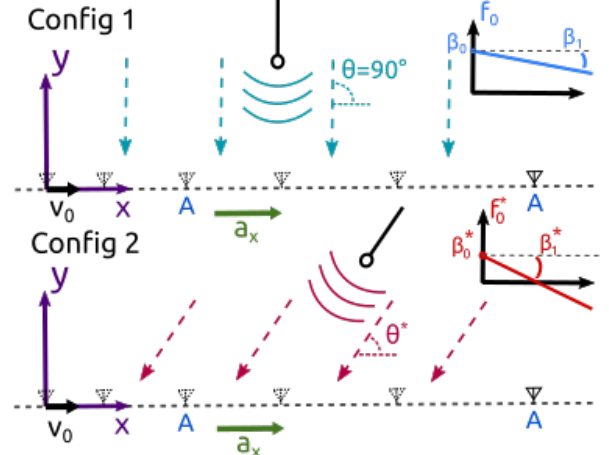


Fig. 2. Two configurations $(\beta_0, \beta_1, \theta)$ and $(\beta_0^*, \beta_1^*, \theta^*)$ providing the same phase on received packets (Case 2).

Both state configurations differ from each other. The first configuration has a frequency offset and AoA of (f_0, θ) , and the second configuration has a frequency offset and AoA of (f_0^*, θ^*) . The goal is to identify if those two different scenarios can provide exactly the same measured signals ϕ^A and x , in which case it would be impossible to distinguish them. Since both receivers have the same dynamics (i.e. the same x), this amounts to only match up both phase profiles. By considering $\theta = 90^\circ$ in the first configuration and using first equation in (7), we get:

$$\begin{aligned}
\phi_k^A + 2\pi f_{0,k} T_0 + 2\pi \frac{\dot{f}_{0,k}}{2} T_0^2 &= \phi_k^A \\
+ 2\pi \left(f_{0,k}^* + \frac{\cos(\theta^*)}{\lambda} \dot{x}_k \right) T_0 + 2\pi \left(\frac{\dot{f}_{0,k}^*}{2} + \frac{\cos(\theta^*)}{\lambda} \frac{\ddot{x}_k}{2} \right) T_0^2 &= \phi_k^A
\end{aligned} \quad (10)$$

It is sufficient to identify each term of the polynomials:

$$\begin{cases} f_{0,k} &= f_{0,k}^* + \frac{\cos(\theta^*)}{\lambda} \dot{x}_k \\ \dot{f}_{0,k} &= \dot{f}_{0,k}^* + \frac{\cos(\theta^*)}{\lambda} \ddot{x}_k \end{cases} \quad (11)$$

By injecting velocity and acceleration profile from (7), we end up with only 2 linearly independent equations:

$$\begin{cases} \beta_0^* &= \beta_0 - \frac{\cos(\theta^*)}{\lambda} \dot{x}_0 \\ \beta_1^* &= \beta_1 - \frac{\cos(\theta^*)}{\lambda} \ddot{x}_0 \end{cases} \quad (12)$$

containing 3 unknowns $(\beta_0^*, \beta_1^*, \theta^*)$. It is obvious that this set of equations is rank-deficient, implying an infinite number of solutions. It means that for a given value θ^* , there is

a corresponding profile of f_0^* providing the same phase on the received packets over time. All of the above confirm the non-observability of the azimuth angle-of-arrival, an important limitation of such common scenario with single-antenna systems. One solution would be to use the Stop-and-Start (SaS) approach presented in previous papers, which estimates the LO frequency offset at standstill, and then compensates the LO frequency offset during receiver movement. This method has proven to be successful, but it is quite restrictive since it involves stopping the receiver for a few seconds. In the following, we present a solution using virtual antenna arrays based on dual-antenna systems, and show that this system yields a fully-observable problem.

D. Case 3 : MIMO with constant LO frequency offset

A second antenna 'B' is attached to antenna 'A' with a relative distance d . The system travels a straight line with a constant acceleration as shown in Figure 3.

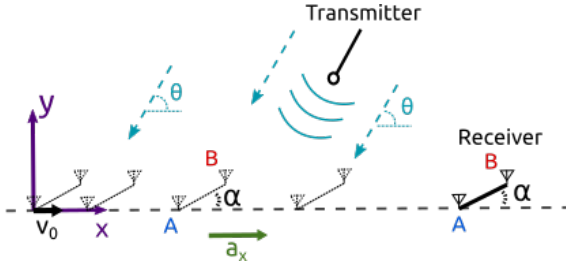


Fig. 3. Dual-antenna moving in a x-y plane (Case 3 and 4).

The state-space model can be written as:

$$\begin{cases} \dot{\phi}^A(\mathbf{x}) = \frac{2\pi}{\lambda} v_x \cos(\theta) + 2\pi f_0 \\ \dot{f}_0(\mathbf{x}) = 0 \\ \dot{\theta}(\mathbf{x}) = 0 \\ \dot{x}(\mathbf{x}) = v_x \\ \dot{v}_x(\mathbf{x}) = a_x \\ \dot{a}_x(\mathbf{x}) = 0 \\ \dot{\alpha}(\mathbf{x}) = 0 \end{cases} \quad (13)$$

$$\begin{cases} h_1(\mathbf{x}) = \phi^A \\ h_2(\mathbf{x}) = \phi^B = \phi^A - \frac{2\pi d}{\lambda} \cos(\theta - \alpha) \\ h_3(\mathbf{x}) = x \\ h_4(\mathbf{x}) = \alpha \end{cases}$$

Two additional variables are measured in this scenario i.e. ϕ^B , the phase of packets received by antenna B and α , the angle w.r.t the x-direction. The computed observability matrix \mathcal{O}_{NL_3} is full rank here. Ambiguity on the solution has been removed by introduction of antenna B. In fact, the true AoA can directly be retrieved by combining measured signals h_1 ,

h_2 and h_4 in system (13). From there, it is possible to compute the last unknown state f_0 using the first state equation.

E. Case 4 : MIMO with linear LO frequency drift

The final case is for a MIMO receiver with a drifting LO frequency offset. In this case, the state-space model can be written as:

$$\begin{cases} \dot{\phi}^A(\mathbf{x}) = \frac{2\pi}{\lambda} v_x \cos(\theta) + 2\pi f_0 \\ \dot{f}_0(\mathbf{x}) = \beta_1 \\ \ddot{f}_0(\mathbf{x}) = 0 \\ \dot{\theta}(\mathbf{x}) = 0 \\ \dot{x}(\mathbf{x}) = v_x \\ \dot{v}_x(\mathbf{x}) = a_x \\ \dot{a}_x(\mathbf{x}) = 0 \\ \dot{\alpha}(\mathbf{x}) = 0 \end{cases} \quad (14)$$

In this final general case, the system is also fully observable. Since knowledge of α implies the knowledge of θ , rank of system (12) becomes equal to space dimension and the solution becomes unique. This important feature could also be seen in reverse, i.e. orientation of the dual-antenna can be retrieved based on the DoA measurement which means that a full localization of the receiver is achievable with this system (position and orientation).

III. SIMULATIONS

Several simulations have been performed to verify previous theoretical results i.e.

- Case 1 : Single antenna with constant LO frequency at constant speed.
- Case 4 : Dual antenna, with drifting LO frequency at constant acceleration.

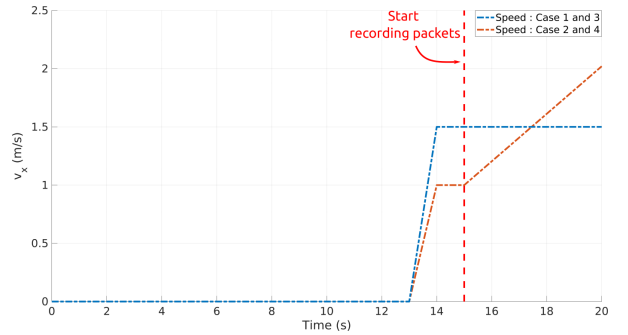


Fig. 4. Speed profiles among different considered cases. Recording of packets starts at $t = 15$ s.

In all cases, we simulated a straight line trajectory of $\simeq 7.5$ m traveled within 5 s. Packets have been recorded at a period of $T_0 = 1$ ms during 10 s. Parameters for the LO frequency offset have been set to $\beta_0 = 50$ Hz and $\beta_1 = -2.5$ 1/s² to be in the range of measured drift on *USRP E312* SDRs in our lab. The AoA has been set to $\theta = 90^\circ$

Distance between two antennas has been set to half a wavelength with $\lambda = 0.15$ m. We considered perfectly known IMU data, with $T_{imu} = 1$ ms as sampling time such that to each received packet corresponds a position of the antenna. Carrier frequency has been set to 2 GHz and sampling frequency to $f_s = 614.4$ kHz. The MUSIC algorithm has been applied to received packets to jointly estimate the azimuth angle and the LO frequency offset.

The MUSIC spectrum for Case 1 is shown in Figure 5, in the f_0 - θ plane. It can be seen that we have an infinity of solutions spanning the f_0 - θ plane, indicating that the system is indeed non-observable when the acceleration $a_x = 0$.

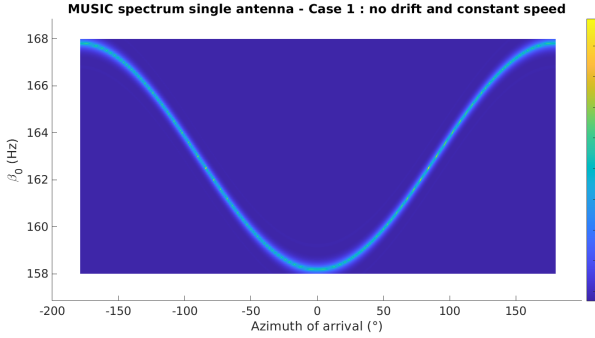


Fig. 5. MUSIC spectrum - Case 1 : single-antenna straight-line trajectory with constant $f_0 = 50$ Hz and speed $v_x = 1.5$ m/s.

Several slices of the MUSIC spectrum for Case 4 are shown in Figure 6. The slices shown correspond to values that fulfill equation (12). The peak corresponding to the correct AoA is significantly higher than the other peaks, showing that the system is indeed observable.

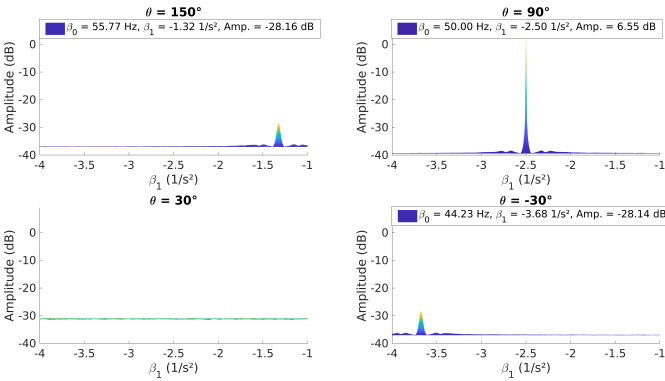


Fig. 6. MUSIC spectra - Case 4 : dual-antenna straight-line trajectory with linear drifting f_0 and linear speed ($v_0 = 1$ m/s, $a_x = 0.204$ m/s²)

IV. CONCLUSION

This paper presents how dual-antenna receiver can solve limitations we face with single-antenna system in the purpose of DoA estimation when using local oscillator that have drifting LO offset. Table I resumes improvements with dual-antenna in terms of observability.

TABLE I
RESULTS OF OBSERVABILITY ANALYSIS

	List of non-observable states	
	$f_0 = \beta_0$ (no drift)	$f_0 = \beta_0 + \beta_1 t$ (drift)
Single-antenna	θ if $a_x = 0$	θ
Dual-Antenna	-	-

It shows that dual-antenna performs better, reaching uniqueness of the AoA solution thanks to the second antenna. In fact, the system is always locally observable without any restriction on the dynamics or profile of the LO frequency offset. Moreover, since the AoA can immediately be retrieved from the orientation in dual-antenna system, knowledge of the AoA can also provide the orientation if the latter becomes unknown. It would allow us to fully localize the dual-antenna array i.e. the position and orientation, allowing for full 6D-localization.

REFERENCES

- [1] Klaus Witrisal and Carles Antón-Haro, "Whitepaper on New Localization Methods for 5G Wireless Systems and the Internet-of-Things," Tech. Rep., COST Action CA15104 - IRACON, 2018.
- [2] Claude Oestges and François Quitin, *Inclusive Radio Communications for 5G and Beyond*, Elsevier, 2021.
- [3] Kutluyil Doğançay, "Bearings-only target localization using total least squares," *Signal Processing*, vol. 85, no. 9, pp. 1695–1710, 2005.
- [4] François Quitin, Philippe De Doncker, François Horlin, and Wee Peng Tay, "Virtual multiantenna array for estimating the direction of a transmitter: System, bounds, and experimental results," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1510–1520, 2018.
- [5] Youssef Agram, Jianqiao Cheng, and François Quitin, "Direction-of-arrival estimation with virtual multi-antenna arrays using dual-antenna receivers : algorithms and controlled experiments,," 2022.
- [6] Jianqiao Cheng, Ke Guan, and François Quitin, "Direction-of-arrival estimation with virtual antenna array: Observability analysis, local oscillator frequency offset compensation, and experimental results," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–13, 2021.
- [7] G. P. Huang, N. Trawny, A. I. Mourikis, and S. I. Roumeliotis, "Observability-based consistent ekf estimators for multi-robot cooperative localization," *Autonomous Robots*, vol. 30, pp. 99–122, 2011.
- [8] Alejandro F. Villaverde, Nikolaos Tsiantis, and Julio R. Banga, "Journal of the Royal Society Interface," vol. 16, 2019.
- [9] R. Hermann and A. Krener, "Nonlinear controllability and observability," *IEEE Transactions on automatic control*, vol. 22(5), pp. 728–740, 1977.
- [10] Z. M. Kassas and T. E. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15(1), pp. 260–273, 2013.
- [11] J. A. Hesck, D. G. Kottas, S. L. Bowman, and S. I. Roumeliotis, "Camera-imu-based localization: Observability analysis and consistency improvement," *The International Journal of Robotics Research*, vol. 33(1), pp. 182–201, 2014.
- [12] J. Jackson, J. Nielsen, T. McLain, and R. Beard, "Improving the robustness of visual-inertial extended kalman filtering," *International Conference on Robotics and Automation, IEEE*, pp. 4703–4709, 2019.

Unsupervised neural decoding of auditory attention using a Binary Quadratic Program

1st Nicolas Heintz

Dept. of Electrical Engineering, STADIUS
Dept. of Neurosciences, ExpORL
KU Leuven
Leuven, Belgium
nicolas.heintz@esat.kuleuven.be

2nd Tom Francart

Dept. of Neurosciences, ExpORL
KU Leuven
Leuven, Belgium
tom.francart@kuleuven.be

3rd Alexander Bertrand

Dept. of Electrical Engineering, STADIUS
KU Leuven
Leuven, Belgium
alexander.bertrand@esat.kuleuven.be

Abstract—Auditory attention decoding algorithms attempt to decode from brain signals to whom a person is listening, for example using electroencephalography (EEG) recordings. These algorithms are typically first trained in a supervised environment for optimal performance [1], [2]. However, such supervised training sessions are cumbersome and undesired in practice, as they require a lot of time from the end user and they can sometimes deliver incorrect ground truth labels [3]. Furthermore, once the decoder is trained during such a supervised session, it is fixed and its performance starts to drop over time due to changes in brain responses, electrode impedances or listening environments [4].

There is therefore a need for unsupervised training and classification of auditory attention. State-of-the-art unsupervised algorithms iteratively retrain a least-squares regression model that reconstructs the attended speech from EEG signals. The iterative procedure contains a feedback process in which the classification decisions of the decoder obtained in the previous iteration are used as labels to train a new decoder in the current iteration [4], [5]. We show that an instantaneous instance of this iterative feedback procedure can be used to reformulate the attention decoding problem into a so-called Binary Quadratic Program (BQP). The aforementioned iterative procedure leads to solutions of this BQP that are biased by the initialisation and converge to a local optimum.

However, by reformulating the unsupervised auditory attention problem as a BQP, we can compare the iterative algorithm to other BQP solvers, such as the heuristic diversification-driven tabu search algorithm [6] and a globally optimal branch-and-bound algorithm from CPLEX [7]. Both algorithms significantly outperform the iterative algorithm, while we find no significant difference between the tabu search and the more expensive branch-and-bound algorithm.

REFERENCES

- [1] J. A. O’Sullivan, A. J. Power, N. Mesgarani, S. Rajaram, J. J. Foxe, B. G. Shinn-Cunningham, M. Slaney, S. A. Shamma, and E. C. Lalor, “Attentional Selection in a Cocktail Party Environment Can Be Decoded from Single-Trial EEG,” *Cerebral Cortex*, vol. 25, no. 7, pp. 1697–1706, 2015.
- [2] S. Geirnaert, S. Vandecappelle, E. Alickovic, A. de Cheveigné, E. Lalor, B. T. Meyer, S. Miran, T. Francart, and A. Bertrand, “Neuro-Steered Hearing Devices: Decoding Auditory Attention From the Brain,” *IEEE Signal Processing Magazine*, vol. 38, pp. 89–102, 8 2021.
- [3] A. de Cheveigné, D. E. Wong, G. M. Di Liberto, J. Hjortkjær, M. Slaney, and E. Lalor, “Decoding the auditory brain with canonical component analysis,” *NeuroImage*, vol. 172, pp. 206–216, 2018.
- [4] S. Geirnaert, T. Francart, and A. Bertrand, “Time-adaptive Unsupervised Auditory Attention Decoding Using EEG-based Stimulus Reconstruction,” *bioRxiv*, p. 2022.01.07.475386, 3 2022.
- [5] S. Geirnaert, T. Francart, and A. Bertrand, “Unsupervised Self-Adaptive Auditory Attention Decoding,” *IEEE Journal of Biomedical and Health Informatics*, pp. 1–1, 2021.
- [6] F. Glover, Z. Lü, J.-K. Hao, F. Glover, Z. Lü, and J.-K. Hao, “Diversification-driven tabu search for unconstrained binary quadratic problems,” *4OR*, vol. 8, pp. 239–253, 1 2010.
- [7] C. Blik, P. Bonami, and A. Lodi, “Solving Mixed-Integer Quadratic Programming problems with IBM-CPLEX: a progress report,” in *Proceedings of the Twenty-Sixth RAMP Symposium*, (Tokyo), 2014.

This research is funded by Aspirant Grant 1S31522N from the Research Foundation - Flanders (FWO) (for N. Heintz), the Research Foundation - Flanders (FWO) project nr. G0A4918N, the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement No 802895 and grant agreement No 637424), and the Flemish Government (AI Research Program). The scientific responsibility is assumed by its authors.

N. Heintz and A. Bertrand are also affiliated with Leuven.AI - KU Leuven institute for AI, Belgium.

Unraveling Finger Veins: An Improvement to Unsupervised Finger Vein Recognition with a Convolutional Autoencoder

Tugce Arican
DMB, EEMCS
University of Twente
Enschede, The Netherlands
t.arican@utwente.nl

Raymond Veldhuis
DMB, EEMCS
University of Twente
Enschede, The Netherlands
r.n.j.veldhuis@utwente.nl

Luuk Spreeuwiers
DMB, EEMCS
University of Twente
Enschede, The Netherlands
l.j.spreeuwiers@utwente.nl

Abstract—A Convolutional Auto Encoder(CAE) is capable of learning data representations without using label information which comes handy where it is hard to realise the label information for large amount of data such as finger veins. However, veins are fine structures such that they are not well reconstructed by CAEs. In this work, a simple image enhancement step and a dual-decoder convolutional auto encoder model are introduced to assist a CAE in learning fine vein structures. The Equal Error Rate of 1.38% achieved on UTFVP dataset indicates the potential of the unsupervised approaches on finger vein recognition.

I. INTRODUCTION

Finger vein patterns are random structures appear under the skin, which carry identity information to identify individuals. Finger vein recognition is performed by comparing two finger vein representations. This representation can be achieved in several ways. One way to extract finger vein representations is to directly extracting vein patterns from an image. Maximum curvatures[4] and repeated line tracking[3] achieve robust vein extraction results. Deep learning methods become popular for finger vein recognition because of their generalisation abilities and robustness against illumination differences and translations. Researchers [5], [6], [8], [16] achieve state-of-the-art recognition results on publicly available finger vein datasets.

Vein patterns are captured under infrared light, which makes difficult to collect large amount of finger vein data. Due to lack of large finger vein datasets, researchers commonly prefer pre-trained models for finger vein recognition. Hu et.al[10] utilise a pre-trained VGG-16 model for finger vein recognition. Evaluation results on a publicly available dataset indicate the competitiveness of pre-trained models over classical methods. Song et.al.[6] compare the performances of pre-trained VGG-16 and ResNet-161 model for finger vein recognition. Authors indicate that ResNet-161 model is superior over VGG-16 on publicly available finger vein datasets. Tang et.al.[5] utilise shallow layers of a pre-trained ResNet-50 model and train additional convolution and fully connected layers on top of it. Authors achieve state-of-the-art performance on some publicly available finger vein datasets. Even though pre-trained

models achieve state-of-the-art performance on finger vein recognition, finger vein images are less complex compared to the dataset used to train those models. It is likely that the feature space of a pre-trained model involves redundancy for finger vein recognition task, which would likely to lead erroneous finger vein matching.

Unsupervised learning methods do not need label information in order to learn data representations, which comes handy when it is difficult to realise the label information for large amount of data like finger veins. In this work, Convolutional Auto Encoders(CAEs) are selected as the unsupervised learning method. The aim of a CAE is to reconstruct its input through a compression and de-compression operations. During these operations, CAE learns a representation of the input, which can be used to compare finger vein images. However, previous work[1] indicates that the vein structures are lost during reconstruction, while CAE reconstructs the global structures such as finger joints and illumination patterns successfully. The vein patterns have low contrast with the finger background, and they are sparse patterns. In this work, an image enhancement method and a dual-decoding approach are proposed in order to improve the vein contrast and the vein contribution on CAE training, so that vein patterns are well encoded in the latent vector in addition to the global structures.

II. RELATED WORK

Auto encoders learn input representations which could be used in a recognition task. Yang et al.[12] show that the representations learned by a de-noising convolutional auto encoder are superior over PCA, and CNN on facial emotion recognition. Bhaswara[13] investigate different type of auto encoder models, including generative models, on extracting facial features for a recognition task. The results of this work indicate that auto encoders are able to extract powerful features, while the generative models provide a better generalisation of the facial features compared to a regular AE. AEs can also be used to initialise classifier networks when the amount of available training data is limited. Silva et.al.[14] utilise a CAE as pre-training of a classification

network. In this work, first a CAE is trained to learn lung tumor representations. Later, the encoder part is transferred as a pre-training model, and a classifier layer is trained on top of it. The results indicate that CAE as a pre-training step could come handy where it is difficult to achieve large amount of labeled training data. There are few work implementing an auto encoder for finger vein recognition. Hou et.al.[9] propose a shallow CAE model in order to extract finger vein features. Later, those features are classified by a CNN model. Proposed CAE + CNN approach outperforms classical approaches on finger vein recognition. Later, the same authors proposed a deeper CAE model[8] which outperforms their previous work. Even though those works indicate the applicability of CAEs on finger vein recognition, performance of the CAEs are not compared against training based methods.

Even though there is literature showing that AEs can learn data representations successfully, they tend to loose fine details in the input data. Ghodrati et.al.[15] compare several loss functions, such as Mean Square Error(MSE), Mean Absolute Error(MAE), structural dissimilarity(DSSIM), and perceptual loss, on MR image reconstruction. Authors achieve the best reconstruction results with perceptual loss, while indicating that MSE and MAE loss functions fail to reconstruct fine textural information in the MR images. Ichimura[17] also shows that high frequency details, like edges, are not well reconstructed with pixel-based loss functions, such as MSE. Author proposes a spatial frequency loss(SFL) component in addition to MSE loss. The results indicate that the SFL component is successfully recovered the high frequency information which is lost with MSE. Previous work[1] implements a spatial frequency loss component in order to reconstruct fine vein details with a CAE. However, in this work, spatial frequency loss is not successful at reconstructing fine vein details. Yet, the authors show that global structures of a finger vein image, such as joint shapes and bone structures, contribute to identity information.

III. METHODOLOGY

A. Finger Vein Image Enhancement

Finger vein patterns appear as dark lines under infrared illumination, where the surrounding tissues, such as muscles, finger joints, and bones, are observed as bright regions(Fig.1). Vein patterns are generally sparse and have a low contrast with the surrounding tissues. Due to the low contrast and sparsity, vein patterns are not well reconstructed by an auto encoder, which indicates the vein patterns are also not well encoded on the latent vector.

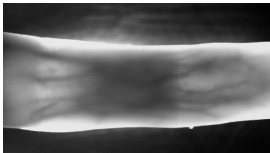


Fig. 1: Finger vein image captured under infrared light

In this work, a vein enhancement method is proposed in order to improve the contrast of vein patterns, so that the auto encoder properly learn vein representations. Figure 2 shows the enhancement steps. First, the negative of a finger vein image is taken in order to highlight the vein patterns, then this negative image is passed through a blurring filter to remove as much vein patterns as possible, so that the difference of the negative and the blurred images highlights the vein patterns. Later, the vein enhancement is completed by subtracting this difference image from the input finger vein image. Beside the vein enhancement, pixels above a threshold in the difference image is zeroed out resulting with a vein image. Later, this vein image is utilised by the dual-decoder architecture.

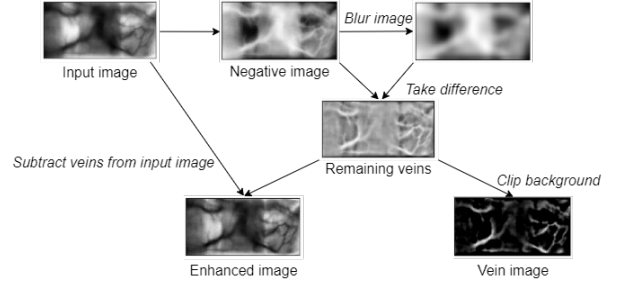


Fig. 2: Finger vein enhancement steps

B. Dual-Decoder Convolutional Auto Encoder

Veins are sparse patterns and they are dominated by bigger structures, such as finger joints and bone structures. Previous work[1] claims that those bigger structures are well reconstructed by an auto encoder, while the vein patterns are severely lost during reconstruction. Beside this finding, the authors conclude that those bigger structures contributes to identity information. Hence, it is important to utilise both the vein and the finger background information together.

In this work, a dual-decoder convolutional auto encoder(DDCAE) architecture is proposed in order to learn the vein patterns and the other aforementioned structures simultaneously. The proposed architecture(Fig.3) consists of one encoder and two identical decoders. One encoder-decoder path reconstructs the finger vein image including finger background, while the second one aims to reconstruct only the vein patterns obtained at the enhancement stage. The decoders share the same latent vector in order to force the encoder part to learn both finger background and the vein features simultaneously.

Loss function of DDCAE combines the errors on finger vein images and vein images(Eq.1). Mean Absolute Error(MAE) loss is preferred while reconstructing the finger vein images with background, while Binary Cross Entropy(BCE) loss is utilised for vein pattern reconstruction. A hyper-parameter called α controls the contribution of the finger vein image and the vein patterns to training. The higher the α value, the higher the contribution of the vein patterns.

$$L = (1 - \alpha) * L1(inputimage, outputimage) + \alpha * BCE(inputveins, outputveins) \quad (1)$$

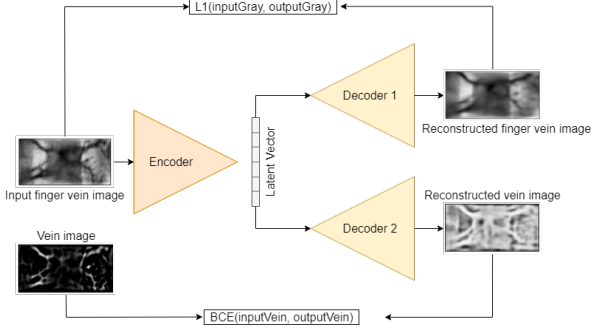


Fig. 3: Dual-Decoder Convolutional Auto Encoder

IV. EXPERIMENTS

A. Dataset

Proposed DDCAE is evaluated on a dataset provided by University of Twente(UTFVP)[2]. The dataset provides 1440 images from 60 subjects. For each subject index finger, middle finger, and ring finger of both hands are captured in 2 sessions. Region of interest(ROI) is extracted, and all ROI images are re-scaled to 128x256 pixels(Fig.4). Contrast Limited Adaptive Histogram Enhancement(CLAHE) is applied to enhance the contrast of the veins at first place. First 20 subjects of the dataset are used in training, while the remaining 40 subjects are utilised for evaluation.

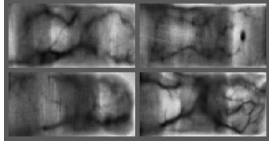


Fig. 4: Input ROI images

B. Dual-decoder CAE Architecture and Training

Tables I and II shows the encoder and decoder architectures, respectively. Encoder part involves 7 layers of convolution, batch normalisation, and ReLU activation function. Dimensionality reduction is performed by only strided convolutions. Output of the last layer of encoder is passed through a fully connected layer with an output dimension of 512, which is utilised as latent vector of the DDCAE.

Layer	Kernel size / Stride	Output shape (HxWxC)
conv(nk=16, BN, ReLU)	3x3 / 2	64x128x16
conv(nk=32, BN, ReLU)	3x3 / 2	32x64x32
conv(nk=64, BN, ReLU)	3x3 / 2	16x32x64
conv(nk=128, BN, ReLU)	3x3 / 2	8x16x128
conv(nk=256, BN, ReLU)	3x3 / 2	4x8x256
conv(nk=512, BN, ReLU)	3x3 / 2	2x4x512
conv(nk=1024, BN, ReLU)	3x3 / 2	1x2x1024
fully connected	2048	512

TABLE I: Encoder Architecture

Decoder networks are identical and the reversed version of the encoder. In decoder, convolution layers are replaced with transposed convolution layers.

Layer	Kernel size / Stride	Output shape (HxWxC)
convT(nk=512, BN, ReLU)	3x3 / 2	2x4x512
convT(nk=256, BN, ReLU)	3x3 / 2	4x8x256
convT(nk=128, BN, ReLU)	3x3 / 2	8x16x128
convT(nk=64, BN, ReLU)	3x3 / 2	16x32x64
convT(nk=32, BN, ReLU)	3x3 / 2	32x64x32
convT(nk=16, BN, ReLU)	3x3 / 2	64x128x16
convT(nk=16, BN, ReLU)	3x3 / 2	128x256x16
conv(nk=1, BN, ReLU)	1x1 / 1	128x256x1

TABLE II: Decoder Architecture

The model is trained with Adam optimiser with a learning rate of 2×10^{-4} for 100 epochs. Batch size is set to 16.

C. Evaluation Metrics

Evaluation is done both in terms of reconstruction and recognition. Accurate reconstruction of the input patterns indicate that those patterns are encoded well in the latent vector. Therefore, it is important for the DDCAE produces visually appealing reconstructions of the vein patterns as well as the finger background.

Recognition performance is measured by Area Under Curve(AUC) and Equal Error Rate(EER) metrics. AUC measures the separability of classes. The higher the AUC, the better the model decides the classes correctly. EER indicates the proportion of the false accepted instances is equal to false rejected instances. The lower EER, the better the model classifies instances correctly.

V. RESULTS

A. Reconstruction

Visually convincing reconstructions of vein patterns and the other structures indicate that those patterns present in the latent vector. Figure 5 compares the reconstruction results with varying values of the hyper-parameter α . It is observed that when vein images are included in training($\alpha > 0.0$), reconstructed images show more accurate vein patterns. More over, with the increasing values of α vein patterns become richer and more accurate in the reconstructed images.

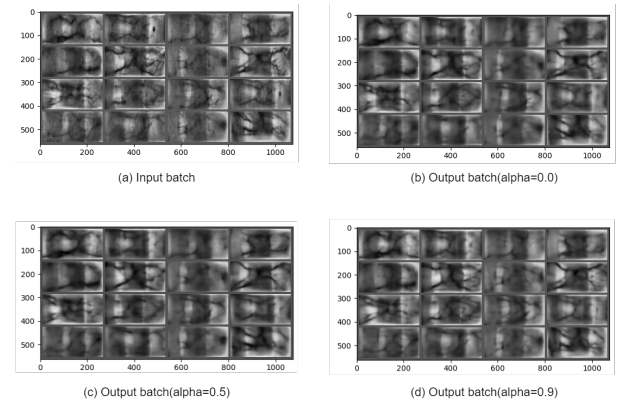


Fig. 5: Reconstruction results (a) Input batch, reconstructions (b) $\alpha=0.0$, (c) $\alpha=0.5$, (d) $\alpha=0.9$

Reconstruction results point out that double-decoder model assists reconstructing fine vein structures accurately by utilising the vein patterns as an additional source of information.

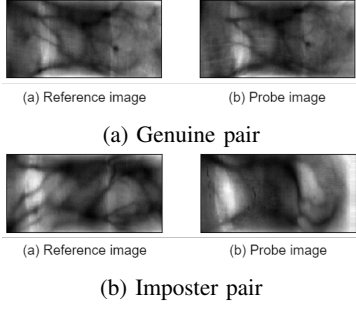


Fig. 6: Image pairs

B. Recognition

Recognition is performed by comparing the encoding of two finger vein images. In total, 720 genuine pair and 720 imposter pair are evaluated. Cosine similarity is utilised as a similarity metric of an image pair. Figure 6 shows samples of genuine and imposter pairs. DDCAE achieves 0.997 AUC and 1.39% EER with $\alpha=0.9$. Table III indicates that DDCAE outperforms the auto encoder approach proposed in the previous work. Yet, DDCAE performs approximately 3 times worse than maximum curvatures.

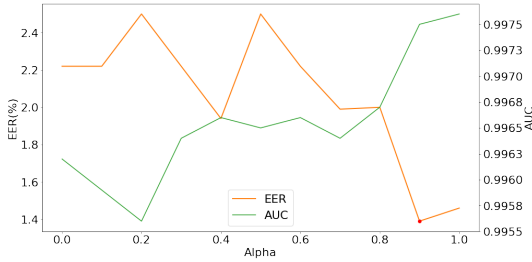


Fig. 7: Performance of DDAE with different α values

Figure 7 compares the performance of the model with different α values. Even though smaller α values does not affect the recognition performance, increasing values of α significantly improved the EER. Furthermore, image pair similarity histograms(Fig. 8) support this finding. Low α values do not change the image pair similarities much. However, it is observed that, when α is set to 0.9, imposter image pair similarities are significantly decreased. It is also observed that with a high α value, genuine image pair similarities are lower compared to a lower α value. This would indicate that the model encodes more vein structures, therefore it becomes more sensitive to changes in the vein patterns.

VI. DISCUSSION

This work investigates whether an auto encoder reconstructs fine structures like veins, so that the learned representation is

¹LLR classifier

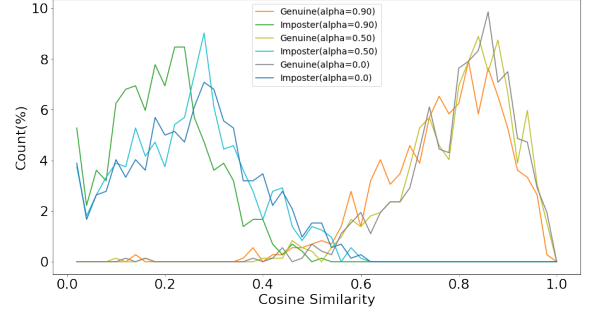


Fig. 8: Cosine similarity histograms of image pairs with different α values

used for comparing finger vein images. For this purpose, a vein enhancement method and a dual-decoder architecture is proposed.

Both the reconstruction and the recognition results show that when the contribution of the veins are increased($\alpha > 0.8$) DDCAE is able to reconstruct and encode vein patterns as well as the finger background. However, when α is low values($\alpha < 0.8$), recognition performance is more or less the same(Fig. 7). This finding would imply that the finger background information is dominant, and it should be reduced, and the vein information should be increased to extreme levels during training.

Figure 8 shows that with higher α values both imposter and genuine image pair similarity scores decreases. When the genuine image pairs are investigated(Fig. 9), it is observed that the decrease in the similarity scores is related to the increasing accuracy of reconstructed vein structures. With low α values, both the reconstruction involves more background and less vein features(Fig. 9a). When α increases, the vein structures are encoded more accurately(Fig. 9b), therefore, cosine similarity becomes more sensitive to the changes in the vein patterns.

Figure 7 indicates that recognition performance is almost the same where $\alpha = 0.9$ and $\alpha = 1.0$. When α is set to 1.0, the DDCAE is trained on only vein images. Even though it is limited, the finger background still exists on the vein images, only the contrast of the veins is higher compared to a finger vein image. Figure 10 indicates that with $\alpha = 1.0$ especially the imposter image pair scores are significantly lower than $\alpha = 0.9$. This findings imply that DDCAE can successfully encode vein patterns in the latent vector, while supporting the findings of [1] by showing that the finger background contributes the identity information.

Model	EER(%)	AUC
DDCAE	1.38	0.997
Previous work[1] ¹	6.74	0.968
Maximum Curvature[4]	0.4	0.999

TABLE III: Performance comparison of DDCAE, previous work and Maximum Curvatures

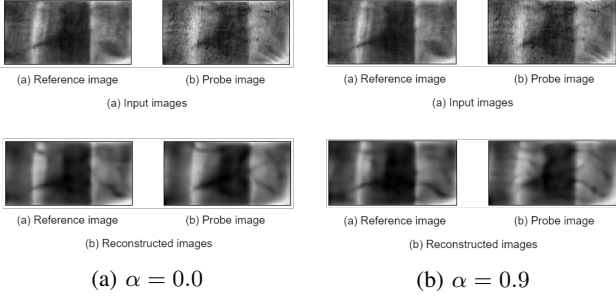


Fig. 9: Comparison of reconstruction with (a) $\alpha = 0.0$, (b) $\alpha = 0.9$

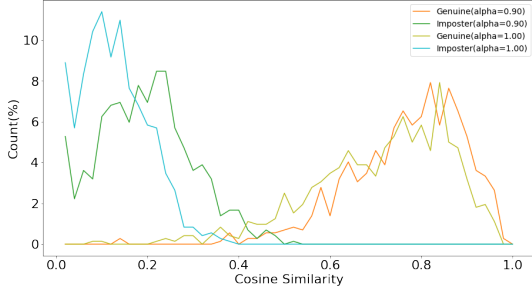


Fig. 10: image pair similarity histograms of $\alpha = 0.9$ and $\alpha = 1.0$

VII. CONCLUSION

This work investigates that whether AEs are capable of reconstructing and encode fine structures like veins, so that the representation can be used in comparing finger vein images. For this purpose, a finger vein enhancement method and a dual-decoder convolutional auto encoder architecture is proposed. The proposed approach achieved 1.38% EER on UTFVP dataset surpassing the previous work[1]. This result indicates the potential of unsupervised learning methods on finger vein recognition.

Beside showing that AEs are able to learn finger vein representations, the results indicates that finger background is dominant to vein structures, so in order to properly encode vein information, the background information should be surpassed to extreme degrees.

REFERENCES

- [1] T. Arican, R.N.J. Veldhuis, and L.J. Spreeuwiers, Finger vein verification with a convolutional auto-encoder, 41st Symposium on Information Theory and Signal Processing in the Benelux 2021. Werkgemeenschap voor Informatie-en Communicatietheorie (WIC), 2021.
- [2] B.T. Ton, R.N.J. Veldhuis, A high quality finger vascular pattern dataset collected using a custom designed capturing device, 2013 International conference on biometrics (ICB), IEEE, 2013.
- [3] N. Miura, A. Nagasaka, and T. Miyatake, Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, Machine vision and applications vol. 15, no. 4, pp. 194-203, 2004.
- [4] N. Miura, A. Nagasaka, and T. Miyatake, Extraction of finger-vein patterns using maximum curvature points in image profiles, IEICE TRANSACTIONS on Information and Systems vol. 90, no. 8, pp. 1185-1194, 2007.

- [5] S. Tang et al, Finger vein verification using a Siamese CNN, IET Biometrics vol. 8, no. 5, pp. 306-315, 2019.
- [6] J.M. Song, W. Kim, and K. R. Park, Finger-vein recognition based on deep DenseNet using composite image, IEEE Access 7, 2019.
- [7] J. Zeng, Y. Chen, C. Qin, F. Wang, J. Gan, Y. Zhai, B. Zhu, A Novel Method for Finger Vein Recognition, Chinese Conference on Biometric Recognition, 2019.
- [8] B. Hou, R. Yan, Convolutional Auto-Encoder Model for Finger-Vein Verification, IEEE Transactions on Instrumentation and Measurement, 2019.
- [9] B. Hou, R. Yan, Convolutional Auto-Encoder Based Deep Feature Learning for Finger-Vein Verification, 2018 IEEE International Symposium on Medical Measurements and Applications (MeMeA), pp. 1-5, 2018.
- [10] H. Hu, W. Kang, Y. Lu, Y. Fang, H. Liu, J. Zhao, F. Deng, FV-Net: learning a finger-vein feature representation based on a CNN, 2018 24th International Conference on Pattern Recognition (ICPR), pp. 3489—3494, 2018.
- [11] H. Hong, M. Lee, K. Park, Convolutional neural network-based finger-vein recognition using NIR image sensors, Sensors, vol. 17, pp. 1297, 2017.
- [12] J. Yang, et.al., Facial Expression Recognition Based on Convolutional Denoising Autoencoder and XGBoost, IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2019.
- [13] I.D. Bhaswara, Exploration of autoencoder as feature extractor for face recognition system, MS thesis, University of Twente, 2020.
- [14] F. Silva, et al, Pre-Training Autoencoder for Lung Nodule Malignancy Assessment Using CT Images, Applied Sciences, vol. 10, no. 21, 2020.
- [15] V. Ghodrati, et al, MR image reconstruction using deep learning: evaluation of network structure and loss functions, Quantitative imaging in medicine and surgery vol. 9, no. 9, 2019.
- [16] W. Yang, C. Hui, Z. Chen, J. Xue, Q. Liao, FV-GAN: Finger Vein Representation Using Generative Adversarial Networks, IEEE Transactions on Information Forensics and Security, vol. 14, pp. 2512 – 2524, 2019.
- [17] N. Ichimura, Spatial frequency loss for learning convolutional autoencoders, arXiv:1806.02336, 2018, arXiv preprint.

Biometric testing: aligning standards and practice

Florens de Wit
University of Twente
Enschede, The Netherlands
f.f.dewit@utwente.nl

Chris Zeinstra
University of Twente
Enschede, The Netherlands
c.g.zeinstra@utwente.nl

Luuk Spreeuwiers
University of Twente
Enschede, The Netherlands
l.j.spreeuwiers@utwente.nl

Abstract—The performance of Biometric recognition systems has improved of the past ten years. For application it is necessary to know how well they perform in specific operational circumstances. This requires performance evaluation based on scientific principles.

The Data Management and Biometrics (DMB) group at the University of Twente, frequently evaluates biometric algorithms for third parties in the public and private sector. We have encountered mismatches between the stakeholders' interest and what is being prescribed in standards and guidelines that apply to biometric performance testing, and reporting of its results.

In this paper we show how standards and practice can be better aligned. First we explore the problem through case studies, and suggest solutions for the issues we find. Given these results we propose a systematic approach to analysing and reducing misalignment. Our goal is threefold:

- increase our own awareness whether biometric performance evaluations are in line with applicable standards; i.e., learn and further improve our testing skills
- Investigate whether the standards reflect the diversity in forms and objectives evaluations have
- suggesting changes to standards so they align more easily with practice and/or developing additional guidelines to facilitate standardised practice in specific cases

Index Terms—Biometric testing, standardisation

I. INTRODUCTION

In recent years biometric devices and systems have come to be commonly applied. Though initially mainly used in a security and law enforcement setting, biometric applications have become part of many people's lives. Many service providers - most notably banks - have started to use mobile apps that use biometric verification of identity e.g. via fingerprint or face recognition. This application of biometric recognition tries to balance security with convenience; i.e.: using biometric features for verification of identity is just as secure, but more convenient than having to use some token - like a bank card - and/or some secret key or password; you can forget to bring your card, or fail to remember your key or password, but you can never fail to take your biometric traits with you.

But how does your smart phone know it is your finger pressing the button - which is also a fingerprint scanner? How do vendors, developers, operators and ultimately users like you, know an application of biometric technology actually works as well as they would like it to?

To answer the last question first: applications of biometric technology are tested - just as practically any technology is -

and the technical performance is one of the aspects the testing covers.

The Data Management and Biometrics (DMB) group of the University of Twente frequently participates in evaluations of biometrics systems for third parties in the public and private sector. We have encountered mismatches between the stakeholders' interests and what is being prescribed in guidelines and standards for biometric performance evaluation and reporting of its results (e.g. the operational conditions differ from those implied by the standard). This mismatch is our main motivation to investigate what causes it, and how to re-align the practice with standards and guidelines.

Therefore our research questions are:

- 1) In what way do standards and guidelines mismatch with the practice of biometric performance evaluation?
- 2) What additional guidelines can help actual evaluations conform more closely with applicable standards?
- 3) What amendments or changes to standards would make them match more closely with evaluation practice?

To provide some context, and provide an introduction into the terminology of biometrics performance testing, next we will explain how biometric technology works in general and how the performance of said technology is evaluated.

All terminology in the following sections has been taken from ISO standards 2382-37 [1], and 19795 parts 1 and 2 [2] [3].

A. the biometric process

To explain how biometric technology works in general we will use the example of smart phones' fingerprint recognition capability. The general biometric process is visualised in fig.1.

Many smart phones can be opened with a fingerprint. This functionality uses the phone's biometric recognition capabilities for the mode of fingerprint. *Biometric recognition* is the automated recognition of individuals based on their biological and behavioural characteristics. The biological and behavioural characteristics used in biometric recognition are called *biometric characteristics*. The *mode* formally is the combination of a biometric characteristic a sensor type and a processing method, but often just the characteristic is mentioned e.g.: fingerprint, face, iris, gait etc.

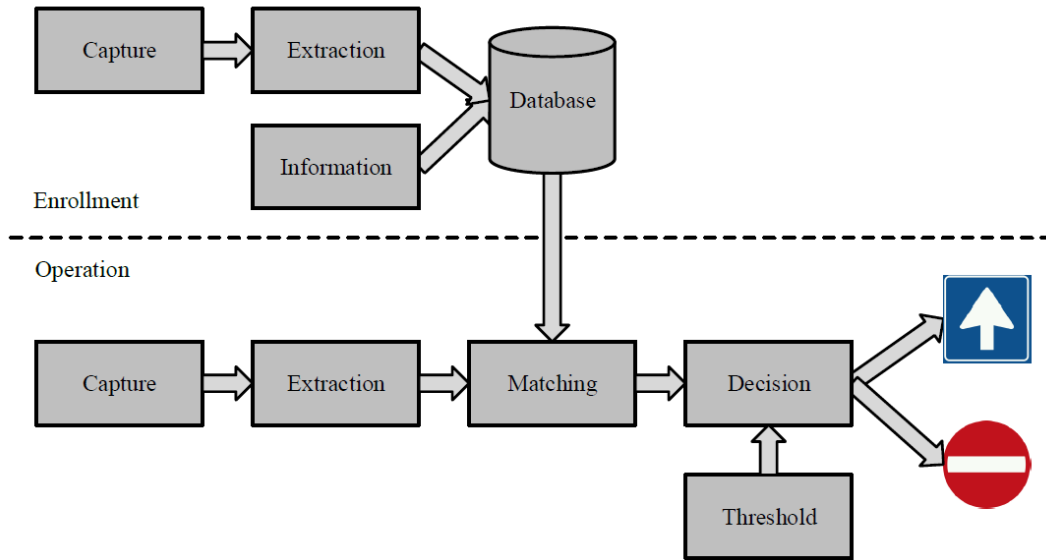


Fig. 1. Essential stages in a biometric system. Top part shows the stages during the enrolment phase, bottom part shows the stages during the operational phase. Taken from [4] with permission from author

Before you can use your smart phone's biometric finger recognition capability, it will need to know what at least one of your fingers looks like and store the necessary information to recognise it later. When activating this capability you therefore will be asked to put your finger on a sensor at least once, so the phone can take an image of your fingerprint - a biometric sample - which is then processed to extract *biometric features*. A *biometric sample* is an analogue or digital representation of biometric characteristics prior to biometric extraction. *Biometric extraction* is the process of extracting biometric features, which are numbers and labels extracted from biometric samples and used for comparison. These features are then stored on your phone as a *biometric template* or turned into a *biometric model*; either will be used as a *biometric reference*. The biometric reference will be stored in a *biometric reference database*. This process - from presenting the biometric sample to storing biometric reference in the database - is called *biometric enrolment*.

When you subsequently use the biometric finger recognition capability to open your phone, the finger scanner takes another image of the finger you press down on it. This biometric sample you offer for recognition, is called *biometric probe*, and is also processed into biometric features and thus can be directly compared to the biometric template using a biometric recognition algorithm or applied to the biometric model. Both the recognition algorithm or the model will output some measure of similarity; a *comparison score*. The biometric recognition algorithm now takes the *comparison decision* i.e.: determines whether the biometric probe and biometric reference is of the same (biometric) source based on the comparison score, and some decision policy like a score threshold (i.e. a comparison score above this value indicates the same source, below different source).

Though we explained this using a smart phone fingerprint recognition capability as an example - a single-user process - the process is essentially the same for any system for the purpose of biometric recognition - i.e. a *biometric system* - indifferent of the mode, or number of users.

The main difference is the number of templates enrolled into the biometric reference database.

When the probe is offered as a claim of identity (i.e., a *biometric claim*) - and therefore is compared to a single reference corresponding to that identity - then the process is called *biometric verification*.

When the probe is offered with no claim of identity - and is compared to all available references - and only enrolled individuals can offer a probe, then the process is called closed-set biometric identification.

When the probe is offered with no claim of identity - and is compared to all available references - and individuals can offer a probe without being enrolled, then the process is called open-set biometric identification.

A set of a probe sample and an enrolment sample whose features are to be compared is called a pair. If the known ground truth indicates the samples originate from the same individual, then this is a *mated pair*. If the samples do not originate from the same individual it is a *non-mated pair*. Each comparison between a probe and a reference is called a *comparison trial*.

B. biometric evaluation

In a biometric evaluation one determines how well a biometric system meets functional and non-functional requirements. Just as any technology, biometric systems are not perfect; one should expect some errors will occur during biometric

recognition. For this practical reason error rates are used to communicate the performance of the biometric system.

For the purpose of this paper we will focus on so called *technology evaluations* - i.e.: offline evaluations of one or more algorithms for the same biometric mode using a pre-existing or especially-collected corpus of samples. For this type of evaluation we should assume the biometric samples have already been captured; any errors that might occur during the capture of the samples is not taken into account.

We will distinguish between basic errors directly resulting from biometric recognition - the *biometric errors* - and errors that result from supporting functionalities.

Starting with the basic system error rates:

a) *failure-to-enrol rate*: any failure in producing a biometric reference from an enrolment sample counts as a *failure-to-enrol*; this includes any failure to process the biometric sample into features, and any failures in the process of producing the biometric reference from said features or store said reference into the biometric reference database. The proportion of enrolment samples where enrolment fails is the failure-to-enrol rate.

b) *failure-to-acquire rate*: Before any recognition can take place, the probe must be captured, and its biometric features need to be extracted. If, for any reason, capture or extraction fails, this counts as a failure-to-acquire. The proportion of initial attempts at capturing a probe and extracting its feature that fails is the failure-to-acquire rate.

Note that for a technology evaluation the probe samples may already have been captured. In such case the failure-to-capture rate for the given corpus must be known for the failure-to-acquire rate to be calculated correctly.

The basic biometric error rates are:

c) *False match rate (FMR)*: If, for a non-mated pair, the biometric recognition algorithm declares a match, this is a *false match*. The proportion of non-mated pairs that have been compared and result in a false match is the *false match rate*.

d) *False non-match rate (FNMR)*: If, for a mated pair, the biometric recognition algorithm declares a non-match, this is a *false non-match*. The proportion of non-mated pairs that have been compared and result in a false non-match is the *false non-match rate*.

From these basic error rates, several specific error rates result; which is relevant depends on the type of recognition task - i.e., verification, open-, or closed-set identification.

For verification the following specific error rates are relevant:

e) *False reject rate (FRR)*: If for a pair of mated samples, the true biometric claim is erroneously rejected, this is a *false reject*. The proportion of mated pairs where the (true) biometric claim is erroneously rejected is the *false reject rate*.

f) *False accept rate (FAR)*: If for a pair of non-mated samples, the false biometric claim is erroneously accepted, this is a *false accept*. The proportion of non-mated pairs where the (false) biometric claim is erroneously accepted is the *false accept rate*.

Note that FRR and FAR only differ from the FNMR and FMR in that they consider the decision to reject or accept the biometric claim, rather than the individual match/non-match decision, and account for the failure-to-acquire rate. If one also accounts the failure-to-enrol and/or failure-to-acquire this is called the Generalised FRR and FAR (GFRR/GFAR).

See ISO/IEC 19795-1 [2] section 9.5 for equations to calculate (G)FRR and (G)FAR.

Next we will review related work and the existing standards for biometric performance evaluation (section II), followed by an overview of our preliminary case studies (section III), discussion of the discrepancies of cases versus standards, and our proposed approach to alignment (section IV). We end with our conclusion(s) in section V.

II. RELATED WORK & STANDARDS

A. Early guidelines and evaluations

Though biometrics have been used in law enforcement since the late 19th century, automated systems only became feasible from the early 1980s, when automated fingerprint identification systems (AFIS) were first deployed (e.g. [5]).

The FERET programme - which was run and funded by the United States government during the 1990s - initiated research into automated face recognition systems, and also tested the performance of the resulting algorithms [6].

The Face recognition vendor test (FRVT) held in 2000 [7] - the first in a series of evaluations of commercial face recognition technology - already notes advances in the few years since the FERET program ended. It implicitly indicates that systematic evaluation of biometric technology is a must when government agencies are to deploy biometric systems for law enforcement.

The Fingerprint Verification Competition also held in 2000 [8], states that it is a way for both commercial and academic parties to compare performance of fingerprint recognition algorithms and track the improvements of one's own and other's algorithms.

Based on experience in evaluating biometric systems (i.e. [9]), [10] is an early attempt to formulate general guidelines for testing and reporting biometric performance.

Given the perceived need for systematic objective and science-based evaluation of biometric performance, it made sense to start standardising how biometric technology was tested, and how to report the results.

B. ISO/IEC standards for biometric performance evaluation and reporting

The International Organisation for Standardisation's (ISO), Joint Technical Committee one (JTC1), subcommittee 37 (SC37) on biometrics (and its working groups), has issued

several standards and guidelines, relevant for our current research, on:

- *Harmonised biometric vocabulary* in ISO/IEC 2382-37 [1]
- *Principles and framework* for biometric testing and reporting in ISO/IEC 19795-1 [2]
- *Testing methodologies for technology and scenario evaluation* in ISO/IEC 19795-2 [3]
- *Evaluation of examiner assisted biometric applications* in ISO/IEC TR 29189 [11]

These standards have been developed further based on comments from researchers and other stakeholders that apply them to their results and products. The multi-part standard ISO/IEC 19795 has several parts that apply to specific application areas (e.g. mobile devices), specific technology (e.g. multi-modal biometrics) or focus of evaluation (e.g. variation of performance across and between demographic groups).

We have compared the aforementioned standards to the practice of evaluations we performed and/or took part in for third parties. In the next section we will give an overview of our findings.

III. CASE STUDIES

A. Case 1: Automated Fingerprint Identification System

1) *Background:* We supported a government organisation (the stakeholder) in selecting the most suitable algorithm for their Automated Fingerprint Identification System (AFIS) by testing the performance of available algorithms using fingerprint and fingermark data available from the organisations own data stores. The fingerprint data consists of sets of prints from all available fingers (a so called "ten-print card") taken to identify the individual (e.g. at arrest) in the course of a criminal investigation. Each ten-print record contains the image files of the fingerprints collected. The data store contained one or more ten-print records of the same individual, depending on the number of times fingerprints were taken.

The fingermark data contained latent fingermarks secured at crime scenes in the form of digital image files. This store contains both fingermarks that have been linked to an individual through matching with the ten-print, and fingermarks of currently unknown source.

Additionally an algorithm for palm-mark identification would be tested concurrently; the data had a similar structure as fingermark and fingerprint data.

2) *The test setup:* The objective of this test was to evaluate the matching performance of fingermarks and palm-marks to three types of fingerprint records and one type of palm-print records. The performance on the four record-type were combined by weights that were decided on in conjunction with the stakeholder based on the expected future use and significance for daily operations.

To measure matching performance two custom metrics were developed, to account for the role of human examiners in the process, without having to involve actual examiners in the evaluation process.

The collection of data for the test corpus faced some technical difficulties which could impact the data quality. The stakeholder therefore opted just to record the failures to enrol and acquire, but not count them against the individual vendor's performance.

Vendors could apply to participate in the test. They volunteered based on a description of the requirements of the system, and a description of what would be required to take part in the test. The test requirements included that the vendors would estimate and provide the hardware necessary to:

- unpack the data from a standardised biometric data exchange format (and log any errors)
- enrol a given number of ten-print and palm-print records (and log any failures)
- for (each of) a given number of probe samples:
 - extract their biometric features (and log any failures)
 - compare the features to all the fingers in all references
 - return a ranked list of the top-20 of matching reference identifiers with their comparison score

Vendors that took part were also required to have their own personnel operate their hardware on site of the stakeholder.

The custom performance metrics then were calculated from the ranked score lists for each type of reference record, and then combined using the aforementioned weights into a single summary performance metric. For the summary performance metric values we calculated a 99% credible interval based on a non-informative prior. Both per-type and summary performance was communicated to the stakeholder for all vendors; vendors received a report of their own performance only.

3) *Main discrepancies:* If we compare our contribution to this test with the requirements stated in relevant standards, some discrepancies stand out;

No reporting or documenting of some test details

The test report does not document or report,

- the test type; i.e., technology evaluation
- the comparison functionality; i.e., open-set identification
- whether meta-data was made available to the systems under test
- whether the corpus of samples was appropriate for the goals of the test
- any details on how the test corpus was gathered, composed and validated, including failure-at-source (i.e., when samples were discarded before use in the test)
- the fact the test corpus was selected from the data gathered using a system partially supplied by one of the vendors taking part

General error metrics nor timing were calculated or reported

Though failures during enrolment and acquisition were reported by the vendors, we have not calculated failure rates. Consequently neither failure-to-enrol nor failure-to-acquire was accounted for in the FRR or FAR. This is consistent with

the intention of the stakeholder but not in accordance with standards.

The basic biometric error rates for matching (FNMR/FMR) were not calculated either, nor were FRR or FAR. The specific derived performance measures we were requested to report do not completely reflect standardised error rates either.

There was no timing of any of the processing or matching tasks required of the vendors, and so no data on timing was reported.

Other (potential) issues According to standards, the fact that vendors have supplied, installed, and configured their hardware is allowed. However, it is not entirely clear whether the vendors were strictly prohibited to run the enrolment and comparison tests, or whether this is just considered as problematic.

B. Case 2: sequential verification and identification for border control

1) *Background:* When large volumes of passengers need to cross a border, even Automated Border Control gates (ABC gates) can lead to congestion in specific areas and delays due to possible biometric errors.

Besides simply increasing the capacity by adding more ABC gates, some stakeholders, such as airports, airline operators and vendors of security solutions, have proposed to redefine the verification of identity of the traveller at a specific location (i.e. the ABC gate) into a fluid transition from one area to the next. This concept of a "seamless" border, can be implemented in different ways however.

In the implementation we tested, the seamless border has two steps:

- 1) The outbound passenger enrolls at a kiosk by verifying a face image taken on site - the *kiosk image* - against the physical or electronic photograph on a travel document (s)he brought. If the kiosk image is verified against the travel document image, it is enrolled in a temporary reference database
- 2) When the traveller enters an area restricted to outbound traffic, images from CCTV-like cameras are used to identify the traveller from the temporary reference database; once identified (s)he can now proceed to the gate.

2) *The test setup:* In this test three algorithms from two suppliers were tested. The stakeholder, a large airport organisation, provided us with a dataset of passport images, images of volunteers taken in a kiosk and by a camera in a more-or-less unrestricted setting - the *camera image*.

The test has two parts:

- 1) test verification capability i.e. the 1:1 comparison of kiosk images against passport images; verify which algorithms are able to achieve a FRR of at most 2.1% at an FAR of 0.06%

- 2) Test identification capability i.e. the 1:many comparison of the camera images against kiosk images; verify which of the algorithms achieve a FNIR of at most 15% at a FPIR of 0.4%

The tests were conducted separately and independently;

For part one, all kiosk images were compared to all passport images and the FMR and FNMR calculated at all available threshold score levels and plotted as a DET plot. Failure to enrol was logged.

For part two, all camera images were compared to all kiosk images and ranked by score. Identifications only counted as true positive when only the corresponding kiosk image had a score above the threshold; multiple kiosk images ranking above the threshold score level results in false negative identification.

The FPIR and FNIR were calculated from the ranked scored lists and a DET plot was constructed. Failure to generate a template from the camera image was logged.

We determined whether the algorithms achieved the desired $FRR < 2.1\%$ at $FAR = 0.06\%$ by determining FAR with a 99% credible interval with an upper limit of 0.06%, and verify that the upper limit of the corresponding FRR 99% credible interval is below 2.1%.

A similar procedure is taken for verifying that the FNIR does not exceed 15% at an FNIR of 0.4%.

3) *Main discrepancies:* Again, some issues come to light when we compare with relevant standards;

multiple experimenters & different test corpus

The application programming interface of one of the algorithms under test proved to be prohibitively complex to use for a single test. The stakeholder decided that the vendor of the seamless border system - not the vendor of the algorithm - who had the algorithm configured and working on its systems, would execute the comparisons and transfer the result data to us, partially delegating the role of experimenter. This execution by a potential stakeholder may already be problematic according to standards.

After receiving the result data from the external, it became clear that the number of images used for the test of the particular algorithm was lower than the number used for the other two algorithms. We could not ascertain which images were missing, since the filename encoding was different for the test corpus used by the system vendor.

Taken altogether, one algorithm was tested by a different experimenter on a different test corpus, which makes the intended direct comparison of results somewhat problematic.

failure rates & timing unknown or not calculated

The corpus of samples had been previously collected by, or under supervision of, the stakeholder. Unfortunately no failure-to-capture data had been recorded. Any failure to process any of the images into templates (i.e. encoded sets of features as created and used by the algorithm) were logged but no

failure-to-extract, failure-to-enrol or failure-to-acquire were calculated.

Timing was not logged, either in the data collection or during the feature extraction or comparison tests.

Other (possible) issues

This evaluation was designed as two separate technology evaluations applied to the same algorithms. The given operating points (e.g. FRR @ FAR = 0.06%) will not reflect the actual overall error rates of the two stages combined. For an individual user the likelihood of rejection at the kiosk is likely to be correlated to the probability of false negative identification.

One might argue that the presentation of the results as separate independent tests might give a unwarrantedly positive impression of the expected performance of the combined system.

IV. DISCUSSION & ALIGNMENT

Reflection on the discrepancies we discussed in section III points to a few ways to improve our own approach, and possibly contribute general lessons to the community. We will first discuss those improvements and lessons, and then propose an approach to incorporate learning into biometric performance evaluation efforts.

A. lessons learned & solutions

In both case studies, we failed to calculate and report some failure and error rates. The main motivation for not calculating these rates despite available data, was practical: the stakeholder involved was not primarily interested in these rates.

The direct and most simple solution to this discrepancy is to simply calculate failure and error rates when data is available, and report them in a standardised test report supplement if the stakeholder is primarily interested in the "custom" results.

The involvement of technology suppliers other than to supply, install, and configure software and possibly hardware is viewed as problematic; especially the involvement in the execution of enrolment and comparison tests is considered to be "not done" (see e.g. [3], page 29). However, having individual vendors execute their own implemented solutions on their own hardware using a given test corpus and a clear task description could become a standardised practice with some guidelines and rules. The main issue is the prevention of what is called "gaming" in the standards we reviewed; the practice of using test data to improve the system's performance during the test.

In the evaluation described in section III-A the suppliers of the algorithms performed all tests themselves under supervision of the testing organisation (which was the stakeholder law enforcement organisation). The hardware was confined to a secure room and strictly run offline except for possible updates before the tests were executed. Vendor employees signed an agreement not to communicate any detail about the test during the execution.

We believe that developing a standardised set of rules governing access to system, data, and information, and expected behaviour of individuals involved, could bring the "self-test" by vendors into the scope of standardised biometric performance testing.

On a more technical note, it is as yet unclear how to report results of an evaluation like described in section III-B; combining the evaluation of two or more component systems should be standard practice rather than merely at the convenience of the tester.

B. a proposal for a systematic approach to alignment

The previous sections demonstrate it is possible to find ways to improve our own expertise in biometric testing practices and possibly to improve the alignment of standards with such practices. However, the described improvements are rather collected on an ad-hoc manner. We therefore propose the following systematic approach to facilitate both these interests.

Case studies

To find out whether individual biometric evaluation efforts were compliant with general and specific standards and guidelines we will analyse a number of such efforts that we took part in. We will compare the practice with what the standards prescribe, and find the gaps between the standard and its application. At the same time we consider what changes to the standard and/or additional guidelines would be required to either make the standard more similar to practice or facilitate the application of the standard.

We will develop tools to support this analysis.

Suggestions for changes and/or guidelines

Based on the degree of misalignment and the potential for closing the gap, we will make proposals for re-alignment. With suggestions to change standards we will work together with international experts to maximise the support for these changes. Suggested guidelines to help application of existing standards will require a trade-off between the specific details of each case, and the ability to generalise the lessons from such case.

Application of proposals

Once we have a consistent set of proposals, we can apply this to existing and new cases to see if the proposals are "fit-for-purpose". If possible we would compare and contrast the proposed changes with the existing situation.

Evaluation

The application phase will give us the data to evaluate whether the proposals indeed helped re-align standards and practice. Based on this evaluation we can refine our proposals and re-iterate using new cases for input.

V. CONCLUSION

The goal of this paper was to investigate what misalignment exists between standards and practice in biometric testing, and

whether re-alignment would be possibly through either providing guidelines to further practical application of standards, or changes or amendments to the standards themselves.

In preliminary case studies we found that;

- non-compliance with calculating and/or reporting standard performance metrics could be due to lack of interest of the stakeholder; re-alignment is possible through guidelines e.g. to routinely draft a standardised supplement report with the standard metrics and results, independent of what is reported to the stakeholder.
- though the supplier of an algorithm under test is allowed to supply and configure the software and hardware it is currently prohibited to have the supplier execute enrolment and/or comparison tests; Such "self-tests" could be brought into the scope of standardised testing by providing prescribed measures and additional guidelines to control the risks of "gaming" and other issues.
- when testing the biometric performance of multiple components of the same system it appears to be up to the experimenter whether to estimate or report the expected combined performance of said components; this could be re-aligned by amending the standards or developing a guideline so experimenters routinely notify stakeholders of the potentially different performance of the component combination.

Since case studies clearly support increasing our expertise in biometric performance testing, and could benefit the broader biometric community through improvements in standardisation, we proposed a systematic approach to alignment of standards and biometric testing practice through a iterative application of case studies, proposed re-alignment efforts, application of said proposals and evaluation of the effect.

REFERENCES

- [1] ISO/IEC, "IS 2382-37:2017: Information Technology – Vocabulary – part 37: Biometrics," international standard, International Organisation for Standardisation, Geneva, CH, 2022.
- [2] ISO/IEC, "IS 19795-1:2021: Information Technology – Biometric performance testing and reporting – part 1: Principles and framework," international standard, International Organisation for Standardisation, Geneva, CH, 2021.
- [3] ISO/IEC, "IS 19795-2:2007: Information Technology – Biometric performance testing and reporting – part 2: Testing methodologies for technology and scenario evaluation," international standard, International Organisation for Standardisation, Geneva, CH, 2007.
- [4] C. G. Zeinstra, *Forensic Face Recognition: From characteristic descriptors to strength of evidence*. PhD thesis, University of Twente, Enschede, The Netherlands, 2017.
- [5] "Nec technical journal – looking back at nec's history – nec's fingerprint identification technology is acclaimed worldwide." <https://www.nec.com/en/global/techrep/journal/nechistory/nh02/index.html>. Accessed: 2022-05-19.
- [6] P. Phillips, H. Moon, S. Rizvi, and P. Rauss, "The feret evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.
- [7] D. M. Blackburn, M. Bone, and P. J. Phillips, "Face recognition vendor test 2000: evaluation report," tech. rep., DEFENSE ADVANCED RESEARCH PROJECTS AGENCY ARLINGTON VA, 2001.
- [8] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "Fvc2000: Fingerprint verification competition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 24, no. 3, pp. 402–412, 2002.
- [9] T. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric product testing; final report," tech. rep., Centre for Mathematics and Scientific Computing, National Physical Laboratory, Teddington, UK, March 2001.
- [10] A. Mansfield and J. Wayman, "Best practices in testing and reporting performance of biometric devices," tech. rep., Centre for Mathematics and Scientific Computing, National Physical Laboratory, Teddington, UK, August 2002.
- [11] ISO/IEC, "TR 29189:2015: Information Technology – Biometrics – Evaluation of examiner assisted biometric applications," technical report, International Organisation for Standardisation, Geneva, CH, 2015.

Min-Path-Tracing: A Diffraction Aware Alternative to Image Method in Ray Tracing

Jérôme Eertmans

ICTEAM

UCLouvain

Louvain-la-Neuve, Belgium
jerome.eertmans@uclouvain.be

Claude Oestges

ICTEAM

UCLouvain

Louvain-la-Neuve, Belgium
claude.oestges@uclouvain.be

Laurent Jacques

ICTEAM

UCLouvain

Louvain-la-Neuve, Belgium
laurent.jacques@uclouvain.be

I. CONTEXT

Over the past decades, Ray Tracing (RT) has gained increased interest in computer graphics [1]–[4] and telecommunication fields [5]–[8]. In both cases, RT offers accurate solutions for problems that require the simulation of electromagnetic (EM) waves, including light, interacting with the environment. Due to its high precision, but also its high computational cost, RT is mainly used as a reference solution when compared to stochastic or hybrid models, or by operators that have greater computational power available. Generally speaking, using a telecommunication terminology, RT's goal is to compute every possible path between two nodes, and later apply appropriate physical wave propagation rules. In the field of radiocommunications, the knowledge of those paths can help to determine a channel model for communication between those nodes, *e.g.*, between base station (BS) and user-equipment (UE). Then, the channel model can be used to derive some important metrics, such as the delay, power attenuation or interference level. A variety of RT implementations can be found, either with deterministic outcomes (*e.g.*, Image RT) or stochastic (*e.g.*, Ray Launching), as well as hybrid versions that try to combine both methods to obtain the best compromise: an accurate and deterministic solution at a relatively low cost. However, regarding image based RT, it seems that modern ray-tracers suffer from limitations on both the number of diffractions and the type of geometries they can handle, *i.e.*, mostly planar surfaces (*e.g.*, polygons) [9].

II. CONTENT DESCRIPTION

In this paper, we describe Min-Path-Tracing (MPT), an alternative to the image method that allows us to generalize the *path finding* process, *i.e.*, the computation of all possible paths between two nodes, regardless of the type of geometries of 3-D scene or the number of diffractions encountered along the path. Our technique leverages, if available, the implicit equations of surfaces and edges in the scene to construct a minimization problem. Then, the paths coordinates—the collection of path interaction points on each surface—are obtained as solutions of this problem. As with the image method, MPT is only concerned with finding the path between two points that performs a certain list of interactions with the

environment. Our method does not take into account possible obstructions that could be caused by other objects. This will be the role of the "validation" step and will be discussed in the paper. Even though our contribution is mainly focused on the path finding problem, we provide many details on all important steps in RT so that the interested reader can produce a functional RT simulation from this document. The structure of this work is organized as follows. First, we summarize the main components of modern radiocommunications-oriented RT engines and in which context our contribution takes place. Next, we establish the problem we are solving by defining appropriate mathematical objects. Since both MPT and the image-based method first require defining a list of interactions, we describe how we generate all possible lists using a directed graph-based approach. Next, we detail how the image method and our alternative work in practice, and we also provide a basic Python implementation that is made available to the reader in open access and shows on a simple example that both methods yield the same solution. After, we summarize the main steps of the computation of paths between the BS and UE nodes in a single algorithm. Then, we compute electric field contributions from different paths, in a simple urban scenario, to highlight the importance of intermediate and multiple diffractions in radiocommunications. Finally, we discuss the differences between the image-based method and the MPT method, and we give a few applications where our method could be useful, as well as future prospects.

III. CONCLUSION

We presented MPT, a method that overcome the inherent limitations of the image-based method in RT by both allowing for any number of diffraction and arbitrarily complex geometries. We also showed that multiple diffractions paths can play an important role in radiocommunications and being able to account for such paths is key. After, we discussed the different pros and cons of our method, such as the difficulty to compute diffraction coefficients in the situation where multiple diffractions are chained [10], [11] or how we can obtain implicit equations of every object in our 3-D scene. Finally, we explained how one could extend MPT to handle ray refraction, and other future improvements.

REFERENCES

- [1] A. Marrs, P. Shirley, and I. Wald, Eds., *Ray Tracing Gems II: Next Generation Real-Time Rendering with DXR, Vulkan, and OptiX*. Berkeley, CA: Apress, 2021.
- [2] A. Dib, G. Bharaj, J. Ahn, C. Thébault, P. Gosselin, M. Romeo, and L. Chevallier, "Practical Face Reconstruction via Differentiable Ray Tracing," *Computer Graphics Forum*, vol. 40, no. 2, pp. 153–164, 2021.
- [3] S. G. Parker, J. Bigler, A. Dietrich, H. Friedrich, J. Hoberock, D. Luebke, D. McAllister, M. McGuire, K. Morley, A. Robison, and M. Stich, "OptiX: A general purpose ray tracing engine," *ACM Transactions on Graphics*, vol. 29, no. 4, pp. 66:1–66:13, Jul. 2010.
- [4] T.-M. Li, M. Aittala, F. Durand, and J. Lehtinen, "Differentiable Monte Carlo ray tracing through edge sampling," *ACM Transactions on Graphics*, vol. 37, no. 6, pp. 222:1–222:11, Dec. 2018.
- [5] V. D. Esposti, "Ray tracing: Techniques, applications and prospect," in *2020 International Symposium on Antennas and Propagation (ISAP)*, Jan. 2021, pp. 307–308.
- [6] F. Fuschini, E. Vitucci, M. Barbiroli, G. Falciasacca, and V. Degli-Esposti, "Ray tracing propagation modeling for future small-cell and indoor applications: A review of current techniques," *Radio Science*, vol. 50, pp. n/a–n/a, May 2015.
- [7] Y. Yang, T. Li, X. Chen, M. Wang, Q. Zhu, R. Feng, F. Duan, and T. Zhang, "Real-time ray-based channel generation and emulation for UAV communications," *Chinese Journal of Aeronautics*, Dec. 2021.
- [8] P. Tang, "Channel Characteristics for 5G Systems in Urban Rail Viaduct Based on Ray-Tracing," in *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Dec. 2021, pp. 24–28.
- [9] D. He, B. Ai, K. Guan, L. Wang, Z. Zhong, and T. Kürner, "The Design and Applications of High-Performance Ray-Tracing Simulation Platform for 5G and Beyond Wireless Communications: A Tutorial," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 10–27, 2019.
- [10] D. S. JONES, "DOUBLE KNIFE-EDGE DIFFRACTION AND RAY THEORY," *The Quarterly Journal of Mechanics and Applied Mathematics*, vol. 26, no. 1, pp. 1–18, Feb. 1973.
- [11] G. Carluccio, F. Puggelli, and M. Albani, "A UTD Triple Diffraction Coefficient for Straight Wedges in Arbitrary Configuration," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 12, pp. 5809–5817, Dec. 2012.

Hardware-Friendly Iterative Projection Aggregation Decoder for Reed-Muller Codes

Marzieh Hashemipour-Nazari and Kees Goossens and Alexios Balatsoukas-Stimming
Eindhoven University of Technology, The Netherlands

Abstract—In this work, we describe a hardware-friendly simplification on recently introduced recursive projection aggregation (RPA) decoding algorithm for Reed-Muller codes. Our simulation results show that the proposed simplification has a negligible error-correcting performance degradation while reducing the computations by up to 67% for an $RM(3, 7)$ code.

I. INTRODUCTION

Achieving high reliability in time-critical machine type communication (MTC) for 5G and future beyond-5G networks is an open research problem in the field of error-correction coding. Among the linear block codes, Reed-Muller (RM) codes have gained interest for MTC recently, as they achieve the capacity for general symmetric channel under maximum-likelihood (ML) decoding. However, ML decoding is not practical due to its high computational complexity. Recursive projection aggregation (RPA) [1] decoding is a more efficient near-ML decoding method for RM codes. However, the hardware implementation of RPA decoding is still challenging due to its complexity and its recursive structure. In this work, we describe a simplification of RPA decoding, called iterative projection aggregation (IPA) [2] decoding that removes the recursive structure of the RPA decoder, making it feasible for parallel hardware implementation for time-critical applications.

II. RPA DECODING

RPA decodes a noisy vector $\mathbf{y} = \mathbf{x} + \mathbf{w}$, where \mathbf{x} is a modulated $RM(m, r)$ codeword with length of n and order of r and \mathbf{w} is Gaussian noise in three steps: 1) projection, 2) recursive decoding, and 3) aggregation. In the projection step, $n - 1$ different vectors with length of $n/2$ are generated by combining elements of \mathbf{y} in pairs. Each of those vectors is recursively decoded using RPA with $m - 1$ and $r - 1$ until $r = 1$, where ML decoding is done efficiently using the fast Hadamard transform (FHT). The decoded codewords for $r = 1$ are recursively aggregated using a per-coordinate majority voting to make an estimation for the transmitted codeword \mathbf{x} . These three steps repeat at every level of recursion until the output of that level is identical to its input (i.e., no further progress can be made) or a predefined maximum number of iterations N_{\max} , which is set to $\lceil \frac{m}{2} \rceil$ in [1], is reached.

III. IPA DECODING

Having multiple iterations at each level of the recursion destroys the potential parallel implementation of RPA algorithm as depicted in Fig. 1a. Our numerical simulation results showed that most of the bit errors are corrected after the first iteration of RPA decoding. Therefore, we introduced IPA that keeps only the first iteration happening in the internal levels of the

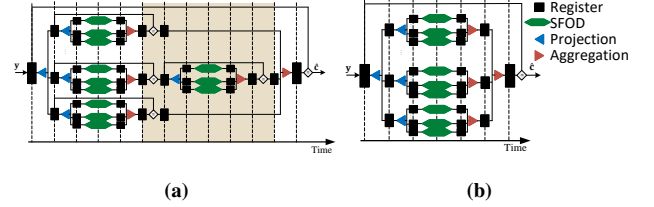


Fig. 1: Data-flow of one iteration of the RPA (a) and IPA (b) decoding of an arbitrary codeword from $RM(m, 3)$ code.

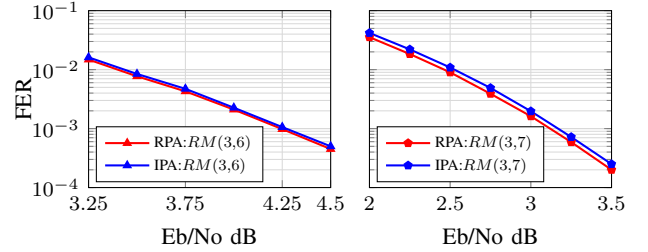


Fig. 2: FER Comparison between IPA and RPA algorithms.

TABLE I: Comparison the number of FHTs required for IPA and RPA without any early stopping condition

	RPA	IPA	Reduction
$RM(3,6)$	7818	3906	50%
$RM(3,7)$	72009	24003	67%

RPA algorithm. The parallelism of the IPA compared to RPA algorithm is depicted in Fig. 1. Besides, the IPA algorithm requires a significantly smaller number of FHTs, which is used to measure the computational complexity of the RPA algorithm.






IV. SIMULATION RESULTS

Fig. 2 shows the simulation results for RPA and IPA decoding method for two $RM(7, 3)$ and $RM(6, 3)$ codes transmitted over the additive white Gaussian noise (AWGN) channel. We set $N_{\max} = 3$ and $N_{\max} = 2$ for $RM(7, 3)$ and $RM(6, 3)$, respectively. We observe that IPA decoding has a negligible degradation in frame error rate (FER) compared to RPA while it reduces the required FHTs by 50% for $RM(6, 3)$ and 67% for $RM(7, 3)$, as shown in Table I.

REFERENCES

- [1] M. Ye and E. Abbe, "Recursive Projection-Aggregation Decoding of Reed-Muller Codes," *IEEE Trans. Inf. Theory*, vol. 66, pp. 4948–4965, Aug 2020.
- [2] M. Hashemipour-Nazari, K. Goossens, and A. Balatsoukas-Stimming, "Hardware Implementation of Iterative Projection-Aggregation Decoding of Reed-Muller Codes," *ICASSP*, Jun 2021.

Strategies for Increasing Longevity of IoT Devices

Jona Cappelle , Jarne Van Mulders , Sarah Goossens , Guus Leenders , Liesbet Van der Perre 

KU Leuven, ESAT-WaveCore, Ghent Technology Campus

B-9000 Ghent, Belgium

jona.cappelle@kuleuven.be

Abstract

The introduction of the Internet of Things (IoT) has opened a new world of opportunities to develop a myriad of applications. The fast-growing number of IoT edge devices that will be deployed is predicted to reach from 5-10 billion in 2020 up to 200+ billion in 2030 [1]. State-of-the-art IoT systems are optimized for ease of installation and operation, i.e., according to the ‘fire and forget’ credo. To date, however, negative effects on the longer term of the massive deployment of IoT have been seriously overlooked. The increasing e-Waste due to the fast-growing number of devices is already leaving its mark on the environment. Thus, increasing the longevity of these devices becomes increasingly important. Most of the reported results that claim a ‘green’ impact relate to the reduction of energy consumption [2], [3]. However, there are many more sides to this story than energy consumption alone. The future IoT requires a novel architectural approach and raises research questions regarding the design and operational procedures.

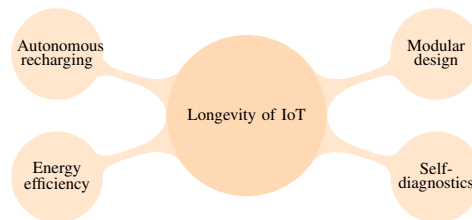


Figure 1: Holistic vision for the longevity of IoT

As shown in Figure 1, the longevity of IoT devices can be increased in a number of ways. A first strategy is the development of a procedure for time synchronized operation. Especially in mesh networks, a reduction in energy consumption is achieved when predefined time slots are used. This allows both sensor nodes and local sensor hosts to sleep for a given time, awoken periodically to receive a beacon signal, and transmit the necessary data. This approach avoids continuous listening on the wireless channel. Secondly, the reduction in wireless data traffic decreases the uplink time, hence the consumed transceiver energy. Beside using the energy efficiently, we can make the future generation of IoT systems ‘smart’ by incorporating self-deployable, self-diagnosing, and self-repairing systems. As a result, fewer devices will need to be replaced when something goes wrong. A third strategy is the consideration of multiple wireless communication technologies (multi-RAT) and selecting the most suitable wireless transceiver technology for each application [4]. Since saving energy is not always possible, another way of increasing the longevity is to provide automated options for recharging the battery. A small drone with a wireless power transfer (WPT) link can be used to recharge the IoT node [5]. Furthermore, e.g., in cities, IoT nodes can generate enormous amounts of data. Transmitting all this data through a low-power wide-area network (LPWAN) is not possible and would require huge amounts of energy. Therefore, an Unmanned Aerial Vehicle (UAV) extension, which can exchange huge amounts of data, is required. Finally, when an intervention is required, i.e., when a software update or a self-repairing system can’t provide a solution, a modular design can help to increase the longevity of IoT devices by enabling heterogeneity, upgradability, and adaptability. Parts can be easily upgraded when approaching end of life (EOL), exchanged when becoming obsolete, or even be replaced by parts with a different functionality. A wireless interconnection between parts is pursued, in which energy harvesting and efficient communications between ‘modules’ still remain a major challenge. Especially with efficient wireless interconnects, such a system becomes very suitable for the future ‘green’ IoT.

REFERENCES

- [1] *White Paper: Economics of a trillion connected devices - ARM Community Blog*. [Online]. Available: <https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/white-paper-the-route-to-a-trillion-devices> (visited on 01/24/2022).
- [2] G. Callebaut, G. Leenders, J. Van Mulders, G. Ottoy, L. De Strycker, and L. Van der Perre, “The Art of Designing Remote IoT Devices—Technologies and Strategies for a Long Battery Life,” *Sensors*, vol. 21, no. 3, p. 913, Jan. 2021, ISSN: 1424-8220. [Online]. Available: <http://dx.doi.org/10.3390/s21030913>.
- [3] J. Lorincz, A. Capone, and J. Wu, “Greener, Energy-Efficient and Sustainable Networks: State-Of-The-Art and New Trends,” *Sensors*, vol. 19, no. 22, 2019, ISSN: 1424-8220. [Online]. Available: <https://www.mdpi.com/1424-8220/19/22/4864>.
- [4] G. Leenders, G. Callebaut, G. Ottoy, L. Van der Perre, and L. De Strycker, “Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT,” *IEEE Communications Magazine*, vol. 59, no. 12, pp. 98–104, 2021.
- [5] J. Van Mulders, G. Leenders, G. Callebaut, L. De Strycker, and L. Van der Perre, “Aerial Energy Provisioning for Massive Energy-Constrained IoT by UAVs,” *CoRR*, vol. abs/2201.09786, 2022. arXiv: 2201.09786. [Online]. Available: <https://arxiv.org/abs/2201.09786>.

Distributed Gaussian Process for Multi-agent Systems

Peiyuan Zhai
Circuits and Systems
Delft University of Technology
Delft, The Netherlands
p.zhai-1@student.tudelft.nl

Raj Thilak Rajan
Circuits and Systems
Delft University of Technology
Delft, The Netherlands
r.t.rajan@tudelft.nl

Abstract—Distributed multi-agent systems (MAS) offer higher robustness and scalability compared to single-agent systems employing centralized solutions. The challenge of learning unknown environmental phenomena can be regarded as learning a hidden function, which can be modeled through non-parametric methods e.g., Gaussian Processes (GP). Our main challenge is to develop a distributed non-parametric model e.g., GP for environment monitoring. In this work, we specifically focus on developing fully-distributed algorithm for GP hyperparameter optimization. An example of hyperparameter set is $\theta = \{s_f, l_1, l_2\}$ for a squared exponential kernel, where signal variance s_f indicates the range of function, and the characteristic lengths l_1, l_2 indicate the smoothness. We also develop an asynchronous version to deal with heterogeneous processing time of agents. Assuming that local datasets at agents are independent with each other, we approximate hyperparameter optimization by maximizing the sum of local Likelihoods. By further defining a unique θ across the network, the problem can be regarded as a distributed consensus problem. Alternating direction method of multipliers (ADMM) with proximal θ update have been applied by Xie et al. [1], which still requires a center computing unit for auxiliary variable update. We propose a fully-distributed algorithm with centralized update replaced by local consensus. In each iteration, an agent collects auxiliary variables from neighbor agents, and use their average in new iteration. Asynchronous behavior is introduced by allowing fast agents to start new iterations without collecting update from slowest agents. Our proposed algorithm allows agents in the network to perform faster iterations and thus saving time.

We perform simulations with artificially generated 2D GP field under pre-defined hyperparameter setting. Noisy measurements are randomly allocated to agents for distributed hyperparameter optimization. Simulation results show that the optimal hyperparameters at agents converge to the expected values. See Figure 1.

In summary, we propose a novel fully-distributed asynchronous GP algorithm for MAS monitoring an unknown environmental phenomena. We show that our proposed solution converges to the expected values in a fully-distributed manner, in contrast to previous methods which rely on a central station. Convergence of the asynchronous version shows the potential of extending such algorithm to other heterogeneous MAS.

REFERENCES

- [1] A. Xie, F. Yin, Y. Xu, B. Ai, T. Chen, and S. Cui, “Distributed Gaussian Processes Hyperparameter Optimization for Big Data Using Proximal ADMM,” *IEEE Signal Processing Letters*, vol. 26, no. 8, pp. 1197–1201, 2019.

This work is partially funded by the European Leadership Joint Undertaking (ECSEL JU), under grant agreement No 876019, the ADACORSA project - “Airborne Data Collection on Resilient System Architectures.”

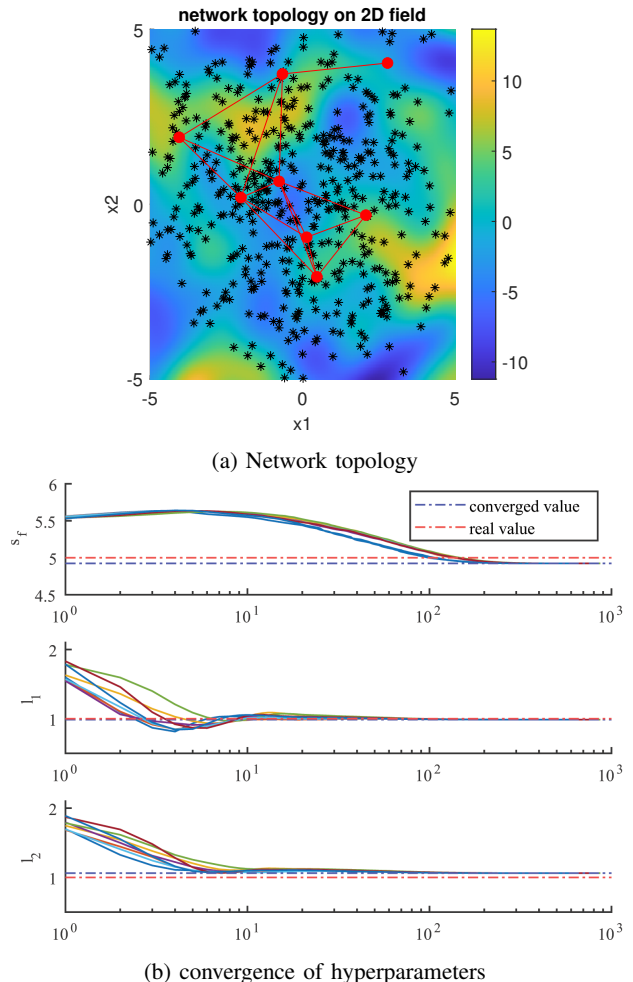


Fig. 1: (a) The background shows the underlying 2D scalar field with intensity indicated by color bar. The black stars represents the sampling positions. Agents are shown in red dots, and the red line represents the communication link between a pair of agents. (b) The figure shows the learning process of hyperparameter set θ . The real hyperparameters are $l_1 = l_2 = 1$ and $s_f = 5$. The characteristic lengths converge to $l_1 = 0.99$ and $l_2 = 1.06$, and the signal variance converges to $s_f = 4.92$, where the errors between converged and real values come from the perturbations in the datasets.

Exploring the GANformer for Face Generation

Investigating the segmentation and smile augmentation potential

Romano Ferla, Chris Zeinstra and Luuk Spreeuwiers

Data Management and Biometrics, EEMCS, University of Twente, Enschede
r.i.ferla@student.utwente.nl, {c.g.zeinstra, l.j.spreeuwiers}@utwente.nl

Abstract—Advancing the research in face applications is limited by proprietary databases and increasing data protection regulations, synthetically generated databases may provide a solution. In this work the GANformer, a hybrid generative image model, is explored for this application. While only trained for unconditioned face generation like many other models, this works shows the potential of two use cases. First, the unique implementation of the attention is examined for the application of segmentation. Second, real labeled faces are reconstructed in latent space to find latent directions describing disentangled attributes. This concept is brought in practice by augmenting neutral to smiling faces, but could be applied on other expressions and attributes as well. This work can be use as basis as it opens up two directions for further research.

I. INTRODUCTION

The performance of neural networks used in computer vision can increase logarithmically with the size of the training data [1], however larger databases are often not freely available. Common databases like VGGFace2 [2] (3.3M faces) are small compared to proprietary databases such as the dataset used to train FaceNet [3] (~150M faces).

The generation of synthetic faces has made huge leaps forward in the past couple of years, notably the style based architecture of StyleGAN [4, 5] delivers high quality faces. With conditional generation, generative models can create variations upon these synthetic identities by controlling the output. In the work of Colbois, Freitas Pereira, and Marcel [6] variations of identities can be generated in an automatic manner using StyleGAN2. A benefit of their exploit method is that it can be done automatically and no additional training or networks are needed.

Meanwhile a new machine learning type called transformers was developed in the natural language processing (NLP) field [7]. The transformer utilizes the attention mechanism to enable interaction amongst each input element on a global scale. Unlike of a local interaction associated with the convolution operation, found in a.o. StyleGAN.

The GANformer by Hudson and Zitnick [8] is a hybrid generative image model, based on the style based architecture of StyleGAN while incorporating



Fig. 1: Cherry picked examples of smile augmentations on neutral faces using the GANformer.

transformers. Like many other transformer based works it is unconditioned. Even so, the authors show additional outputs in the form of attention maps with segmenting behaviour. Unfortunately this is not shown in the case of face generation, while the additional segmentation information can yield a multi-purpose database. This makes it an interesting candidate to explore further for the sake of the creation of synthetic databases.

In this work the GANformer is explored and exploited to gain a broader set of functions than the face generator is trained for. Our main research question is: *To what extent can the GANformer be used for synthetic face database generation?* This will be answered using three additional sub-questions:

- To what extent can we interpret the attention in the synthesis network as a semantic segmentation of the face?
- To what extent can we reconstruct existing identities from the latent space of the GANformer?
- To what extent can we control the smile expression while maintaining the same identity?

II. RELATED WORK

A. Exploitation

One control method is exploitation. It has two key ingredients: (1) projection that finds a latent vector that yields a similar image and (2) manipulation in which small changes in the latent space correspond to small semantic changes within the same identity.

Shen et al. [9] showed that semantic attributes are linearly separable in W . After generated faces are classified, the authors fit a linear support vector machine

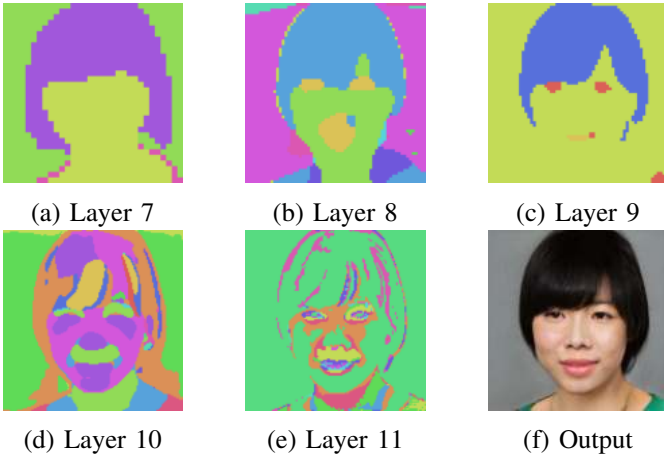


Fig. 2: Examples of the attention maps for one generated face using the default model. The rightmost bottom figure is the resulting face, layer 7 - 11 resemble a facial structure. Note that the resolution increases at higher layers.

(SVM) to acquired latent directions that provide control over the attributes. Colbois, Freitas Pereira, and Marcel [6] improves this method by using the labeled dataset Multi-PIE [10], containing 337 identities under 15 view points, 19 illumination conditions with 6 different facial expressions. Figure 7 shows an example of aligned faces. As it is based on real faces, the projected identities incorporate a scale that describes the local range of an identity within the latent space. The GANformer architecture is based on StyleGAN, which makes the exploitation a viable solution to gain control. This averts the resource intensive adjusting and training of a new model.

B. GANformer

In another work the GANformer is proposed by Hudson and Zitnick [8], a StyleGAN adaptation with bipartite attention. In bipartite attention, attention is applied between two disjoint sets. The intermediate latent vector w is broken down into m latent components. With the use of bipartite attention, the style information is propagated to the n image features. Each latent component can model long range spatial interactions to guide the synthesis process.

III. ATTENTION AND SEGMENTATION

This section will focus on answering the first sub-question: *To what extent can we interpret the attention in the synthesis network as a semantic segmentation of the face?* To answer this question, the segmentation of the attention maps are analysed. Besides that, additional models with varying parameters will be trained from scratch. An example of the attention maps is shown in Figure 2.

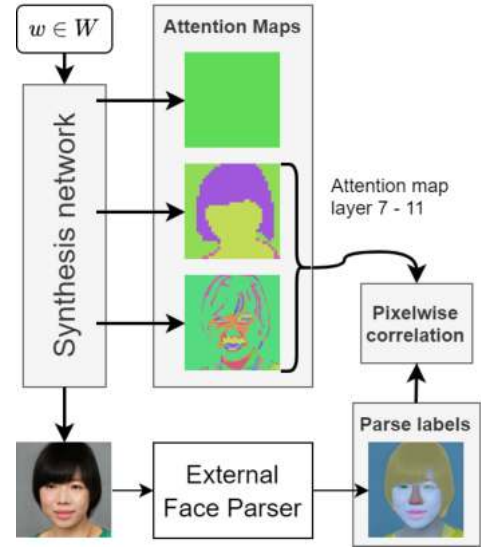


Fig. 3: The approach for inspecting semantic segmentation in attention maps, which is exported in each attention layer. The correlation between the parse labels and each latent component is determined. Only the layers showing facial traits are used.

A. Methods

1) Segmentation

A qualitative analysis will investigate whether segmented facial traits are present within the attention maps. In addition, the correlation is determined between the location of each active latent component and parse labels which are determined by a face parser [11]. Figure 3 shows the approach.

2) Additional Models

To determine the robustness of the segmentation, additional models are used. By retraining a model, its repeatability on the segmentation is investigated. Moreover models with varying number of latent components and their dimensions are trained, to study the effect on the attention operation. These parameters have a direct effect on the attention computation.

B. Experiments and Results

A pre-trained model is provided in [12], this will be referred to as the default model. It should be noted that the model parameters of this model are different with regard to the model as described in the GANformer paper [8].

1) Default model

With the default model 1000 faces and their corresponding attention maps were generated. The first 100 were used in the qualitative analysis. For the correlation between the latent components and parse labels the whole set of 1000 samples was used. The attention maps of layer 1 to 6 do not suggest any segmentation of facial traits, while these are seen from layer 7 onward. Therefore correlation between the active latent components

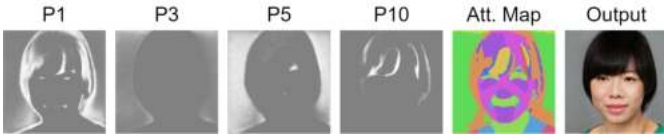


Fig. 4: The probability map for some latent components for attention layer 10. Each P_i indicates the probability map for that layer component.

and the parse labels was only determined from layer 7 until layer 11.

The attention maps from layer 7 onward can be roughly divided into two groups. In layer 7, 8 and 9, as shown in Figures 2a, 2b and 2c, only a few latent components seem to be active that each attend to segments of the face. The skin, hair, eyes and mouth are noticeable as segments. In the highest layers 10 and 11 the attention map seem to focus more on details, in line with the observation of [8].

Overall, the segmented facial traits are not perfect. In some cases they are combined with other facial traits in one latent component, making it hard to extract the correct information. The segmentation can be improved by combining the information of latent components, such as taking the separation of background and skin in layer 7, but using the detail of the hair and eyes from layer 9. Another option is to use the raw probability maps of each latent component, an example is shown in Figure 4.

2) Additional models

As the default model suggests an opportunity for segmentation, the additional models were (close) variants of this model. The training algorithm was kept at default as provided in [12], except for the varying model parameters. The models were trained on the cropped and aligned FFHQ database [4] at a resolution of 256x256. The general face quality is determined using Fréchet Inception Distance [13], a common metric which compares distribution between the 50000 samples of training data and the generated data. A lower FID describes a higher quality generation.

a) Repeatability

For the repeatability of the results three models with the default parameters (16 latent components with a dimension of 32) were trained for about 1 GPU week on about 2500k steps. Their FIDs were respectively 12.2, 12.6 and 12.9, indicating that retraining results in a similar general face quality.

The attention shows a similar behaviour, latent components attend in a holistic manner onto the image features.

It might be that the default model is trained for deviating parameters, since the three trained models are highly similar, while the model parameters are the same.

TABLE I: FID of each trained model variant at about 2500k steps with the respective number of latent components and their dimension. For the models trained for the repeatability the mean is displayed.

FID	Latent Dimension			
	32	16	12	8
# Latent Components	32	/	14.9	20.3
	16	12.6	15.9	19.5
	12	12.5	16.0	/
	8	12.4	/	/

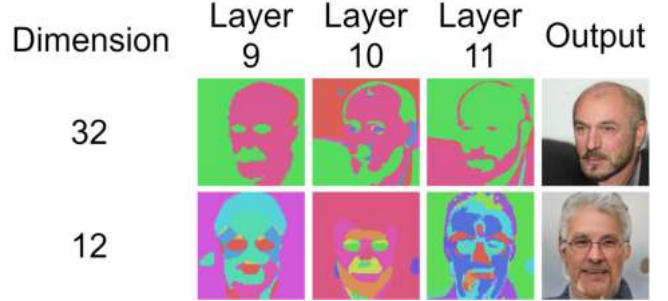


Fig. 5: Example how the latent dimension influences the number of active latent components and thus the segmentation present.

With this assumption, the process does result in similar attention behaviour. This may suggest that with knowing the training parameters of the default model, its highly informative attention can be acquired in a robust manner.

b) Varying Model Parameters

To study the effect of varying model parameters, eight variants were trained as well on about 2500k steps. The resulting FIDs for the trained models are shown in Table I. The dimension of the latent components seems to have the most significant influence on the quality of the generated faces, a higher dimension seems to be beneficial for the facial quality.

There is a clear distinction between models with $d = 32$, versus a lower dimension of $d = [12, 16]$. An example is shown in Figure 5. In the high dimensional models only a small number of latent components is active throughout the layers, attending in a holistic manner on the face. On the contrary the attention maps of $d = [12, 16]$ seem to have more active latent components in each layer, which provide a higher level of semantic segmentation. None of the models seem to provide the level of segmentation information of the default model.

The many active components in the $d = [12, 16]$ models are mandatory, as the same level of detail of the $d = 32$ models has to be described within more latent components, due to a smaller embedding dimension. The results of the training in Table I supports this, as a smaller dimension seems to negatively impact the generation quality in terms of FID.

C. Conclusion on Attention Maps

The attention mechanism does not provide a direct means for segmentation, the attention layers are optimized to fool the discriminator, not to function as a segmentation tool. Nevertheless the default model does show segmented facial traits within several layers, especially the background, the skin and hair have high correlations.

IV. SEMANTIC CONTROL

In this section the method as presented by [6] is used. An overview of the process is shown in Figure 6. The process for synthetic identity generation, as used in this work, consists out of three parts:

- 1) Expression faces of the Multi-PIE dataset [10] are projected into the latent space to acquire labelled latent vectors.
- 2) Using the labeled data for the each neutral-expression pair, the corresponding latent directions are computed.
- 3) Reference faces are created using random generated w latent variables, the faces are neutralized with regard of their expression. Augmented faces are determined by moving the reference face in the direction of the computed latent directions.

Since a projector has not been implemented on the GANformer, research is done to answer the sub-question: *To what extend can we reconstruct existing identities from the latent space of the GANformer?* Using this data the third sub-question will be answered: *To what extend can we control the smile expression while maintaining the same identity?*

A. Methods

1) Projection

The GANformer is not provided with a projector like the one implemented in StyleGAN2 [5]. However since the GANformer is also a style-based architecture, the StyleGAN2 projector was used as a base.

a) Subspace

It appeared that $W_{face} \subset W$ such that W_{face} describes faces, but the base projector was unable to retain the faces within this subspace. On the other hand, the mapping network is able to map random vectors $z \rightarrow w \in W_{face}$. It was found out that W_{face} can be roughly approximated, therefore an additional loss based on the Mahalanobis distance was added to regularize the projected latent w_p , as shown in Equation (2).

The Mahalanobis distance was implemented such that it determined the distance of the projected vector w_p to the distribution of the subspace, based on the mean μ_m and its covariance of 10000 mapped latents, as shown in Equation (1). The inverse covariance matrix S_m^{-1} will

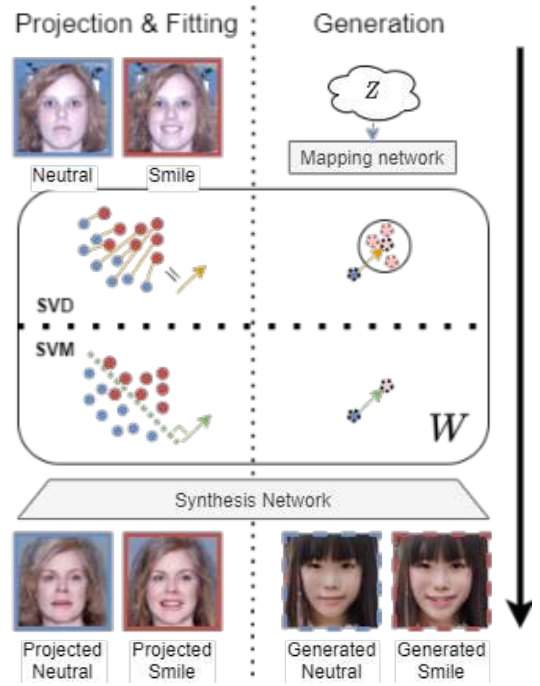


Fig. 6: The process to gain control over the latent space. Real faces are projected into the latent space, using either SVD or SVM the latent direction can be determined to augment sampled faces. Inspired by [6].

scale the loss inversely proportional to the scale of the approximated distribution.

$$D_M(w_p) = \sqrt{(w_p - \mu_m)^T S_m^{-1} (w_p - \mu_m)} \quad (1)$$

$$L_M = a * D_M + b \quad (2)$$

where $a = a_w * \frac{t}{T}$

b) Projection of Real Faces

With a working projector real faces can be projected that serve as training data for the latent directions. For the projection of real faces, it is important that the difference between the projected neutral and attribute faces describe only that certain attribute, to acquire disentangled latent directions. Therefore the projected faces within an identity must have a similar identity.

The quality of the projected faces are validated using FaceVACS 9.6, where $0.5 = 0.1\%$ FAR. The score between aligned and projected pairs, describe the performance of the projector and the latent spaces completeness. Whereas the scores between faces in an identity describe the consistency of the projected faces and their value as training data for the latent directions.

For benchmark purposes the method is applied on StyleGAN2 as well. Note that this model is trained from 3x to 14x longer than the GANformer model.

2) Latent Directions and Exploration

The latent of the projected faces can be used to explore the latent space and as a training set to deter-

mine the latent directions. SVD is used for both the exploration and finding latent directions, while a linear SVM is used solely to find the latent directions.

$$U, S, V = \text{SVD} \left(\frac{X - \mu_m}{\sqrt{\dim(X) - 1}} \right) \quad (3)$$

$$L \sim N(0, 1)$$

$$w = USL + \mu_m$$

The classes within the latent space of the GAN-former are not linearly separable. The SVD is used as a low dimensional manifold to describe changes between neutral and specific expressions. The first step all pairwise vectors are determined, that is $w_{i,neutral} - w_{i,expression}$. Then SVD is applied on these vectors, as shown in Equation (3), where X are the vectors and μ_m the mean of those vectors. By sampling L from a standard normal distribution, multiple direction vectors are generated. These can be added to the reference faces to find a suitable expression variation. As additional parameters the number of singular components can be adjusted to acquire a more or less specific movement and the resulting sample vectors of USL can be scaled with a scalar. The multiple samples show variations around the expression acquired by moving the neutral latent with the mean.

In the SVM method, to goal is to fit a linear SVM as a hyperplane between the neutral and the expression class. The normal onto this hyperplane describes the direction between the neutral and expression. The mean of the distance between both classified populations to the hyperplane, reflects the scale as in how much variation can be applied while preserving the identity.

3) Generation of Synthetic Identities

The generation of synthetic identities is done in two subsequent steps, generate reference faces and adding augmentations. The reference faces are sampled by generating faces from Z , which return its mapped w vector and the face itself. Neutralization is done by moving the sampled latent towards the neutral direction along the neutral smile vector, as done in [6]. Duplicate faces are prevented by requiring a minimum embedding distance of the faces using a pre-trained Inception-Resnet v2 model.

The second part consists out of generating the augmented identities. The SVD method samples direction vectors while varying the number of singular components as mentioned before. For the SVM method each attribute face is determined by adding the mean of the latent direction, normal to the found hyperplane.

B. Experiments and Results

The default model as referred to Section III-B is used for this section as well.

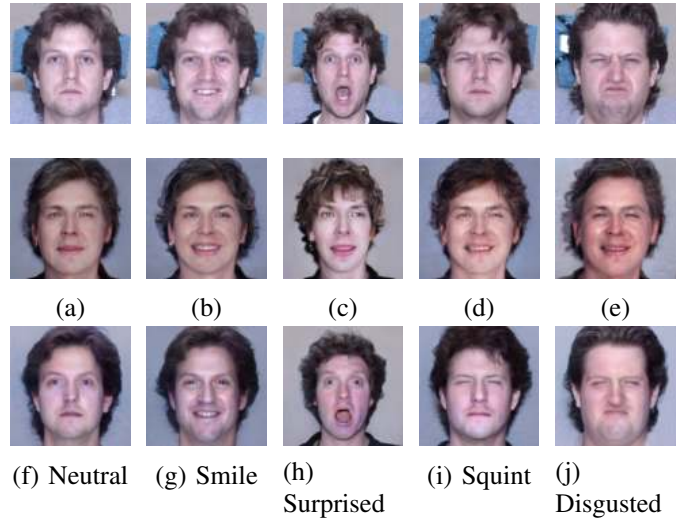


Fig. 7: Example of one aligned (upper) and projected (GANformer middle, StyleGAN2 bottom) identity with a neutral face and various expressions.

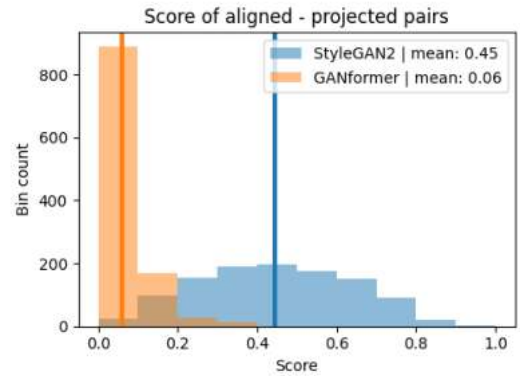


Fig. 8: The FaceVACS score distribution of the aligned - projected pairs using the GANformer and StyleGAN2.

1) Projection of Multi-PIE Faces

The projection of the expression dataset resulted in 1095 alignment projection pairs with 208 identities ranging from 2 to 8 expressions divided over 1 to 4 sessions.

a) Alignment Projection Pairs

The FaceVACS scores of the alignment and projected pairs are shown in Figure 8, all the pairs are regarded as non-mated. A projected identity is shown in Figure 7.

Only the neutral and smile expression seems to be successfully projected in most cases. The model seems to be unable to project open mouths and subtle details as found in other expressions, which might be due to underrepresented expressions in the training data.

While the projection of generated faces was very successful, the projection of the Multi-PIE expression faces under performs. The projection of generated faces is a more trivial task as the optimal solution does exist somewhere in the latent space. This does show that the latent space of the GANformer has a rather low

variability in faces it can generate. The next sections will look specifically at the smile expression. As the latents of the projected faces are the training data for the latent directions and the majority of the expressions but smile is not correctly projected.

b) Within Projected Identities

For the latent direction to be disentangled, the neutral smile pairs need to be similar in identity. Note that this is not a metric to assess the quality of the expression itself, in some cases a smile face looks very neutral and results in a high FaceVACS score. The FaceVACS scores of the projected neutral - smile pairs shows a left-skewed distribution with a mean of 0.86. It is noticed that the variations of the subjects of the sessions such as hairstyle can have a major impact on the resulting face. Note that the aligned expression faces have a high similarity with a mean of 0.990, despite the variation in expressions.

c) StyleGAN2

The projections of StyleGAN2 seem to be much more similar to the aligned faces, as shown in Figures 7 and 8. Nevertheless the majority is still considered as non-mated. The score distribution of the projections within the identities is similar that of GANformer, with a mean of 0.86.

2) Latent Space Analysis and Generating Synthetic Identities

a) SVD

The SVD method was used on the GANformer to analyse the latent space around the face, moved with the mean neutral smile vector. The neutral smile pairs with various thresholds on their FaceVACS score were used to determine the relevant SVD parameters. In all cases the mean vector did not seem to transform the reference face to a smiling face, neither was adding singular components showing clear changes towards smiling. Instead, by adding additional singular components the face decayed quickly, as shown in Figure 9.

For StyleGAN2 the unfiltered mean vector was used, which did seem to represent the smile direction. The added singular components augmented attributes such as hair style and skin colour, as shown in Figure 9. This variation is likely due to the orthogonal property of the SVD. The latent space of StyleGAN is linearly separable, therefore any other direction induced by the multiple neutral-smile vectors acts on other linearly separable attributes.

The contrasting results between the models support the fact that the latent space of StyleGAN2 is better described. This is something that is seen throughout this method. As the GANformer needs an additional loss to retain the projector within W_{face} . In addition to that the lack of completeness is shown with the fact that all but neutral and smile are not projected correctly. It is expected that with longer training the latent space will be more fully described.

TABLE II: The mean FaceVACS score of 100 generated neutral smile pairs per scale for each model

Scale	0.5	1.0	2.0	5.0
GANformer	0.99	0.98	0.96	0.77
StyleGAN2	0.97	0.95	0.89	0.37

b) SVM

In a linearly separable latent space, fitting a linear SVM between the projected neutral and smile latents, the normal onto the hyperplane describes the neutral - smile latent direction. Finding a working latent direction by filtering the latents was not trivial. A proper filter was implemented by removing latents based on their FaceVACS entry if their score was $s < 0.9$, resulting in a fitting accuracy of 0.92.

The latent direction did seem to be oriented in the neutral smile direction, causing smiles on neutral faces, Figure 10 shows an example. In general the identities are kept, but the neutralisation was not always successful. In addition to this, latent direction is not completely disentangled, the pose, hair color, eye direction, appearance of glasses and teeth structure changes over the augmentations. It should be noted that in some instances, the latent direction did not change the expression at all.

The linear SVM on unfiltered projected StyleGAN2 latents was fitted perfectly and resulted in a representative latent direction, as shown in Figure 10. In contrast to the GANformer, the neutralisation did work on all samples. Like the GANformer, the latent direction was not completely free of entanglement and male faces got more feminine towards the smiling direction. It is noted that the reference faces are closer to the smile than the neutral face in the SVD method, as in SVM mean distance from hyperplane is taken, rather than the distance between the two populations in the SVD method.

Table II show the mean FaceVACS score between the neutral and scaled smile faces for both models. While the GANformer shows a higher similarity, the actual variety in smile is smaller than in StyleGAN2. A higher scale is needed for the same variation in smile. This small augmentation is likely due to the scale acquired during the training of the latent direction. Some projected neutral faces have slight smiles and while some projected smile faces are very similar to the neutral faces. Therefore the populations are closer to each other and the inherent scale too small. While the filter filters deviating identities to encourage disentangled data, this does not guarantee a well defined neutral and smile pair in terms of expression. In fact, it may even encourage pairs that are too similar. Because of this, a higher scale for the neutralization is needed as well, examples are shown in Figure 11.

The neutral smile latent direction of the GANformer

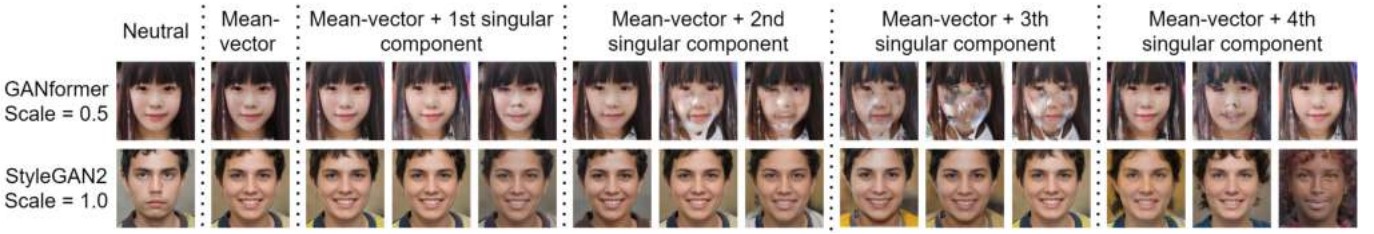


Fig. 9: The results of the SVD generation on one identity for both models. The augmentations are done on the reference face using the mean vector and additional sampled singular components. The upper row use the GANformer where the transformation with vector USL is scaled with 0.5. The bottom row uses StyleGAN2 and has a scaling of 1.0.

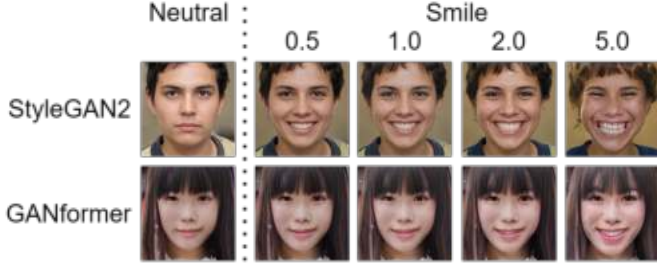


Fig. 10: The results of the SVM generation on one identity for both models.

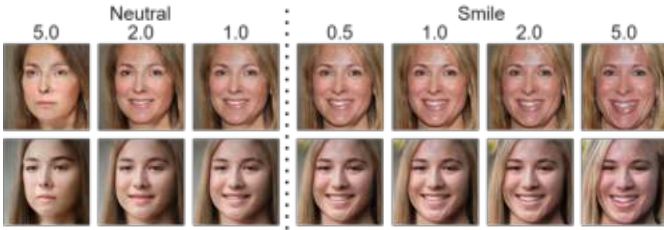


Fig. 11: Effect of scaling the the distance for both neutralisation and the smiling attribute on two generated identities using the GANformer.

is not completely disentangled. One cause can be the that the latent space has a limited separability and requires more training. In addition to that, it may be that the found latent direction is not optimal. As noted finding a latent direction is not trivial, it is very sensitive to the selection neutral smile latents.

The fact that a very specific set is needed is a downside of the projection method. This method needs to provide reliable results, such that the training set for the SVM consists out of representative data. As a recommendation for future research to improve this method, a system that classifies the magnitude of the smile and neutral expressions should be added. This can advance this work in two directions. First, the current training set is based on similar identities, but this still allows mislabeled faces. The classifier may serve as an extra quality control for a better latent direction. Second, the current evaluation is done qualitatively and with

the use of FaceVACS. As shown some generated smile and neutral faces are mislabeled. With the classifier the expressions of the generated faces and the effect of the scaling can be quantized, which leads in turn to a better comparison between other models such as StyleGAN2.

To improve the separability of the latent space, the model should be trained for more steps. This will also improve the representation of under represented expressions in the latent space, such as scream and disgust.

C. Conclusion on Semantic Control

The first goal of this section was to evaluate whether existing identities can be reconstructed from the latent space of the GANformer. The projector on the current model needs a regularization term, to retain the projected latent in the subspace of faces, W_{face} . The FaceVACS verification shows that none of the existing projected pairs have the same identity. Nevertheless most neutral and smile expressions are projected and the majority of the projected faces within an identity do have the same identity. Better projections can be acquired by more training, providing a more versatile latent space.

The second objective was to investigate to what extent the smile expression can be controlled while maintaining the same identity. It is shown that projected latents are noisy and need to be filtered. While the SVD method works on StyleGAN2, neither the mean vector and added singular components can construct smiling faces in the GANformer. The variations by adding the orthogonal singular components emphasizes the linear separability and high descriptiveness of the StyleGAN2 latent space, while the lack of in the used GANformer model.

The SVM method is, with a specific subset of projected latents, able to find a latent direction that controls the neutral smile attributes. The scale is inherently small due to the training set. Therefore a larger scale is needed to find similar degree of change in expression as found in StyleGAN2. The found latent direction is not completely disentangled. The latent direction is likely not optimal, in addition to that the latent space is only linearly

separable to a certain extent. In some cases the latent direction does not control the smile expression.

Two suggestions are provided. A classifier should be used to classify the magnitude of the projected and generated expressions, this improves the filtering and makes the evaluation and comparison more explicit. In addition to that, it is argued that the shortcomings concerning the various expressions and entanglement are mostly due to the lack of training. With further training the latent space will likely head towards the descriptiveness and disentanglement of the fully trained latent space of StyleGAN2.

V. CONCLUSION

In this work the GANformer model is explored for two uses in creating synthetic face databases, without the need of training the model for the specific applications, but general face synthesis instead.

First the attention is investigated on the use of segmentation. This unique property makes this model beneficial to use over well known models such as StyleGAN2. The results show segmenting behaviour, though more work is needed to put this into practice. Suggestions for future work are to use multiple layers and probability maps and to fine tuning model and training parameters.

With augmentation multiple faces of the same identity can be created, this requires generation based on a condition. Using the reconstruction of faces to find latent directions, it is seen that some control over the neutral smile direction is gained. It is suggested to include a expression classifier to improve and evaluate the process. In addition to that the model should be trained longer for a higher descriptiveness to include other expression and to achieve a higher level of separability.

In both the segmentation and the smile augmentation cases compelling results are shown and indicate the possibilities to use the GANformer for multiple applications in synthetic face database generation. However further work is needed in both objectives to acquire working solutions and to create synthetic face databases.

REFERENCES

- [1] Chen Sun et al. "Revisiting Unreasonable Effectiveness of Data in Deep Learning Era". In: *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*. Oct. 2017.
- [2] Qiong Cao et al. "VGGFace2: A Dataset for Recognising Faces across Pose and Age". In: *2018 13th IEEE International Conference on Automatic Face Gesture Recognition (FG 2018)*. 2018, pp. 67–74. DOI: 10.1109/FG.2018.00020.
- [3] Florian Schroff, Dmitry Kalenichenko, and James Philbin. "FaceNet: A Unified Embedding for Face Recognition and Clustering". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. June 2015.
- [4] Tero Karras, Samuli Laine, and Timo Aila. "A Style-Based Generator Architecture for Generative Adversarial Networks". In: *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 2019, pp. 4396–4405. DOI: 10.1109/CVPR.2019.00453. URL: <https://ieeexplore.ieee.org/document/8953766>.
- [5] Tero Karras et al. "Analyzing and Improving the Image Quality of StyleGAN". In: *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 2020, pp. 8107–8116. DOI: 10.1109/CVPR42600.2020.00813. URL: <https://ieeexplore.ieee.org/document/9156570>.
- [6] Laurent Colbois, Tiago de Freitas Pereira, and Sébastien Marcel. "On the use of automatically generated synthetic image datasets for benchmarking face recognition". In: *2021 IEEE International Joint Conference on Biometrics (IJCB)*. 2021, pp. 1–8. DOI: 10.1109/IJCB52358.2021.9484363.
- [7] Ashish Vaswani et al. "Attention Is All You Need". In: *CoRR* abs/1706.03762 (2017). URL: <http://arxiv.org/abs/1706.03762>.
- [8] Drew A. Hudson and C. Lawrence Zitnick. "Generative Adversarial Transformers". In: *CoRR* abs/2103.01209 (2021). URL: <https://arxiv.org/abs/2103.01209>.
- [9] Yujun Shen et al. "Interpreting the Latent Space of GANs for Semantic Face Editing". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. June 2020.
- [10] Ralph Gross et al. "Multi-PIE". In: *2008 8th IEEE International Conference on Automatic Face Gesture Recognition*. 2008, pp. 1–8. DOI: 10.1109/AFGR.2008.4813399.
- [11] shaoanlu. *Face Toolbox Keras*. URL: https://github.com/shaoanlu/face_toolbox_keras.
- [12] Drew Arad Hudson. *gansformer*. URL: <https://github.com/dorad/gansformer/tree/3c0bcdee049d82318cb2f9327c8d6c7808664cd2>.
- [13] Martin Heusel et al. "GANs Trained by a Two Time-Scale Update Rule Converge to a Nash Equilibrium". In: *CoRR* abs/1706.08500 (2017). URL: <http://arxiv.org/abs/1706.08500>.

Grant-Free Random Access in Massive MIMO for Static Low-Power IoT Nodes

Gilles Callebaut, Liesbet Van der Perre and François Rottenberg
 KU Leuven, ESAT-WaveCore, Ghent Technology Campus, 9000 Ghent, Belgium
 E-mail: gilles.callebaut@kuleuven.be

Abstract—Massive MIMO is a promising technology to enable a massive number of Internet of Things nodes to transmit short and sporadic data bursts at low power. In conventional cellular networks, devices use a grant-based random access scheme to initiate communications. This scheme relies on a limited set of orthogonal preambles, which simplify signal processing operations at network access points. However, it is not well suited for Internet of Things (IoT) devices due to: (i) the large protocol overhead, and (ii) the high probability of collision. In contrast to the grant-based scheme, a grant-free approach uses user-specific preambles and has a small overhead, at the expense of more complexity at access points. In this work, a grant-free method is proposed, applicable for both co-located and cell-free deployments. The method has a closed form solution, which results in a significantly lower complexity with respect to the state-of-the-art. The algorithm exploits the static nature of IoT devices through the use of prior channel state information. With a power budget of 1 mW, 6 antennas are sufficient to support 1000 nodes with 200 simultaneous access requests with a probability of false alarm and miss detection below 10^{-6} and 10^{-4} , respectively.

Index Terms—cell-free, grant-free, initial access, internet-of-things, massive mimo, random access

I. INTRODUCTION

In IoT networks, a high number of devices are connected. However, only a handful of these devices are active at the same time, resulting in sporadic uplink transmissions. In order to serve these nodes, the active devices need to be detected, prior to decoding the data. Due to this sporadic traffic and the high number of IoT devices, allocating orthogonal preambles to these devices would incur an unacceptable overhead. As the network is unable to predict when these devices are active, an adequate initial access scheme needs to be implemented. The specificities of massive IoT, i.e., energy-limited, uplink focused, and low-payload size transmissions, call for a tailored initial access scheme.

Several multiple access techniques have been proposed for massive IoT [1–5]. These techniques follow a grant-based or grant-free approach, as illustrated in Fig. 1a and 1b, respectively. In the former, the devices request access to the network, prior to the communication. This is commonly done by competing for a dedicated orthogonal pilot sequence. In the latter approach, the devices are not required to request access and other approaches to mitigate and resolve potential collisions are implemented. An overview of different techniques can be found in literature [6, 7].

The project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 101013425.

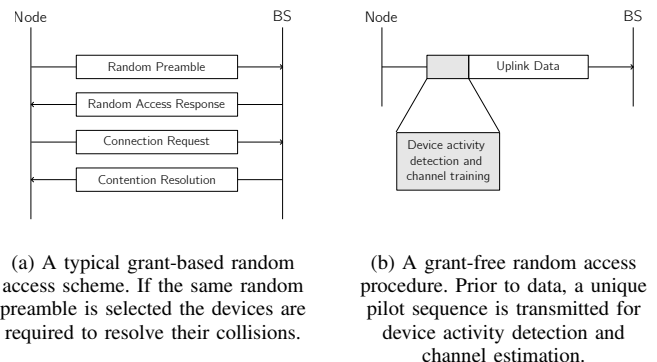


Fig. 1: Grant-based and grant-free random access mechanisms.

Grant-based random access. Based on the random access protocol used in long term evolution (LTE), Björnson et al. [8] propose the strongest-user collision resolution (SUCRe) protocol, illustrated in Fig. 1a. Each active device requests a dedicated and unique orthogonal pilot by transmitting a random access pilot, with the possibility of using the same pilot as another contending device. The base station estimates the channel to each user based on the received pilots, after which it responds with orthogonal precoded downlink pilot signals, corresponding to the used pilots in the uplink. In case multiple devices have used the same pilot, the downlink signal is multicasted in a maximum ratio transmission fashion towards these devices, causing the expected received signal strength to be lower than expected. The (average) expected signal strength can be determined at the device side thanks to the channel hardening effect experienced in massive MIMO. Each device can, hence, detect whether a collision occurred. In this protocol, the strongest user is considered the winner and is scheduled for communication using a dedicated and unique pilots sequence. Other work has extended this technique by introducing, a.o., a higher fairness among the contenders [9, 10].

Grant-free random access. In contrast to the grant-based random access, in a grant-free scheme, the devices use preassigned pilot sequences [11]. As shown in Fig. 1b, by skipping the grant request and collision resolution, both the pilot and data are sent in a single step. As mentioned earlier, the disadvantage of this approach is that it is not possible to utilize orthogonal pilots because the number of devices is much larger than the preamble length, i.e., $K \gg \tau_p$. The challenge in grant-free random access

is device activity detection. Taking advantage of the sparse nature of the activity of the devices, different algorithms have been proposed to tackle this challenge through compressed sensing techniques [12–15]. These algorithms perform well because of the high number of access point (AP) antennas in massive MIMO, facilitating device detection in massive IoT networks.

Fengler et al. [16, 17] study the performance of several estimators to detect the active devices for a co-located massive MIMO system. In [18, 19], this work is extended to the cell-free case by considering different large-scale fading coefficients per AP. They, however, were unable to directly use the proposed algorithm of [17] and had to consider only the contribution of the most dominant AP.

In this work, we consider the generic case where devices are not scheduled, and they transmit whenever needed, i.e., they are uplink-centric. As in conventional systems, we consider that all devices are time synchronized and work in a time slotted fashion. This can be easily achieved through downlink synchronization reference signals. Because of the large number of devices, providing orthogonal preambles to each user would generate a too large pilot overhead, i.e., pilots of length K . In this algorithm, a unique but non-orthogonal preamble is randomly generated and assigned to each user. Similar to key distribution in conventional low-power wide-area network (LPWAN), this sequence is known by both the network and the device, and is easy to implement. Based on prior channel state information (CSI), the active devices are detected. In case both the IoT node and APs are static, i.e., immobile, the channel response will be static in time as long as the environment is static as well. Hence, we can expect that the previously estimated CSI can be used for a longer time period than assumed in literature [20], given the static nature of the devices.

The proposed approach has a lower complexity than the techniques reported in literature. Our algorithm is evaluated through numerical simulations. Next to conventional massive MIMO, i.e., co-located massive MIMO, a cell-free deployment is included in the investigation.

Notations: vectors are denoted by boldface lower case \mathbf{x} and matrices by boldface capital letters \mathbf{X} . The superscript $(\cdot)^T$ is used to denote the conjugate transpose operation. The absolute value is denoted by $|\cdot|$. The Kronecker product is denoted by \otimes . The notation $\mathbb{E}\{\cdot\}$ denotes the expectation of a random variable. The set of complex numbers is denoted by the symbol \mathbb{C} . The uniform distribution bounded by the closed interval between a and b is denoted by $[a, b]$. The complex normal and normal distribution with mean μ , standard deviation σ and covariance matrix Σ is denoted by $\mathcal{CN}(\mu, \Sigma)$, respectively. The identity matrix \mathbf{I}_n is a $n \times n$ square matrix with ones on the main diagonal and zeros elsewhere.

II. MOTIVATION – RECURRENCE IN CSI

IoT – and more specifically LPWAN – technologies are often put in the field with a deploy-and-forget strategy, where the devices remain immobile afterwards. As such, we can expect

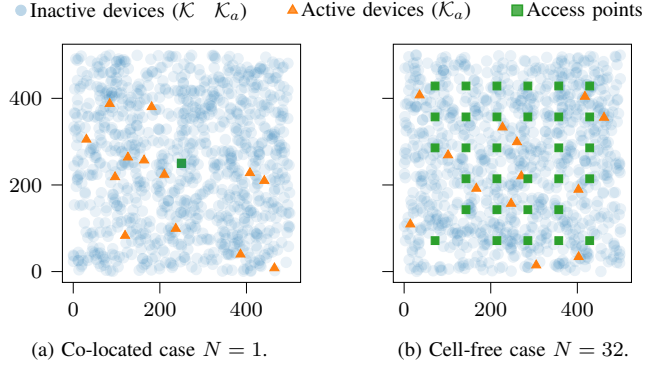


Fig. 2: Example of a simulation scenario with an area of $500 \times 500 \text{ m}^2$ for the case of 32 total base station antennas for a co-located (a) and cell-free (b) deployment.

that the channel conditions are less time-variant than assumed in theoretical models often assumed in literature [20, 21]. To investigate the long-term behavior of the channel, a uniform linear array (ULA), described in [22], is used to estimate the channel of two static IoT nodes, shown in Fig. 3, over a time period of more than 8 hours. This measurement campaign represents a typical IoT scenario where the base station or gateway is located at an elevated height and the IoT devices are fixed in place. As shown in Fig. 3b, during the experiment, movement in the proximity of the nodes is present. Furthermore, the line-of-sight (LoS) was sometimes blocked due to cars passing by, as would be the case in real deployments.



(a) ULA at the balcony with Node 1 positioned right and Node 2 left.



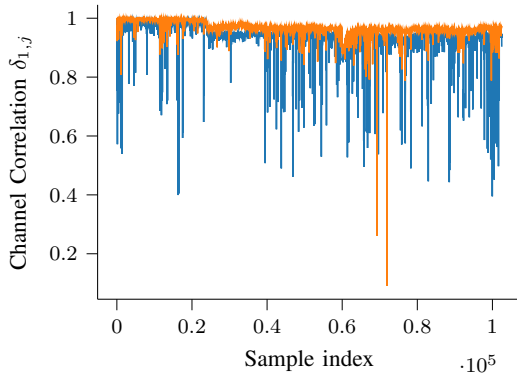
(b) Movement in the proximity of Node 2 during the measurements.

Fig. 3: Measurement setup to study long-term channel behavior.

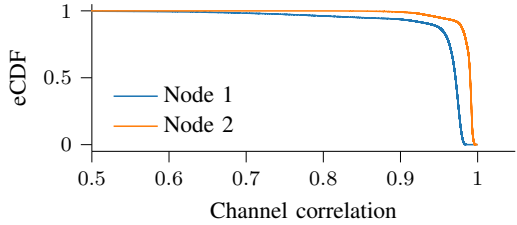
The long-term behavior is measured by taking the channel correlation (Eq. 1) of the first channel estimate and the other channel N measurements, i.e., $\delta_{1,j}$ for $j \in \{1, \dots, N\}$.

$$\delta_{i,j} = \frac{|\bar{\mathbf{h}}_i \cdot \bar{\mathbf{h}}_j|}{\|\bar{\mathbf{h}}_i\| \|\bar{\mathbf{h}}_j\|} \quad (1)$$

The observed channel correlations are depicted in Fig. 4a. The empirical cumulative distribution function (eCDF) of these correlation coefficients is shown in Fig. 4b. Fig. 4a illustrates that most of the time the correlation coefficient is close to 1, indicating that the channel is highly correlated with the first estimate and thus can be considered static. It also shows that, while in some occasions the correlation drops, the channel quickly becomes again highly correlated with the first channel instance. More than 90% of the measured channels¹ have a correlation coefficient higher than 0.9 over a window of more than 8 hours. This demonstrates the potential of re-using channel estimates in IoT contexts.²



(a) Channel correlation with respect to the first channel instance. Although the correlation sporadically drops, the majority of the channel instances are highly correlated, as shown in Fig. 4b.



(b) The eCDF of the channel correlations. It indicates that 91% for Node 1 and 95% for Node 2 of the channel correlations are above 0.9.

Fig. 4: Channel correlation over a full day (9h24-17h48) with over 10 000 channel instances.

III. SYSTEM MODEL

Two deployment strategies, i.e., co-located and cell-free massive MIMO, are considered, as shown in Fig. 2. The former follows the conventional massive MIMO where all antennas are

¹More specifically, 91% and 95% for Node 1 and Node 2, respectively.

²We use here the term “re-using” to indicate that we no longer operate in a block fading model with independent channel realizations. Typically, these blocks are considered in the order of 50 ms.

located in one array, often spaced by half a wavelength. In cell-free systems, APs are geographically distributed over the area equipped with one or more antennas. In our study, we assume single-antenna APs in the cell-free case. In the remainder of the manuscript, we will use the term AP to denote the base station (in the central case).

There are K devices, each trying to access the network with a certain activity probability ϵ_a . To do so, each active device $k \in \mathcal{K}_a$ sends a unique, non-orthogonal preamble of length τ_p , known to the network. The pilot symbol of the preamble sent by device k at pilot symbol t is denoted by $s_{k,t}$. The vector of received symbols at the M antennas of the APs at time t is

$$\mathbf{y}_t = \sum_{k=0}^{K-1} s_{k,t} \gamma_k + \mathbf{w}_t, \quad (2)$$

where $\gamma_k \in \mathbb{C}^{M \times 1}$ is the known prior CSI of device k , γ_k is an unknown complex scalar and $\mathbf{w}_t \in \mathbb{C}^{M \times 1}$ is additive white gaussian noise (AWGN), distributed as $\sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I})$. The unknown complex scalar, $\gamma_k = \sqrt{\rho_k} a_k e^{j\phi_k}$, contains the transmit power ρ_k , device activity $a_k \in \{0, 1\}$ and a potential phase offset ϕ_k . The device-specific phase offset can account for a carrier frequency offset (CFO), where the CFO is considered constant over the preamble duration. By assuming that all M antennas are perfectly synchronized, this offset is only dependent on the device. In case the device is inactive, γ_k will be zero. Defining the matrices of channel vectors and pilot symbols at time t ,

$$\mathbf{D}_t = [\mathbf{0}, \dots, \mathbf{0}] \in \mathbb{C}^{M \times K},$$

$$\mathbf{D}_t = \text{diag}(s_{0,t}, \dots, s_{K-1,t}) \in \mathbb{C}^{K \times K},$$

the received signal at the M base station antennas at time t can be rewritten as

$$\mathbf{y}_t = \mathbf{D}_t \boldsymbol{\gamma} + \mathbf{w} \quad (3)$$

$$(4)$$

The matrix $\mathbf{D}_t \in \mathbb{C}^{M \times K}$ is known at the APs as it consists of the known CSI, γ_k , and the transmitted preamble symbols from the K devices, \mathbf{D}_t . By stacking the τ_p consecutive $\mathbf{y}_t \in \tilde{\mathbf{y}}$, the received signal becomes,

$$\tilde{\mathbf{y}} = \begin{pmatrix} \mathbf{D}_0 \\ \dots \\ \mathbf{D}_{\tau_p-1} \end{pmatrix} \boldsymbol{\gamma} + \tilde{\mathbf{w}} \quad (5)$$

$$\begin{aligned} &= \begin{pmatrix} \mathbf{D}_0 \\ \dots \\ \mathbf{D}_{\tau_p-1} \end{pmatrix} \begin{pmatrix} \mathbf{D}_0 \\ \dots \\ \mathbf{D}_{\tau_p-1} \end{pmatrix} \boldsymbol{\gamma} + \tilde{\mathbf{w}} \\ &= (\mathbf{I}_{\tau_p} \otimes \mathbf{D}) \boldsymbol{\gamma} + \tilde{\mathbf{w}} \\ &= \boldsymbol{\gamma} + \tilde{\mathbf{w}}, \end{aligned}$$

$$\text{where } \mathbf{D} = \begin{pmatrix} \mathbf{D}_0 \\ \dots \\ \mathbf{D}_{\tau_p-1} \end{pmatrix} \text{ and } \mathbf{D} = (\mathbf{I}_{\tau_p} \otimes \mathbf{D}) \in \mathbb{C}^{M \tau_p \times K}.$$

IV. DEVICE ACTIVITY DETECTION

A novel algorithmic solution is proposed to find the active devices. After determining the active devices, conventional detection techniques, e.g., zero forcing (ZF), can be used to separate the devices in the uplink.

As soon as $\tau_p \geq K/M$ and for well-conditioned channels and pilot sequences, the matrix \mathbf{Y} will be of full rank K and γ can be estimated by using a left pseudo inverse,

$$\begin{aligned}\hat{\gamma} &= \left(\mathbf{Y}^H \mathbf{Y} \right)^{-1} \mathbf{Y}^H \tilde{\mathbf{y}} \\ &= \gamma + \left(\mathbf{Y}^H \mathbf{Y} \right)^{-1} \tilde{\mathbf{w}}.\end{aligned}\quad (6)$$

This corresponds to the maximum likelihood estimate. Note that, when $M\tau_p \gg K$, $\mathbf{Y}^H \mathbf{Y}$ is expected to become a diagonal matrix because the device channels and unique preambles will become orthogonal [20]. This can lower the complexity of the inverse operation and allows for distributed processing.

A non-negative activity threshold $\gamma_{th,k}$ is applied for each device k . A device is considered active if $|\hat{\gamma}_k| > \gamma_{th,k}$. We define the real-valued threshold as,

$$\gamma_{th,k} = v\sqrt{\text{SNR}_k}^{-1}, \quad (7)$$

where v is chosen to have a desired probability of false alarm and miss detection performance, as discussed in Section V. The signal-to-noise ratio (SNR) of device k , SNR_k , is $\rho_k \|\mathbf{s}_k\|^2 / \sigma^2$, with σ^2 the noise power.

V. SIMULATION RESULTS

The performance of the proposed scheme is explored for a co-located and a cell-free system. An example of a simulation scenario, with a co-located or cell-free AP deployment, is shown in Fig. 2. The number of APs is denoted by N . The default simulation configurations are summarized in Table I.

TABLE I: Simulation parameter set.

Parameter	Symbol	Default value
Number of devices	K	1000
Number of APs	N	-
Number of total AP antennas	M	-
Area size	A	$500 \times 500 \text{ m}^2$
Device activity probability	ϵ_a	0.01
Transmit power of the device	ρ	1 mW
Bandwidth	B	125 kHz
Thermal noise	σ^2	-122.88 dBm
Path loss	β	urban model[23]
Carrier Frequency	f_c	868 MHz
Pilot sequence	\mathbf{s}_k	$\sim \mathcal{CN}(0, 1)$
Pilot length	τ_p	40 symbols
IoT device height	h_k	1 m to 4 m
AP height	h_{BS}	29 m
Phase offset	ϕ_k	$\sim \mathcal{U}_{[0, 2\pi]}$
Number of simulations	N_{sim}	1000

We consider an area of $500 \times 500 \text{ m}^2$ with 1000 devices. The positions of the devices are randomly generated for each simulation. The locations are kept constant among the different scenarios in order to have a fair comparison. The locations of the access points are generated in order to have, on average, a

uniform distribution of the AP positions, as shown in Fig. 2b. For each simulation, a grid of size \sqrt{N} by \sqrt{N} is generated of which N random positions are selected for the APs. In case there is only one AP, the AP is located in the center.

The device activity profile is generated randomly and independently for each device with a probability $\epsilon_a = 0.01$, meaning that on average 10 devices are active simultaneously. Or equivalently, the devices have an average duty cycle of 1%, which can be considered high [24] for the investigated applications and hence represents a worst-case scenario. A higher number of simultaneously active devices is simulated by increasing the activity probability ϵ_a . All devices use the same transmit power of 1 mW. We assume the same bandwidth as used in long-range wide-area network (LoRaWAN), i.e., 125 kHz, and have adopted the thermal noise floor for a 125 kHz signal, i.e., $\sigma^2 = -122.88 \text{ dBm}$, at the receiver. The channel between AP n and device k is modeled as $h_{k,n} = \sqrt{\beta_{k,n}}h$, with $\beta_{k,n}$ the path loss and h the small-scale fading independently and identically distributed (i.i.d.) $\sim \mathcal{CN}(0, 1)$. The large-scale path loss follows the reported model in [23] for an urban environment operating at 868 MHz, i.e., $\beta_{k,n} = 128.95 + 23.2 \log_{10}(d_{k,n}) + \chi$ dB with $d_{k,n}$ the distance between device k and AP n and χ the shadow fading $\sim \mathcal{N}(0, 7.8)$. For the co-located case, $\beta_{k,n}$ becomes β_k . In the proposed scheme, we consider that the channel is static in time. The pilot sequence is randomly generated from a complex Gaussian distribution $s_k \sim \mathcal{CN}(0, 1)$, and is assumed to be known by all APs. Each device uses a pilot sequence of 40 symbols, respecting the requirement of τ_p being greater than or equal to K/M . A random phase offset $\phi_k \sim [0, 2\pi]$ is generated to simulate a carrier frequency offset (considered time-invariant over the simulation period).

1) *Trading-off the probability of false alarm and miss detection:* The receiver operating characteristic (ROC) is studied based on the probability of miss detection and false alarm. False alarm happens when a device is considered active, while it was actually not transmitting. In contrast, a miss detection occurs if a device was active but is undetected. As in [11], the probability of miss detection is defined as the average ratio of undetected devices to the number of active devices

$$P_{md} = 1 - \mathbb{E} \left\{ \frac{|\mathcal{K}_a \cap \hat{\mathcal{K}}_a|}{|\mathcal{K}_a|} \right\}, \quad (8)$$

where \mathcal{K}_a is the set of active devices and $\hat{\mathcal{K}}_a = \{k | \hat{a}_k = 1, \forall k \in [1, K]\}$ denotes the estimated set of active devices. Note that on average $|\mathcal{K}_a| = K\epsilon_a$. Similarly, the probability of false alarm is the ratio of inactive devices considered active to the number of inactive devices and is given by

$$P_{fa} = \mathbb{E} \left\{ \frac{|\hat{\mathcal{K}}_a \setminus \mathcal{K}_a|}{K - |\mathcal{K}_a|} \right\}. \quad (9)$$

The results presented in Fig. 5, 6, and 7, are scaled to the lowest non-zero probability measurable, which depends on the

number of nodes, active nodes $|\mathcal{K}_a|$ and number of simulations N_{sim} . The minimum obtained probability of miss detection is observed if only one device of all active devices is undetected, i.e., $1/\left(\sum_{i=1}^{N_{\text{sim}}} |\mathcal{K}_{a,i}|\right) \approx 1/(K_a * N_{\text{sim}})$. Equivalently, the lowest false alarm is perceived when only one inactive device is considered active, i.e., $1/\left(KN_{\text{sim}} - \sum_{i=1}^{N_{\text{sim}}} |\mathcal{K}_{a,i}|\right) \approx 1/((K - K_a) * N_{\text{sim}})$. For the default case with 1000 simulations, this becomes on average 10^{-6} and 10^{-4} for the probability of false alarm (P_{fa}) and miss detection (P_{md}), respectively. A trade-off can be made between the two probabilities by varying v in (7). A lower v yields a lower activity threshold, resulting in more devices considered active. This in turn lowers the probability of miss detection, while increasing the probability of generating a false alarm. In the simulations, the parameter v is swept across the range $[10^{-2}, 10^5]$. In the remainder of the manuscript, the optimal threshold v_{opt} is used to denote the choice of v yielding the lowest probability of false alarm and miss detection. Due to the limits imposed by the minimum probabilities observable, there exists a region where no errors of false alarm and miss detection, were observed.

In the following, the impact of varying the device transmit power, area size and activity level on the device detection performance is studied.

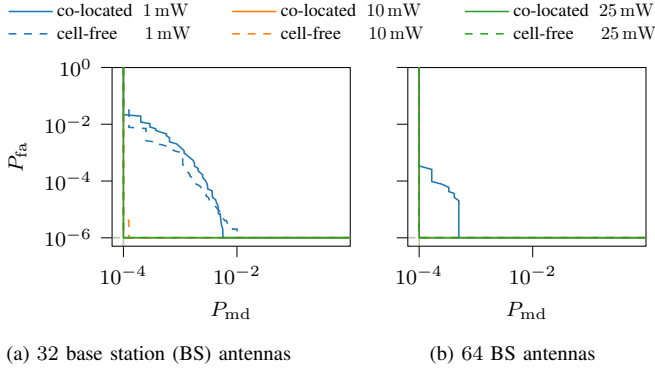


Fig. 5: ROC for 32 and 64 base station antennas for different transmit power. By using only 64 antennas in a cell-free system, the IoT devices can lower their transmit power to 1 mW or 0 dBm.

a) Effect of the transmit power: The impact of the devices' transmit power (1 mW, 10 mW and 25 mW) when using 32 and 64 antennas is shown in Fig. 5. In the case of 128 antennas, no false alarm or miss detection has been observed when using the optimal threshold v_{opt} for all three transmit powers. For both 10 mW and 25 mW transmit power the cell-free and co-located case, even with only 32 antennas, perform optimal. In case of using 1 mW transmit power, 32 antennas show not to be sufficient. As of 64 antennas only in the co-located system, miss detection and false alarm are observed, but the probabilities are reduced by a factor of 100. This demonstrates that the transmit power of IoT devices could be greatly reduced by moving to a cell-free scenario, while still requiring only a limited number of AP antennas.

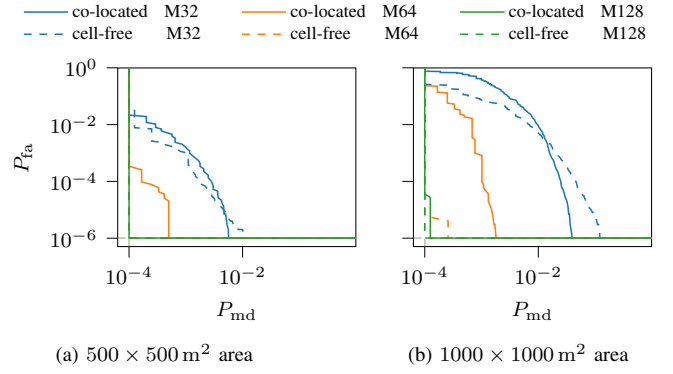


Fig. 6: ROC for a $500 \times 500 \text{ m}^2$ and $1000 \times 1000 \text{ m}^2$ area. The cell-free systems experience a lower performance degradation due to the higher path loss (PL) of the $1000 \times 1000 \text{ m}^2$ area.

b) Effect of the area size: Fig. 6 illustrates the impact of the area size on the performance of the initial access scheme for a 500×500 and a $1000 \times 1000 \text{ m}$ area size. The first obvious effect is the degradation of the SNR due to a higher path loss of the larger area, yielding a decrease in performance for all scenarios. The cell-free system is less affected by the increase in area size, as also observed in [11].

c) Effect of the activity level: Fig. 7 shows the impact of an increase in activity probability from 0.01 to 0.2. The latter implies that, on average, 200 devices simultaneously access the network. Similar to previous observations, the cell-free systems outperform the co-located networks. Despite this, even with 20% of the devices being active on average, the systems using 64 (cell-free) 128 (both cell-free and co-located) AP antennas, do not detect any errors.

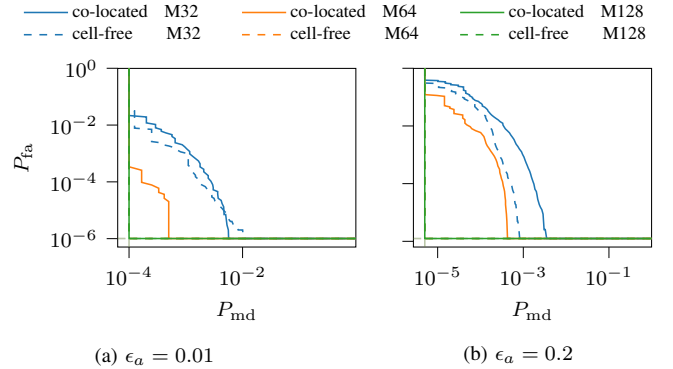


Fig. 7: The co-located system experiences more performance degradation than cell-free systems when increasing the activity probability. Even with 20% of the devices being active, the systems using 6 (cell-free) and 12 (both cell-free and co-located) AP antennas do not detect any errors.³

³Notice that the x-axis is scaled differently as the minimal observable probability of miss detection is lower for the $\epsilon_a = 0.2$ case due to a higher number of active devices, which is on average 200 opposed to 10 for $\epsilon_a = 0.01$.

VI. CONCLUSIONS

A grant-free algorithm is proposed using prior CSI for initial access in massive MIMO networks. It serves as a baseline for the potential of re-using channel state information to support massive and low-power IoT. The initial scheme has a closed form solution, without the need for iterations, is scalable to a large number of devices, and is robust to CFO.

The performance of the proposed algorithm is studied for a conventional co-located and cell-free system. A trade-off between the probability of false alarm and miss detection can be made. The simulation results demonstrate that with only 1 mW of transmit power, 64 base station antennas, deployed in a cell-free setup, will suffice to support a large area (1000×1000 m) and a high number of access requests (up to 200) and still having a probability of false alarm and miss detection below 10^{-6} and 10^{-4} , respectively. Furthermore, the results also indicate that we could greatly reduce the transmit power of IoT devices by moving to a cell-free scenario, while requiring only a limited number of total AP antennas.

In contrast to what is observed in [25], with our algorithm, the performance of a cell-free topology performs better than a co-located case. This is because we are able to exploit the full channel state information and thus also the increase in channel diversity due to the geographical distribution of the APs.

As an extension, the model and algorithm could be adapted to include partial CSI, as opposed to perfectly knowing the full channel state information. In addition, currently, single-antenna APs are considered for the cell-free case. The simulations can be extended by investigating the optimal number of APs for a fixed number of total receive antennas.

REFERENCES

- [1] P. Tuset-Peiro, F. Vazquez-Gallego, J. Alonso-Zarate, L. Alonso, and X. Vilajosana, "LPDQ: A self-scheduled TDMA MAC protocol for one-hop dynamic low-power wireless networks," *Pervasive and Mobile Computing*, vol. 20, pp. 84–99, 2015. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1574119214001576>
- [2] B. Wang, L. Dai, Y. Yuan, and Z. Wang, "Compressive Sensing Based Multi-User Detection for Uplink Grant-Free Non-Orthogonal Multiple Access," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1–5.
- [3] H. Nikopour and H. Baligh, "Sparse code multiple access," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2013, pp. 332–336.
- [4] C. Bockelmann, N. K. Pratas, G. Wunder, S. Saur, M. Navarro, D. Gregoratti, G. Vivier, E. De Carvalho, Y. Ji, C. Stefanovic, P. Popovski, Q. Wang, M. Schellmann, E. Kosmatos, P. Demestichas, M. Raceala-Motoc, P. Jung, S. Stanczak, and A. Dekorsy, "Towards Massive Connectivity Support for Scalable mMTC Communications in 5G Networks," *IEEE Access*, vol. 6, pp. 28 969–28 992, 2018.
- [5] Z. Chen, F. Sahrabi, and W. Yu, "Multi-Cell Sparse Activity Detection for Massive Random Access: Massive MIMO Versus Cooperative MIMO," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4060–4074, 2019.
- [6] A.-S. Bana, E. de Carvalho, B. Soret, T. Abr o, J. C. Marinello, E. G. Larsson, and P. Popovski, "Massive MIMO for Internet of Things (IoT) connectivity," *Physical Communication*, vol. 37, p. 100859, 2019. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1874490719303891>
- [7] E. De Carvalho, E. Bjornson, J. H. Sorensen, P. Popovski, and E. G. Larsson, "Random Access Protocols for Massive MIMO," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 216–222, 2017.
- [8] E. Bjornson, E. de Carvalho, J. H. Sorensen, E. G. Larsson, and P. Popovski, "A Random Access Protocol for Pilot Allocation in Crowded Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2220–2234, Apr. 2017, arXiv: 1604.04248. [Online]. Available: <http://arxiv.org/abs/1604.04248>
- [9] J. C. Marinello and T. Abr o, "Collision Resolution Protocol via Soft Decision Stochastic Retransmission," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–6.
- [10] J. C. Marinello, T. Abr o, R. D. Souza, E. de Carvalho, and P. Popovski, "Achieving Fair Random Access Performance in Massive MIMO Crowded Machine-Type Networks," *IEEE Wireless Communications Letters*, vol. 9, no. 4, pp. 503–507, 2020.
- [11] U. K. Ganesan, E. Bjornson, and E. G. Larsson, "An Algorithm for Grant-Free Random Access in Cell-Free Massive MIMO," in *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2020, pp. 1–5.
- [12] Z. Chen, F. Sahrabi, and W. Yu, "Sparse Activity Detection for Massive Connectivity in Cellular Networks: Multi-Cell Cooperation Vs Large-Scale Antenna Arrays," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2018, pp. 6618–6622.
- [13] L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. de Carvalho, "Sparse Signal Processing for Grant-Free Massive Connectivity: A Future Paradigm for Random Access Protocols in the Internet of Things," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 88–99, 2018.
- [14] M. Ke, Z. Gao, Y. Wu, X. Gao, and R. Schober, "Compressive Sensing-Based Adaptive Active User Detection and Channel Estimation: Massive Access Meets Massive MIMO," *IEEE Transactions on Signal Processing*, vol. 68, pp. 764–779, 2020.
- [15] J. Dong, Y. Shi, and Z. Ding, "Sparse Blind Demixing for Low-latency Signal Recovery in Massive IoT Connectivity," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 4764–4768.
- [16] A. Fengler, S. Haghighatshoar, P. Jung, and G. Caire, "Grant-Free Massive Random Access With a Massive MIMO Receiver," in *2019 53rd Asilomar Conference on Signals, Systems, and Computers*, 2019, pp. 23–30.
- [17] —, "Non-Bayesian Activity Detection, Large-Scale Fading Coefficient Estimation, and Unsourced Random Access With a Massive MIMO Receiver," *IEEE Transactions on Information Theory*, vol. 67, no. 5, pp. 2925–2951, 2021.
- [18] U. K. Ganesan, E. Bjornson, and E. G. Larsson, "An Algorithm for Grant-Free Random Access in Cell-Free Massive MIMO," in *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2020, pp. 1–5.
- [19] U. K. Ganesan, E. Bjornson, and E. G. Larsson, "Clustering Based Activity Detection Algorithms for Grant-Free Random Access in Cell-Free Massive MIMO," *IEEE Transactions on Communications*, pp. 1–1, 2021.
- [20] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge University Press, 2016.
- [21] E. Bjornson, J. Hoydis, and L. Sanguinetti, "Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency," *Foundations and Trends in Signal Processing*, vol. 11, no. 34, p. 154655, Nov. 2017. [Online]. Available: <https://doi.org/10.1561/20000000093>
- [22] G. Callebaut, S. Gunnarsson, A. P. Guevara, A. J. Johansson, L. Van Der Perre, and F. Tufvesson, "Experimental exploration of unlicensed sub-ghz massive mimo for massive internet-of-things," pp. 2195–2204, 2021.
- [23] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pet-tissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology," in *2015 14th International Conference on ITS Telecommunications (ITST)*, 2015, pp. 55–59.
- [24] G. Callebaut, G. Leenders, J. Van Mulders, G. Ottoy, L. De Struyker, and L. Van der Perre, "The Art of Designing Remote IoT Devices — Technologies and Strategies for a Long Battery Life," *Sensors*, vol. 21, no. 3, 2021. [Online]. Available: <https://www.mdpi.com/1424-8220/21/3/913>
- [25] K. Senel and E. G. Larsson, "Grant-free massive MTC-enabled massive MIMO: A compressive sensing approach," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6164–6175, 2018.

Epileptic Seizure Detection using a Tensor-Network Kalman Filter for LS-SVMs

Seline de Rooij
Circuits and Systems (CAS)
Delft University of Technology
Delft, Netherlands
s.j.s.derooij@tudelft.nl

Borbála Hunyadi
Circuits and Systems (CAS)
Delft University of Technology
Delft, Netherlands
b.hunyadi@tudelft.nl

Abstract—Epilepsy is one of the most common neurological conditions, affecting nearly 1% of the global population. It is defined by the seemingly random occurrence of spontaneous seizures. Anti-epileptic drugs provide adequate treatment for about 70% of patients. The remaining 30%, on the other hand, continue to have seizures, which has a significant impact on their quality of life as they are constantly unsure when these seizures will occur. Reliable seizure detection methods would thus have a significant impact on the lives of these patients.

Despite ongoing research efforts involving academia and industry in large international collaborations, epileptic seizure detection and especially prediction is still an unsolved problem. The key to the solution could lie within ultralong-term, real-life datasets that are currently being generated using wearable sensors. However, due to the size of these datasets, conventional learning techniques such as least-square support vector machines (LS-SVMs) can become intractable.

Therefore, this work proposes the use of a recently developed tensor network Kalman filtering approach for LS-SVMs (TNKF-LSSVM) to detect epileptic seizures [1]. In the TNKF-LSSVM algorithm, the dual problem of the LS-SVM is solved using a recursive Bayesian filtering approach. This way the least-square problem can be solved row-by-row using a Kalman filter, thereby avoiding explicit matrix inversions, while also being able to provide confidence bounds on the estimates. By making use of the tensor-train format [2] to represent the matrices and vectors in the Kalman equations, it is even possible to avoid the construction of the $(N + 1) \times (N + 1)$ covariance matrix¹.

To be able to apply the TNKF-LSSVM algorithm for seizure detection there are still some issues that need to be tackled. One such problem is that the TNKF-LSSVM only performs well when the dataset is properly balanced, which is generally not the case for seizure datasets. Furthermore, for the TNKF-LSSVM to work efficiently for large scale problems the modes of the tensor-trains representing the matrices and vectors should be as small as possible, thus it must hold that $N + 1 = \prod_i n_i$, such that n_i is ‘small’ for all i . To overcome both of these challenges we propose using the SMOTE method to oversample the seizure class, such that a balanced training set can be generated that has good factorization properties.

Some preliminary results using a small subset of data from a public EEG dataset [3] show that taking the above considerations into account, the TNKF-LSSVM method can have performance that is competitive with a regular LS-SVM. Where the TNKF-LSSVM method has the benefit of scaling log-linearly with the size of the dataset (in terms of memory usage) and can provide an uncertainty estimate of the detection. Future work will need

to show whether this scaling up works as expected for the entire dataset.

Index Terms—tensors, tensor-train, Kalman filter, SVM, seizure, epilepsy, detection

REFERENCES

- [1] M. Lucassen, J. A. K. Suykens, and K. Batselier, “Tensor Network Kalman Filtering for Large-Scale LS-SVMs,” *arXiv:2110.13501 [cs, eess]*, Oct. 2021. arXiv: 2110.13501.
- [2] I. V. Oseledets, “Tensor-Train Decomposition,” *SIAM Journal on Scientific Computing*, vol. 33, pp. 2295–2317, Jan. 2011. Publisher: Society for Industrial and Applied Mathematics.
- [3] I. Obeid and J. Picone, “The Temple University Hospital EEG Data Corpus,” *Frontiers in Neuroscience*, vol. 10, May 2016.

¹ N is the number of data points in the training set and 1 is added for the bias.

DECODER-ONLY TRANSFORMERS FOR PASSIVE HUMAN ACTIVITY RECOGNITION

Shervin Mehryar, Lin Fei Kang, Yue Fei, and Shahrokh Valaee

Department of Electrical & Computer Engineering, University of Toronto, Toronto, Canada
{linfei.kang, y.feifei}@mail.utoronto.ca, {valaee,shervin.mehryar}@ece.utoronto.ca

ABSTRACT

Due to the prevalence of passive Wifi signals, recently researchers have focused on using the Channel State Information (CSI) for the purpose of activity recognition in indoor applications. Many Machine Learning algorithms have been proposed to this end that aim to address this issue by focusing on the sequential property of time-series data. In this work, we propose a Transformer-based architecture which in addition aims to take advantage of the spatial diversity inherent in multi-antenna and multi-channel CSI data as input. Through experimentation we show the benefits of proposed architecture, particularly in indoor settings where the effects of environment geometry, including line-of-sight versus non-line-of-sight, matter most.

Index Terms— Activity Classification, Channel State Information, Transformer Model, Machine Learning, Multi-channel

1. INTRODUCTION

The prevalence of Wifi transmit-receive signals has in recent years given rise to increasing research in emerging IoT applications. An area of interest is related to applications that utilize the untapped and passive signals propagating through open air. Already present in the environment, Channel State Information (CSI) is one of the most promising sources of such signals, essentially anywhere with a Wifi Access Point (AP). The presence of many Wifi enabled devices, (e.g. routers, smart TVs, etc), entails the following research question: can smart devices use the signal in a non-intrusive way to their benefit and provide useful service for their users? This work focuses on classifying a user's activity captured in passive signal sources, in particular the multi-channel CSI, using a Transformer architecture.

Traditionally, such applications have relied on direct communication which consumes much needed bandwidth. Recently, there has been a number of proposals to use CSI packets opportunistically for activity recognition [1, 2, 3, 4]. The problem with such approaches is that the Wifi channel experiences fast and non-predictable changes. This seeming short-

coming, as counter intuitive as it may seem, can be utilized to the benefit of such systems.

According to a recent survey on algorithms for stationary and single subject setup [1], classical machine learning algorithms, such as Support Vector Machine (SVM), can be improved using recurrent neural networks such as a Long Short Term Memory (LSTM) network. In the multi-room scenarios [5], Convolutional Neural Networks (CNN) plus LSTM classifiers that rely on spectrogram analysis have shown promising results in multi-class predictions task where the activity of the subject can be different in different rooms. Transformers are a type of neural networks that can capture temporal relations in the input signal through the power of attention mechanisms. While in the discrete and finite signal domains such as sentence and word prediction, Transformers have been shown to perform outstandingly, in the case of time-series signal the research is pre-mature and on-going.

In this work, we propose a new application of Transformer networks to the CSI data for activity recognition. Particularly, we investigate and show analysis where diversity of signals can prove useful. In Section 2, we provide the model and algorithm to perform activity recognition (classification) based on CSI input. The model can be trained using the Stochastic Gradient Descent method, commonly used in training deep neural networks. We derive mathematical expressions for the update rules. In Section 3, we describe the experimentation setting and environment geometry through which data for training has been collected. Unlike previous research, we put emphasis on location variations of subjects.

2. SYSTEM MODEL & ARCHITECTURE

The signal space behaviour of a communication channel is well described by its Channel State Information (CSI) [6]. Among other effects, the CSI captures and represents the effect of scattering, fading, and distance-related power attenuation. Compared to RSSI, recent research shows that CSI better embodies the subtleties related to location and motion in indoor environments [7], known as spatial dependencies. In a classical posture recognition setting, there are mainly four components that make up the system, namely data acquisition, preprocessing, feature extraction, and a final classification stage. We formulate these steps for end-to-

The authors acknowledge Huawei Canada for the financial support of this project.

end training as follows. Let the collected CSI matrix be $\mathbf{H} = [\mathbf{h}_1, \dots, \mathbf{h}_N] \in \mathbb{C}^{N \times K}$ where N is the sequence length corresponding to the time index and K the total number of sub-carriers over a multi-antenna, multi-channel communication link. This taken as raw input can be used to perform activity recognition, as described next.

2.1. Convolutional Signal Pre-Processing

We perform a pre-processing or filtering computation as a first-step, in each sub-carrier with a sliding window to carry convolution summation, in order to smooth out the collected CSI. Let \mathbf{W}_ϕ be the learned parameter. Then the smoothing formula is of the form:

$$\mathbf{Z} = f_\phi(\mathbf{W}_\phi \mathbf{H} + \mathbf{b}_\phi), \quad (1)$$

where $f(\cdot)$ is an activation function of choice and \mathbf{b}_ϕ is the bias term. In this case, the learning parameters are $\Phi = [\mathbf{W}_\phi, \mathbf{b}_\phi]$ for all sub-carriers. We note that this can be viewed as a convolutional neural network pre-processing step, where the set of parameters are kernel weights of a fixed, often small, size, shared across all the sub-carriers. Let $\mathbf{Z} = [\mathbf{z}_1, \dots, \mathbf{z}_N] \in \mathbb{C}^{N \times K}$ be the matrix of stacked smoothed CSI data through the convolution operation.

2.2. Transformer (Decoder-Only) Architecture

We form the following transformations of the columns of \mathbf{Z} which correspond to sub-carrier frequencies of the CSI data. Let $\Psi = [\mathbf{W}_q, \mathbf{W}_k, \mathbf{W}_v] \in \mathbb{C}^{K \times 3K}$ be a set of trainable transformation parameters, adopting the notation in [8], we take:

$$\mathbf{Q} = \mathbf{W}_q \mathbf{Z}, \quad (2)$$

$$\mathbf{K} = \mathbf{W}_k \mathbf{Z}, \quad (3)$$

$$\mathbf{V} = \mathbf{W}_v \mathbf{Z}, \quad (4)$$

or in compact notation $\mathbf{Q} = [\mathbf{q}_1, \dots, \mathbf{q}_N]$, $\mathbf{K} = [\mathbf{k}_1, \dots, \mathbf{k}_N]$, and $\mathbf{V} = [\mathbf{v}_1, \dots, \mathbf{v}_N]$. Note that each column in \mathbf{Q} , \mathbf{K} , and \mathbf{V} corresponds to an expression that is a linear combination of all CSI sub-carrier data at a given time. We are interested in normalized coefficients α_i across sub-carriers $i \in \{1, \dots, K\}$ computed as:

$$(\alpha)_{ij} = \frac{1}{\sqrt{N}} \frac{(\mathbf{K}\mathbf{Q})_{ij}}{\sum_{j=1}^K (\mathbf{K}\mathbf{Q})_{ij}}, \quad \forall j \in \{1, \dots, K\} \quad (5)$$

where the notation $(\cdot)_{ij}$ refers to the j 'th element of the i 'th row of its argument matrix. Note that $(\alpha)_{ij}$'s are in the range $[0, 1]$ and add to one across rows when viewed as a $K \times K$ matrix. Essentially, the higher the value of j 'th element in α_i , the more the influence of the j 'th and i 'th sub-carriers on each other at a given time, which we consider important for classification. In relation to the attention mechanism of [9], we note that in this case, the index of time refers to signal CSI at each time stamp rather than a word index. Similarly,

in order to ensure that the predictive blocks remain causal, we impose a constraint on each of the matrices \mathbf{W}_q , \mathbf{W}_k , and \mathbf{W}_v to be lower triangular. We can then form the new CSI vectors 'with attention' as:

$$\hat{\mathbf{h}}_i = \vec{\alpha}_i \mathbf{V}, \quad (6)$$

for each $i \in \{1, \dots, K\}$, where we have used the notation $\vec{\alpha}_i$ to view all the influences from other sub-carriers on the i 'th sub-carrier in a vector form. After this operation, we can write in compact form $\hat{\mathbf{H}} = [\hat{\mathbf{h}}_1, \dots, \hat{\mathbf{h}}_N] \in \mathbb{C}^{N \times K}$. In short, the relation between the matrix of original CSI denoted by \mathbf{H} and the transformed matrix of CSI, denoted by $\hat{\mathbf{H}}$, becomes:

$$\hat{\mathbf{H}} = f_\Psi(\mathbf{H}), \quad (7)$$

where $f_\Psi(\cdot)$ is a multi-variable function parametrized by $\Psi = [\mathbf{W}_q, \mathbf{W}_k, \mathbf{W}_v]$.

2.3. Linear Discriminant Classifier

The above development allows us to form a classifier given $\hat{\mathbf{H}}$. With that, it's the task of the recognition module to detect the type of posture captured by the CSI data. By properly capturing the information in the new CSI due to the movement of the human body causing classifiable propagation effects, passive recognition becomes feasible in this setting. Formally, given $\hat{\mathbf{H}}^t$ as a column vector of features at instance t consisting of K transformed measurements, we are interested in predicting the activity class given by:

$$p(y = c | \hat{\mathbf{H}}^t; \Theta) = \frac{\exp(\theta_c^T \hat{\mathbf{H}}^t)}{\sum_{j=1}^C \exp(\theta_j^T \hat{\mathbf{H}}^t)}, \quad (8)$$

where y is the model prediction among C classes and T is the transpose operator, θ_c denotes the weight corresponding to the feature set of activity c in a linear model, and $\Theta = [\theta_1, \dots, \theta_C]$ in compact vector notation. This formulation lends itself to type of hypothesis thesis in which the correct class can be predicted conditioned on the system parameters and input. Indeed, in (8) other variations of the input and feature signals can be incorporated.

In this case, let $f_\Theta(\hat{\mathbf{H}})$ denote the vector function of likelihoods under all hypotheses. Therefore, the elements of this vector function are precisely the ones from relation (8) and its size is C . One mode of classification would be to choose the element with the highest likelihood to be the prediction from the model. Without any prior knowledge of the input, this would correspond to the Maximum Likelihood estimate, also known as the *soft-max* learning. More formally,

$$f_\Theta(\hat{\mathbf{H}}^t) = \begin{bmatrix} p(y = 1 | \hat{\mathbf{H}}^t; \theta_1^t) \\ \vdots \\ p(y = C | \hat{\mathbf{H}}^t; \theta_C^t) \end{bmatrix}, \quad (9)$$

where Θ^t are the classifier's learned parameters at time t .

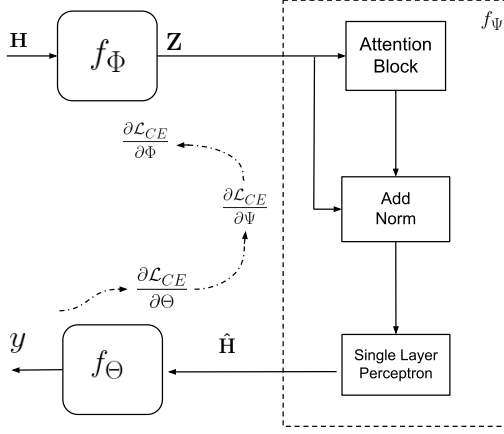


Fig. 1: System diagram of the proposed activity recognition method.

2.4. Learning with Stochastic Gradient Descent

It must be noted that the proposed architecture in this paper bears resemblance to that of (decoder-only) Transformer architecture applied in machine learning and Natural Language Processing (NLP). Similar to the learning process proposed in [8], we define the following cross-entropy loss function:

$$\mathcal{L}_{CE} = -\frac{1}{N'} \sum_{i=1}^{N'} \log \left(\frac{p(y = c_i | \hat{\mathbf{H}}^t; \theta_1 \dots \theta_C)}{\sum_{j \neq i} p(y = c_j | \hat{\mathbf{H}}^t; \theta_1 \dots \theta_C)} \right), \quad (10)$$

where the summation is over N' data samples. The learning rules corresponding to the parameters for the pre-processing, the Transformer model, and the classifier head are given by:

$$\Phi^{(t+1)} \leftarrow \Phi^{(t)} + \lambda \frac{\partial \mathcal{L}_{CE}}{\partial \Phi}, \quad (11)$$

$$\Psi^{(t+1)} \leftarrow \Psi^{(t)} + \lambda \frac{\partial \mathcal{L}_{CE}}{\partial \Psi}, \quad (12)$$

$$\Theta^{(t+1)} \leftarrow \Theta^{(t)} + \lambda \frac{\partial \mathcal{L}_{CE}}{\partial \Theta}, \quad (13)$$

to obtain the parameters at epoch $t + 1$, given the parameters at epoch t , where λ is the learning rate. Automatic differentiation libraries readily exist for computationally carrying out updates in relations (11), (12), and (13). In summary, the proposed architecture performs the following processing steps on CSI, which is passively received. Any filtering and smoothing such as denoising or Gaussian smoothing, which are necessary as pre-processing, may be performed on the inputs. The first step requires smoothing and filtering of the CSI data in which a one-dimensional convolution layer is applied to the original CSI. Next, the filtered CSI is transformed using the attention mechanism in (7), in order to determine which carrier frequencies hold the most information about the activity,

capturing spatial and inter-frequency dependencies. The results of the last processing stage are passed through a linear classifier given in (9), which then outputs the predicted category for the human activity. The overall system diagram is shown in Figure 1.

3. EXPERIMENTS

In this section, we provide experimental results and compare the performance of the proposed algorithm with the state-of-the-art. Our measurements are taken using two Asus AC86u routers, each equipped with 3 antennas and 52 frequency modes per antenna, resulting in $K = 156$ sub-carriers. In our experiments, we consider a single subject in one of 6 different locations. The room is 8ft-by-18ft, with one transmitter fixed in one corner while the receiver positions are changed in parallel along the room, to capture the effect of geometry. Overall 13,942 data points (3 seconds long at 0.02 sampling rate, i.e. $N = 150$) are collected from 5 classes (“pickup”, “sitdown”, “standup”, and “walk”, and from an “empty room”). We trained the algorithm described in [5] with the settings of the authors on our dataset, named Spec-CNN. Each is trained for 100 epoches, with 20% of data held out for test on a computer with Tesla K80 GPU. Table 1 summarizes the results.

3.1. Accuracy & Effect of Diversity

As compared to a CNN based classifier’s accuracy of 81%, the proposed architecture achieves a higher accuracy of $(87.83 \pm 0.64)\%$ as reported over all configurations of subjects and receivers. Furthermore, the benefit from selecting sub-carrier modes through the attention mechanism can be seen when all 1 – 156 sub-carriers are used as opposed to when 10%, 30%, 50%, and 70% of subcarriers are used. This is deemed to be due to the network’s capability to attend to sub-carrier CSI that contribute the most to the output of the classifier, attesting to the capacity of network to incorporate more data in order to improve its performance. In general, increasing K does not imply increased performance as the results show.

3.2. Accuracy & Environment Geometry

In order to investigate the effect of environment geometry, we perform two types of experiments. In the first case, we compare the effect of line-of-sight (LOS) including all data points where the subject, transmitter, and receiver are along a direct path, against the case when they are not (non-line-of-sight or NLOS). Here, we report on three activities (“walk” and “no activity” would be ambiguous). In general, it’s believed that CSI data is very susceptible to environment changes. When it comes to LOS versus NLOS, our results show that changes in activities matter just as much — evident in drop in accuracy in almost all other classes — when the subject is in NLOS.

Lastly, for each activity we compare the prediction accuracy as a function of distance. The models are only trained on

Table 1: Classification accuracy on data collected using Asus Router model AC86u with 3 antennas and total of $K = 152$ sub-carriers. The classification accuracy results are shown when 10%, 30%, 50%, 70% selected at random, and all 1 – 152, sub-carriers are used. The results for Line-of-Sight (LOS) and None-Line-of-Sight (NLOS) as well as for distances $d = 12$, $d = 14$, $d = 16$, $d = 18$ feet between the transmitter and receiver are provided.

Class						Proposed					
	10%	30%	50%	70%	1-156	LOS	NLOS	d=12	d=14	d=16	d=18
No Activity	50.79	29.36	67.46	84.12	97.62	-	-	98.52	98.25	98.26	100.00
pickup	62.54	24.34	47.19	82.77	86.33	93.96	84.63	85.38	85.84	96.21	72.83
sitdown	17.01	23.67	50.34	83.44	97.24	96.93	98.27	99.24	94.98	97.30	90.87
standup	50.23	84.33	97.23	72.58	88.94	97.20	87.00	90.12	87.10	77.36	85.38
walk	09.38	53.52	51.17	34.27	72.30	-	-	74.78	75.56	80.70	56.86
Acc (%)	40.75	43.05	62.39	74.56	87.83	96.14	88.23	88.61	89.53	92.20	79.09

all data-points, however, we test the model when the two receivers are placed in parallel, at $d = 12$, $d = 14$, $d = 16$, and $d = 18$ feet away from the transmitter. We notice that given the geometry of the room, there are sweet spots where the accuracy is highest and generally the accuracy diminishes when the distance between the transmitter and receiver increases. This accuracy is however necessarily not a linear function of distance. For instance, at $d = 14$ ft over all classes, the accuracy is the highest while there is a dip in accuracy for “pickup” and “walk” at distance $d = 12$ ft, bringing the overall accuracy down. This demonstrates the susceptibility of the networks to distance. For such settings, re-training for a few epochs in our experience proves helpful to mitigate the effect of over generalization. Beyond 18ft, accuracy experiences a significant drop expect for no activity (i.e. high false negative).

4. CONCLUSION

One of the main challenges in human activity recognition in indoor applications using CSI data lies in the ability to utilize spatial as well as temporal properties of signals due to environmental effects. In this work, we propose a Transformer-based model that leverages these properties in order to achieve desired performance in complex indoor settings where LOS versus NLOS scenarios prevail. By combining all CSI and allowing the attention mechanism in relation (7) to process all sub-carriers simultaneously, the model is able to considerably improve its performance where accuracies as high as 96% and 88% are achieved in LOS and NLOS settings, respectively. With an overall accuracy of 87.83%, our model outperforms the state-of-the-art in full room settings where transmitter and receiver distances as well as subject locations may vary.

5. REFERENCES

- [1] Zhenguo Shi, J. Andrew Zhang, Rithard Xu, and Gengfa Fang, “Human activity recognition using deep learning networks with enhanced channel state information,” in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.
- [2] Zhenghua Chen, Le Zhang, Chaoyang Jiang, Zhiguang Cao, and Wei Cui, “Wifi csi based passive human activity recognition using attention based blstm,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2714–2724, 2019.
- [3] Chunjing Xiao, Daojun Han, Yongsan Ma, and Zhiguang Qin, “Csgan: Robust channel state information-based activity recognition with gans,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10191–10204, 2019.
- [4] Liu Wenyuan, Wang Siyang, Wang Lin, Li Binbin, Su Xing, and Jing Nan, “From lens to prism: Device-free modeling and recognition of multi-part activities,” *IEEE Access*, vol. 6, pp. 36271–36282, 2018.
- [5] Hoonyong Lee, Changbum R Ahn, and Nakjung Choi, “Fine-grained occupant activity monitoring with wi-fi channel state information: Practical implementation of multiple receiver settings,” *Advanced Engineering Informatics*, vol. 46, pp. 101147, 2020.
- [6] Antonia M. Tulino, Angel Lozano, and Sergio Verdu, “Impact of antenna correlation on the capacity of multi-antenna channels,” *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2491–2509, 2005.
- [7] Zhihui Gao, Yunfan Gao, Sulei Wang, Dan Li, and Yue-dong Xu, “Crisloc: Reconstructable csi fingerprinting for indoor smartphone localization,” *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3422–3437, 2021.
- [8] Zhuolin Chen, Fanglin Gu, and Rui Jiang, “Channel estimation method based on transformer in high dynamic environment,” in *2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, 2020, pp. 817–822.
- [9] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, and Illia Polosukhin, “Attention is all you need,” 2017.

Object Detection and Person Tracking in CathLab with Automatically Calibrated Cameras

Yingfeng Jiang* Renjie Dai* Jincheng Zeng* Rick Butler Teddy Vijfvinkel
Yanbo Wang John van den Dobbelsteen Maarten van der Elst Justin Dauwels
Delft University of Technology, 2611 DX, Delft, Netherlands

Workflow analysis is a young research field that has been gaining traction in recent years. Work in this field aims to improve the efficiency and safety in operating rooms by analysing surgical processes and providing feedback or support, where observations are made and evaluated by algorithms rather than human experts. For our study, we mount five cameras from different angles in a Catheterization Laboratory (CathLab) to observe and analyse Cardiac Angiogram procedures. To automate the classification of workflow and personnel activities, we propose a pipeline that first automates the camera calibration of the 5-camera network then detect locations of medical equipment and track personnel activities.

One of the most common ways to calibrate camera networks is to use coded targets or markers [1]. However, cameras might accidentally move after the calibration, causing all 3D data calculated wrongly, therefore, the cameras need to be re-calibrated. The re-calibration can be time-consuming. An alternative is to use techniques based on Structure from Motion (SfM) which exploit the image correspondences between different views. But these are often difficult to establish when there is limited overlap between different views. To address the above limitations, we propose an automatic camera calibration framework in the CathLab, which relies on Scaled-YOLOv4 [2] to detect fixed objects and uses automatic model based on artificial neural networks to extract selected key-point features from each image frame. Then point-correspondences between the image frame and the 3D coordinates are used to compute one calibration set. A RANSAC-based filtering and aggregation algorithm is used to generate a robust estimate of the extrinsic parameters of each camera. The calibration framework is shown in Fig. 1.(b).

For object detection, we apply the state-of-the-art method Scaled-YOLOv4 [2], as it has extremely fast processing speed and decent precision. However, we find Scaled-YOLOv4 still has difficulties detecting transparent objects such as lead shields. In order to detect such objects, we propose an object detection algorithm based on Scaled-YOLOv4 with an auxiliary Dice Loss. The Dice Loss [3] establishes the right balance between objects and backgrounds automatically, making the boundary of objects attract more attention and contribute to more discriminative features. The proposed algorithm is consequently more powerful in detecting transparent objects. Moreover, Scaled-YOLOv4 is tailored for datasets of single

view without taking advantage of the information contained in multiple views. In this work, we also design a filter following the object detection algorithm to refine the bounding boxes of objects by considering detection results from different cameras. The full pipeline of our object detection algorithm is shown in Fig. 1.(a).

Multi-person tracking hinges on the accurate estimation of 3D human poses from multiple views. Most previous 3D pose estimation methods train their models directly on a 3D pose dataset, however, such data is unavailable for the task at hand. To solve this problem, we decompose 3D human pose estimation task into two stages (see Fig. 1.(c)), avoiding the need to large amounts of 3D pose data: we fine-tune Scaled-YOLOv4 and HRNet for 2D pose estimation in the first stage, and use a matching algorithm [4] to match corresponding 2D poses from multiple views and then reconstruct 3D poses in the second stage. The proposed 3D human pose estimation algorithm is orthogonal to the traditional multi-view tracking algorithm, and hence can be integrated with them flexibly. Once trained, our method can be easily generalized to different Cathlabs.

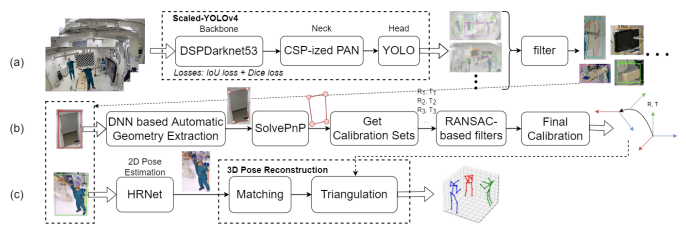


Fig. 1: Diagram of the proposed pipeline: (a) Object detection algorithm; (b) Automatic Extrinsic Calibration Framework; (c) Multi-person tracking algorithm.

REFERENCES

- [1] J. L. Schönberger *et al.*, “Structure-from-motion revisited,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 4104–4113.
- [2] C.-Y. Wang, A. Bochkovskiy, and H.-Y. M. Liao, “Scaled-yolov4: Scaling cross stage partial network,” 2020. [Online]. Available: <https://arxiv.org/abs/2011.08036>
- [3] F. Milletari *et al.*, “V-net: Fully convolutional neural networks for volumetric medical image segmentation,” in *2016 fourth international conference on 3D vision (3DV)*. IEEE, 2016.
- [4] J. Dong *et al.*, “Fast and robust multi-person 3d pose estimation from multiple views,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019.

*Equal contribution

Reliability of wireless intra-aircraft networks: A comparative analysis of IEEE 802.15.4 protocols

Berna Eraslan, Sonia Heemstra de Groot, Georgios Exarchakos, and Ignas Niemegeers

Center for Wireless Technology Eindhoven

Eindhoven University of Technology

Eindhoven, Netherlands

{b.eraslan, sheemstradegroot, G.Exarchakos and I.G.M.M.Niemegeers}@tue.nl

Abstract—In recent years, the wireless networks for avionics systems have been attracting the attention of researchers from different fields, airline companies, and industries. Specifically, the wireless avionics intra-aircraft communications (WAIC) aims to increase efficiency and flexibility while decreasing weight, fuel consumption, and maintenance costs compared to traditional wired avionics systems. WAIC solutions must offer reliability and latency values satisfying intra-aircraft application requirements to take full advantage of wireless networks. However, there are challenges such as limited resources, complex propagation environments, interference, and security. In this paper, we have analytically evaluated and compared the performance of representative industrial wireless networks, WirelessHART, Time Slotted Channel Hopping (TSCH), and Low Latency Deterministic Network (LLDN) using the mathematical model proposed by Park et al. [1], in terms of the average deadline missing probability per flight hour. This metric is derived mathematically for each protocol and investigated for different application classes.

Index Terms—wireless avionics intra-communications, industrial wireless sensor networks, deadline missing probability

I. INTRODUCTION

Wireless communication is already used for non-avionics intra-aircraft communication, e.g., to provide communication and entertainment services to passengers. However, wireless communication for avionics or Wireless Avionics Intra-Communications (WAIC) is still in the research stage. WAIC has significant potential advantages over wired solutions: life-cycle cost reduction, weight saving, flexibility, and safety. On the other hand, several challenges need to be overcome to meet the stringent reliability requirements imposed by avionics applications: limited resources, complex propagation environment, interference, and security. In the EU-funded Advanced Data and power Electrical Network Architectures and Systems (ADENEAS) [2], we are investigating WAIC solutions.

First of all, let us examine a conceptual topology for WAIC shown in Figure 1 [3] for a passenger airplane. Wireless devices (sensors and actuators) communicate exclusively with a gateway in a star topology centered on that gateway. These are connected via a wired backbone. In this paper we will only consider sensor traffic, i.e., unidirectional traffic from a sensor to its gateway in a star topology, illustrated in

This work is conducted under EU-funded Advanced Data and power Electrical Network Architectures and Systems (ADENEAS) project with Grant agreement ID: 101006728

Figure 2. The failure of one device or link does not affect the rest of the network. Devices can be added or removed easily without affecting the rest of the network. Reliability and latency requirements of applications are defined for this simple and generic case.

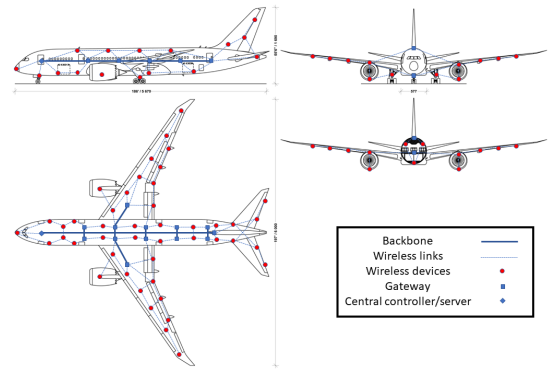


Fig. 1. An example aircraft network [3]

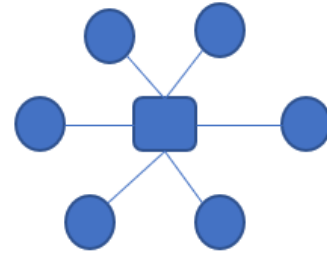


Fig. 2. A star network

II. TRAFFIC MODEL

In [1], Park et al. proposed that a WAIC network should support various avionics applications, generating three traffic types: periodic, event-triggered, and event-triggered periodic. For example, structural health monitoring and many engine sensors periodically transfer data. Event-triggered traffic is generated when an event occurs such as triggering a smoke

sensor. Some applications transfer event-triggered periodic data, which means that a periodic transmission of data is started when a specific event occurs such as the lowering of the landing gear [1]. We consider three different types of traffic sources:

- periodic traffic sources which generate a packet with a fixed interval, T_d ;
- event-triggered traffic sources which generate a packet with probability p_e in each T_d ;
- event-triggered periodic traffic sources which generate asynchronously a packet with probability p_h when T_d is expired, then stay to generate periodic packets with probability $1 - p_q$ in each T_d . Otherwise, it does not have a packet to transmit.

Let us denote the number of nodes with periodic traffic $N_{p,max}$, event-triggered traffic $N_{e,max}$ and event-triggered periodic traffic $N_{ep,max}$. The total number of nodes is $N_{max} = N_{p,max} + N_{e,max} + N_{ep,max}$. T_d is the time interval which is the application deadline. When a device cannot transmit the generated packet within the deadline, it discards the packet and generates a new one in next sampling interval [1]. The Gilbert Elliot model is used for burst noise binary channel [4]. The intra-aircraft environment is dynamic and unreliable so multiple transmissions will be needed. During flight hours, multiple samples are collected after each deadline. The expected number of periodic nodes at the first transmission of each j -th sampled data is dynamically updated as

$$N_p(1, j) = N_{p,max} + p_h N_{ep}(1, j-1) + (1 - p_q) p_h \times \sum_{k=0}^{j-1} N_{ep}(1, k) (1 - p_q)^{j-k-2} \quad (1)$$

The expected number of event-triggered periodic nodes at the first transmission of each j -th sampled data is dynamically updated as

$$N_{ep}(1, j) = N_{ep,max} - p_h N_{ep}(1, j-1) - (1 - p_q) p_h \times \sum_{k=0}^{j-1} N_{ep}(1, k) (1 - p_q)^{j-k-2} \quad (2)$$

III. RELIABILITY METRIC DERIVATION

The reliability requirements of the avionics applications have been characterized by their Development Assurance Level (DAL) [5], which, based on the safety assessment process in DO-178B [6], distinguishes 5 classes and associates a maximum failure rate per flight hour to each of them. These are shown in Table I. The application must ensure that the failure rate will be lower than the value in the table during real-time operation. Failure is defined as the inability to receive the message within the application deadline (worst case latency). The deadline values for avionics applications vary between 10-1000 milliseconds (ms) [7]–[10].

The average probability per flight hour is a quantitative metric, used for flight certification. It is normally calculated as the probability of a failure condition occurring during a typical

TABLE I
DEVELOPMENT ASSURANCE LEVEL (DAL)

Level	Failure Condition	Failure Rate per Hour
A	Catastrophic	10^{-9}
B	Hazardous	10^{-7}
C	Major	10^{-5}
D	Minor	10^{-3}
E	No effect	NA

flight of mean duration divided by that mean duration. A mathematical model is proposed by Park et al. [1] to evaluate and compare the reliability of the network for WAIC. It is assumed that the applications will generate data at periodic intervals of length T_d . T_d can also be called as the deadline of the transmission between one sensor and the gateway. For a safe operation, the applications need at least one successful transmission within a deadline, T_d . T_{dur} is defined as the flight duration in hours. T_{dur} must be greater than T_d : $T_{dur} \gg T_d$. Since beacon and ACK frames are relatively much smaller than data frames, the effect of their frame loss is neglected. Moreover, the packet loss probability, p_{loss} , is assumed to be constant and independent.

The total number of samples in the flight duration is

$$N_t = \frac{T_{dur}}{T_d} \quad (3)$$

The transmission time is shorter than the deadline of the applications for multiple transmissions. The i -th transmission time of the j -th sampled data is denoted as: $T_{cyc}(i, j)$, and $T_{cyc}(i, j) < T_d$. Then, the maximum allowable number of transmissions to delivery j -th sampled data, m_j , satisfies

$$\sum_{i=1}^{m_j} T_{cyc}(i, j) \leq T_d \quad (4)$$

Note that, $i \in [1, m_j]$, and $j \in [1, N_t]$.

The failure probability per flight hour P_f for each sample is independent. If the expected number of failures is denoted by N_f , P_f can be calculated as

$$P_f = \frac{T_d * N_f}{T_{dur}} = \frac{T_d}{T_{dur}} * \sum_{j=1}^{N_t} P_{f_{m_j}}^j = \frac{1}{N_t} * \sum_{j=1}^{N_t} P_{f_{m_j}}^j \quad (5)$$

$P_{f_{m_j}}^j$ denotes the deadline missing probability of j -th sampled data

$$P_{f_{m_j}}^j = \prod_{i=1}^{m_j} p_{loss_{i,j}} \quad (6)$$

where $p_{loss_{i,j}}$ packet loss probability of i -th transmissions of j -th sampled data.

IV. PERFORMANCE ANALYSIS

In this section, we will investigate the failure probability per flight hour of three industrial wireless networks, namely, LLDN, WirelessHART, and TSCH. LLDN and WirelessHART are presented by Park et al. in [1]. Table II illustrates a summary of the characteristics of the protocols.

A. WirelessHART

WirelessHART is a wireless implementation of the HART (Highway Addressable Remote Transducer) protocol (IEC 62591), developed by the HART Communication Foundation [11]. Each transmission and its corresponding acknowledgment occur within a 10 ms time slot in a periodic communication superframe.

At the beginning of every superframe is dedicated slots assigned to devices generating periodic traffic and event-triggered periodic traffic. The rest of the slots of the superframe are shared by devices generating event-triggered traffic. They compete to communicate using random access. Thus, the length of the superframe will be the sum of the beacon length T_{bc} , dedicated and shared slots, which is

$$T_{cyc}(i, j) = T_{bc} + (N_{\Sigma}(i, j) + N_s(i, j)) T_s \quad (7)$$

where $N_{\Sigma}(i, j)$ is the number of dedicated time slots, $N_s(i, j)$ is the number of shared time slots of i -th superframe to transmit j -th sampled data, respectively. T_s is slot duration.

The expected number of dedicated slots will be

$$N_{\Sigma}(i, j) = p_{loss}^{(i-1)} N_p(1, j) \text{ for } i \in [2, m_j] \quad (8)$$

and $N_{\Sigma}(1, j) = N_{p,max} + N_{ep,max}$.

Since the retransmission of the failed data transmission is not allowed at the same superframe, the expected failure probability per flight hour of the dedicated slots is

$$P_{f,d} = \sum_{j=1}^{N_t} \frac{p_{loss}^{m_j}}{N_t} \quad (9)$$

In the scope of this work, the failure probability of the event-triggered traffic of the shared slots is not considered. The number of shared slots is assumed to be constant and assigned to event-triggered nodes such that $N_s = N_{e,max}$.

B. Low Latency Deterministic Network (LLDN)

IEEE 802.15.4e provides three Medium Access Control (MAC) behaviors targeting time-critical applications: Deterministic and Synchronous Multi-channel Extension (DSME); Time Slotted Channel Hopping (TSCH) and Low Latency Deterministic Network (LLDN) [12]. The LLDN superframe is shown in Figure 3.

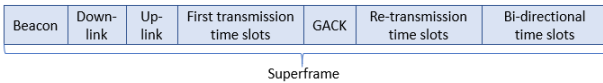


Fig. 3. LLDN Superframe

Assume time slots are assigned to all devices N_{max} in the first superframe of each sampling interval and no management, and no bidirectional time slots. Then, the expected length of the superframe is

$$T_{cyc}(i, j) = T_{bc} + (N_{\Sigma}(i, j) + N_{\Sigma,r}(i, j)) T_s + T_{gack} \quad (10)$$

where $N_{\Sigma}(i, j)$ and $N_{\Sigma,r}(i, j)$ are the expected number of first transmission slots and retransmission slots of i -th superframe to transmit j -th sampled data, respectively. T_{bc} is the sum of the beacon length. The expected number of retransmission slots of the superframe is

$$N_{\Sigma,r}(i, j) = p_{loss} N_{\Sigma}(i, j) \text{ for } i \in [2, m_j] \quad (11)$$

where $N_{\Sigma,r}(i, j) = p_{loss}(N_p(1, j) + N_e(1, j))$ are the expected number of first transmission slots and retransmission slots of i -th superframe to transmit j -th sampled data, respectively. The expected number of first transmission slots after the first transmission is

$$N_{\Sigma}(i, j) = p_{loss}^{2(i-1)} N_p(1, j) + p^{2(i-1)} N_e(1, j) \quad (12)$$

The data packet transmission in the superframe is successful when either the first transmission attempt or the retransmission is received. Hence, the expected failure probability per flight hour is

$$P_{f,d} = \sum_{j=1}^{N_t} \frac{p_{loss}^{2m_j}}{N_t} \quad (13)$$

C. Time Slotted Channel Hopping (TSCH)

TSCH uses fixed-size time slots and frequency (multi-channel) hopping. In the frequency hopping mechanism, the retransmission of the data packet is deferred to the next time slot assigned to the same sender-destination pair of nodes on a different frequency. It mitigates the effects of interference and multipath fading at a considerable [13]. Hopping can be performed over up to 16 channels $N_{channels}$, yet some channels can be left out that have low quality or to improve energy efficiency. A wide synchronization number, Absolute Slot Number (ASN), is a global value denoting the number of time slots elapsed since the beginning of the network. Channel offset is an integer value ranging from $[0, N_{channels}]$. A link between nodes is defined by channel offset and slot offset at the data link layer. The function F can be defined as a lookup table. Thus, the transmission channel frequency for each link is

$$f = F[(ASN + channelOffset) \pmod{N_{channels}}] \quad (14)$$

A time slot is the sum of the transmission of a frame and its acknowledgment, including encryption and decryption times. A unit of dedicated and shared time slots is called the slotframe, shown in Figure 4. Shared slots offer contention-based access, while dedicated slots offer guaranteed contention-free access. The expected length of slotframe is

$$T_{cyc}(i, j) = T_{bc} + (N_{\Sigma}(i, j) + N_s(i, j)) T_s \quad (15)$$

in which $N_{\Sigma}(i, j)$ is the number of dedicated time slots and $N_s(i, j)$ is the number of shared time slots.

TSCH standard does not provide any scheduling mechanism for assigning time slots. Let us assume similar assumptions with WirelessHART. The beginning of every slotframe is assigned to dedicated slots, which are assigned to devices having periodic traffic and event-triggered periodic traffic.

TABLE II
COMPARISON OF PROTOCOLS

Protocol	Frequency band	Data rate	Slot duration	Topologies	Advantages	Disadvantages
WirelessHART	2.4 GHz (ISM)	250 kb/s	10 ms	Star, mesh	usability, inheritance, collision free and deterministic	fixed slot duration
LLDN	2.4 GHz (ISM)	250 kb/s	10 ms	Star	low, deterministic latency no overhead due to turnaround time	lack of flexibility
TSCH	2.4 GHz (ISM)	1.2-1000 kb/s	10 ms	Star, mesh	time critical assurances high reliability more spectrum utilization	

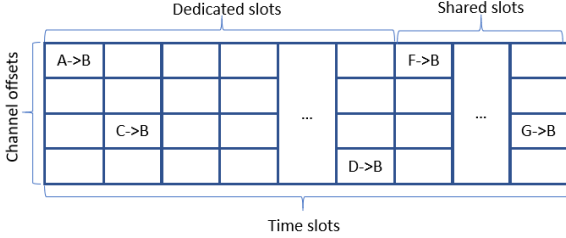


Fig. 4. TSCH Slotframe

They are followed by shared slots assigned to the event-triggered traffic.

Let us denote the packet loss probabilities of channels as $p_{loss_1}, p_{loss_2}, \dots, p_{loss_{N_{channels}}}$. The probability of choosing each specific channel is $\frac{1}{N_{channels}}$. To have fair comparison with LLDN and WirelessHart,

$$p_{loss_{TSCH}} = \frac{1}{N_{channels}} \sum_{n=1}^{N_{channels}} p_{loss_n} \quad (16)$$

Frequency hopping is performed uniformly over all available channels in a rotating manner. Thus, we can assume $p_{loss_1} = p_{loss}$ and $p_{loss_2} = p_{loss_3} = p_{loss_4} = \dots = p_{loss_{N_{channels}}} = p_{loss_o}$, p_{loss_o} is a generic variable. Thus, probability of packet loss for TSCH;

$$p_{loss_{TSCH}} = \frac{p_{loss}}{N_{channels}} + \frac{N_{channels} - 1}{N_{channels}} p_{loss_o} \quad (17)$$

If there is only one channel, $N_{channels} = 1$, that means no channel hopping and $p_{loss_{TSCH}} = p_{loss}$. This case will be same as WirelessHART. If all of the channels have equal packet loss probabilities, then $p_{loss_{TSCH}} = \frac{p_{loss}}{N_{channels}}$.

At the beginning of the operation, all periodic and event-triggered periodic nodes are assigned to dedicated slots at the first channel. The expected number of dedicated slots is

$$N_{\Sigma}(i, j) = \left((p_{loss_{TSCH}})^{(i-1)} N_p(1, j) \right) \text{ for } i \in [2, m_j] \quad (18)$$

and $N_{\Sigma}(1, j) = (N_{p,max} + N_{ep,max})$.

In the scope of this work, the failure probability of the event-triggered traffic of the shared slots is not considered. For dedicated slots, the number of shared slots of TSCH is assumed to be constant and fully assigned to event-triggered nodes such that for TSCH $N_s = (N_{e,max})$.

Since the retransmission of the failed data is not allowed in the same slotframe, the expected failure probability per flight hour of the dedicated slots is

$$P_f = \sum_{j=1}^{N_t} \frac{(p_{loss_{TSCH}})^{m_j}}{N_t} \quad (19)$$

V. RESULTS AND ANALYSIS

The failure probability per flight hour of each protocol is compared for deadline and packet loss probability. This approach could help to choose which protocol will be best for a specific application having strict latency and reliability requirements. The parameter values used in computations can be seen in Table III.

TABLE III
COMPUTATION PARAMETERS

Parameter	Symbol	Value
Slot size	T_s	10 ms
Number of periodic nodes	$N_{p,max}$	20
Number of event-triggered nodes	$N_{e,max}$	2
Number of event triggered periodic nodes	$N_{ep,max}$	2
Event triggered probability	p_e	0.5
Event triggered periodic first probability	p_h	0.1
Event triggered periodic probability	p_q	0.1
Number of channels	$N_{channels}$	4

Figure 5 compares the performances of protocols for $p_{loss} = 0.1$, markers show the closest values to DAL levels. When the deadline is lower than 230 ms, LLDN offers the most reliable operation for 24 nodes. As the deadline increases above 230 ms, TSCH offers significantly less probability of failure. It can even reach DAL A, at 330 ms. WirelessHART performs better than LLDN when the deadline is above 310 ms. WirelessHART can reach DAL A, at 410 ms.

In Figure 6, the deadline is assumed to be 480 ms for the same scenario. The failure probabilities are generally increasing with packet loss probability. TSCH is the most resilient one to packet loss probability. TSCH supports the highest DAL levels with the assumption that one channel has a higher packet loss probability than others. WirelessHART shows better performance than LLDN until p_{loss} is smaller than 0.41.

The scalability of the model in terms of the number of nodes is observed. The number of nodes increased to 120 for $p_{loss} = 0.1$. The number of nodes multiplied by 5 such

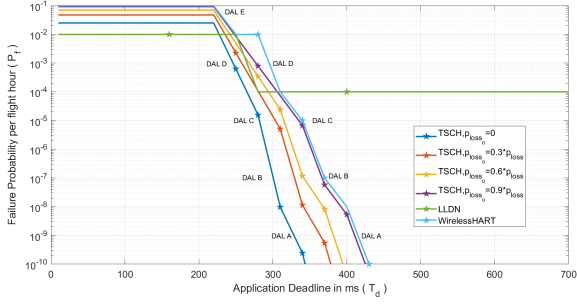


Fig. 5. Failure probability per flight hour as a function of application deadline for 24 nodes

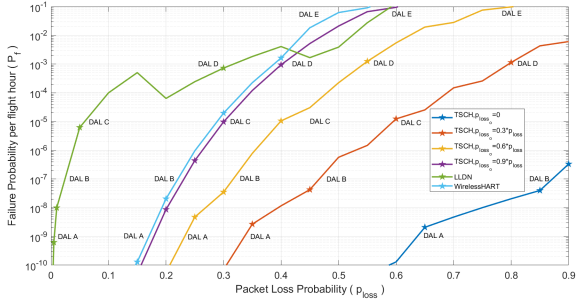


Fig. 6. Failure probability per flight hour as a function of packet loss probability for 24 nodes

that $[N_{p,max}, N_{e,max}, N_{ep,max}] = [100, 10, 10]$. The failure probability per flight hour as a function of the application deadline for scaled scenarios can be seen on Figure 7. Similar results were obtained with an increase in deadline for the same probability of failure values. When the deadline is below 1150 ms and between 1350-1450 ms, LLDN is the most reliable. For other values, TSCH shows superiority over other protocols, especially the one with $p_{loss_o} = 0$. WirelessHART performs better than LLDN when the deadline is above 1.8 s. TSCH can reach DAL A at 1.65 s, and WirelessHART at 2.1 s.

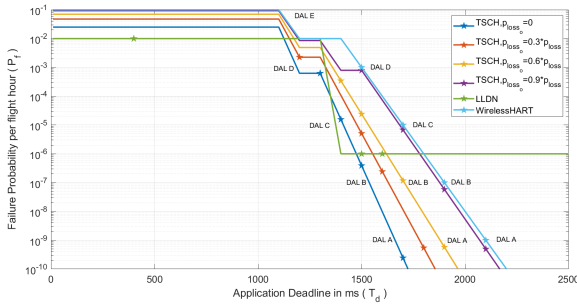


Fig. 7. Failure probability per flight hour as a function of application deadline for 120 nodes

In Figure 8, the deadline is assumed to be 2.4 s for the same scenario. The failure probabilities are generally increasing with packet loss probability. TSCH is the most resilient one to

packet loss probability. LLDN offers higher reliability than WirelessHART when $p_{loss} \geq 0.35$.

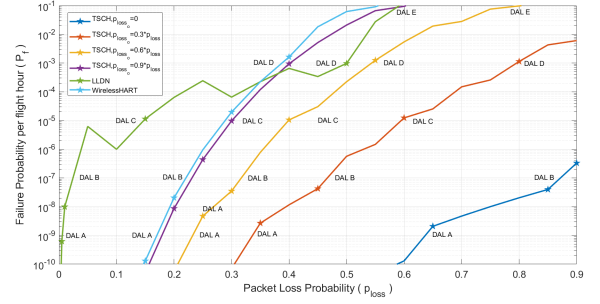


Fig. 8. Failure probability per flight hour as a function of packet loss probability for 120 nodes

VI. CONCLUSION

This paper compares the performance of three representative industrial wireless protocols, namely, LLDN, WirelessHART, and TSCH for wireless intra-aircraft avionics applications. Both TSCH and WirelessHART can offer all reliability levels for avionics applications at different deadlines. Moreover, TSCH and WirelessHART offer flexibility since while LLDN supports only star topologies, they enable both star and mesh topologies. For avionics applications requiring a very low deadline, LLDN is the best protocol to use. However, when the deadline is shown above a limit, TSCH and WirelessHART offer higher reliability than LLDN. If a very low deadline is not a primary concern compared to the reliability, TSCH is the protocol showing the highest performance with its channel hopping and resilience to interference. Channel hopping improves the performance of TSCH over WirelessHART by the assumption that the packet loss probability of one channel is higher than others. The model can include the effect of beacon and acknowledgment by extension. The failure probability for different traffic types can be observed.

REFERENCES

- [1] P. Park and W. Chang, "Performance Comparison of Industrial Wireless Networks for Wireless Avionics Intra-Communications," *IEEE Communications Letters*, vol. 21, pp. 116–119, Jan. 2017.
- [2] "Home - ADENEAS." <https://www.adeneas-project.eu/>, July 2021.
- [3] P. Park, P. Di Marco, J. Nah, and C. Fischione, "Wireless avionics intracommunications: A survey of benefits, challenges, and solutions," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7745–7767, 2021.
- [4] E. N. Gilbert, "Capacity of a burst-noise channel," *The Bell System Technical Journal*, vol. 39, no. 5, pp. 1253–1265, 1960.
- [5] R. F. S. 167, *Software considerations in airborne systems and equipment certification*. RTCA, Incorporated, 1992.
- [6] T. K. Ferrel, F. Uma D. Ferrel, and A. Consulting, "Rtca/do-178b, software considerations in airborne systems and equipment certification," tech. rep., RTCA SC-167, 1992.
- [7] "Technical characteristics and spectrum requirements of Wireless Avionics Intra-Communications systems to support their safe operation." <https://www.itu.int:443/en/publications/ITU-R/Pages/publications.aspx>.
- [8] A. Baltaci, S. Zoppi, W. Kellerer, and D. Schupke, "Evaluation of Cellular Technologies for High Data Rate WAIC Applications," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, May 2019.

- [9] A. Baltaci, S. Zoppi, W. Kellerer, and D. Schupke, "Evaluation of Cellular IoT for Energy-constrained WAIC Applications," in *2019 IEEE 2nd 5G World Forum (5GWF)*, pp. 359–364, Sept. 2019.
- [10] P. Park, P. Di Marco, J. Nah, and C. Fischione, "Wireless Avionics Intracommunications: A Survey of Benefits, Challenges, and Solutions," *IEEE Internet of Things Journal*, vol. 8, pp. 7745–7767, May 2021.
- [11] International Electrotechnical Commission, International Electrotechnical Commission, and Technical Committee 65, *Industrial Networks - Wireless Communication Network and Communication Profiles - WirelessHARTTM*. 2016.
- [12] H. Kurunathan, R. Severino, A. Koubâa, and E. Tovar, "Worst-case bound analysis for the time-critical mac behaviors of ieee 802.15. 4e," in *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, pp. 1–9, IEEE, 2017.
- [13] H. Kurunathan, R. Severino, A. Koubaa, and E. Tovar, "IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 1989–2010, 2018.

Relative Affine Localization for Robust Distributed Formation Control

Zhonggang Li
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
z.li-56@student.tudelft.nl

Raj Thilak Rajan
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
r.t.rajan@tudelft.nl

Abstract—Multiagent systems have been widely researched and deployed in the industry for their potential to collectively achieve goals by distributing tasks to individual agents [1]–[4]. Formation control, one of the many applications of multiagent systems, aims at steering agents into a stable geometric pattern in space [3], [4]. There has been a variety of crafted distributed controllers in literature based on different dynamics that agents follow, and different variables that agents sense and control [5]. Affine formation control is brought to the spotlight where N agents in \mathbb{R}^D converge to the target formation up to an affine transformation [6]. A more general scenario of affine formation control is the dynamic formation maneuvering problem where the target configuration is time-varying and the agents need to not only converge to the desired formation but also track the maneuvering pattern. This problem is addressed in [7] where a series of controller designs are introduced depending on the dynamics of the agents.

One of the practical challenge for affine formation control is the awareness of relative positions of the neighbouring nodes, which may not be always available due to e.g. sensor malfunctioning and environmental interference. Missing relative positions entail an adverse impact on the control, which leads to a suboptimal or even unstable formation. In this work, we present relative affine localization (RAL) to estimate unavailable relative positions from the known ones in dynamic affine formation control settings. It is found that the global affine transformation parameters over the network can be locally estimated through a set of linear equations. As such, the missing relative positions of the neighboring agents can also be localized and then employed by the controller. We also conclude that in \mathbb{R}^D , D relative positions for each agent are sufficient for localization in general. Furthermore, a sequential Least Squares (SLS)-based adaptive filter across time is also implemented on top of RAL to track the underlying affine parameters and improve the performance. Fig. 1 shows the improvements in tracking error $\delta(t)$ when using RAL and SLS-based filtering. We also study two practical scenarios where the system is subject to a percentage of loss of relative positions and out-of-service agents, respectively. As a result, RAL is robust to these cases in terms of convergence and optimality. It is worth mentioning that this method applies to all the controllers introduced in [7] since they involve relative positions.

Index Terms—affine formation control, missing observations, sequential Least Squares

This work is partially funded by the European Leadership Joint Undertaking (ECSEL JU), under grant agreement No 876019, the ADACORSA project - "Airborne Data Collection on Resilient System Architectures."

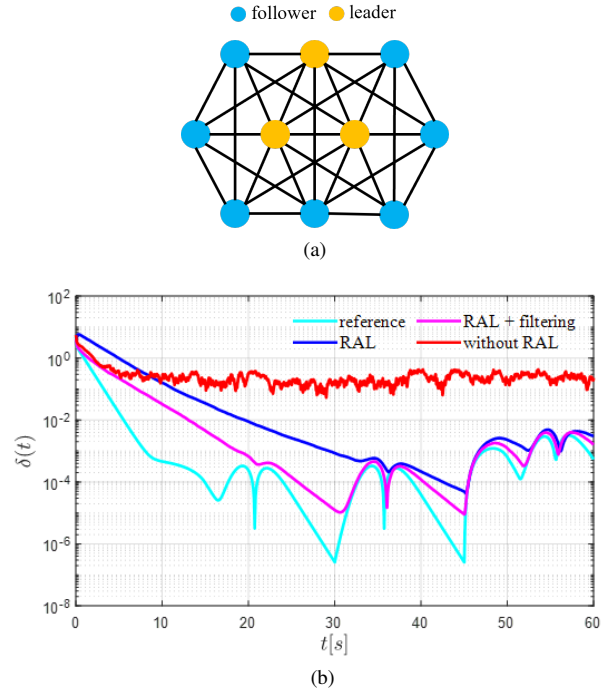






Fig. 1. (a) is the graph representation of formation where the vertices denote mobile agents and edges denote relative measurements. The time-varying target formation will be an affine transformation of the spatial locations of the vertices. (b) shows the mean tracking error $\delta(t)$ (difference of actual and target positions) across time t in seconds when only 3 relative positions are available per agent. The “reference” case is when all relative positions are available. This figure shows that without RAL the formation only converges suboptimally, but with RAL and SLS-based filtering the performance is much improved.

REFERENCES

- [1] S. Zhang, J. Zhou, D. Tian, Z. Sheng, X. Duan and V. C. M. Leung, “Robust Cooperative Communication Optimization for Multi-UAV-Aided Vehicular Networks,” in *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 780-784, April 2021, doi: 10.1109/LWC.2020.3043365.
- [2] R. T. Rajan, et al., “Applications and Potentials of Intelligent Swarms for magnetospheric studies,” in *Acta Astronautica*, Vol. 193, pp. 554-571, 2022, doi: 10.1016/j.actaastro.2021.07.046.
- [3] H. Li, P. Xie and W. Yan, “Receding Horizon Formation Tracking Control of Constrained Underactuated Autonomous Underwater Vehicles,” in *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5004-5013, June 2017, doi: 10.1109/TIE.2016.2589921.

- [4] J. Alonso-Mora, S. Baker and D. Rus. "Multi-robot formation control and object transport in dynamic environments via constrained optimization," in *The International Journal of Robotics Research*, vol. 36, no. 9, pp. 1000-1021, 2017, doi: 10.1177/0278364917719333.
- [5] K. K. Oh, M. C. Park and H. S. Ahn, "A survey of multi-agent formation control," in *Automatica*, Vol. 53, pp. 424-440, 2015, doi: 10.1016/j.automatica.2014.10.022.
- [6] Z. Lin, L. Wang, Z. Chen, M. Fu and Z. Han, "Necessary and Sufficient Graphical Conditions for Affine Formation Control," in *IEEE Transactions on Automatic Control*, vol. 61, no. 10, pp. 2877-2891, Oct. 2016, doi: 10.1109/TAC.2015.2504265.
- [7] S. Zhao, "Affine Formation Maneuver Control of Multiagent Systems," in *IEEE Transactions on Automatic Control*, vol. 63, no. 12, pp. 4140-4155, Dec. 2018, doi: 10.1109/TAC.2018.2798805.

Tracking Rental Bikes in Smart Cities: a Multi-RAT Approach

Guus Leenders , Gilles Callebaut , Liesbet Van der Perre , Lieven De Strycker 

KU Leuven, ESAT-DRAMCO, Ghent Technology Campus

Ghent, Belgium

name.surname@kuleuven.be

As cities ban polluting cars from city centers, bikes are becoming ever more popular for traveling last-mile, short distances in a commute towards the city center. The concept of bike-sharing involves a collection of bikes, spread out across a city. For customers of the bike sharing platform, these bikes are freely available for rent - when not in use. The two main problems, afflicting bike sharing concepts, is the loss of or theft of bikes [1] and the limited energy budget for tracking bikes. Traditionally, these bikes are being tracked using a Global Navigation Satellite System (GNSS) connection for localization, and a cellular 2G connection for cloud connection. However, both technologies consume large amounts of energy: which is troublesome for battery-operated trackers. To mitigate power consumption, Croce et al. [2] studied the applicability of LoRaWAN cloud communication for rental bikes.

Our research, however, indicates several zones where Long Range Wide Area Network (LoRaWAN) coverage is non-existent or extremely unreliable. Underground parking lots proof to be the most challenging environment for tracking bikes. In this work, we propose a Multiple Radio Access Technology (Multi-RAT) approach using both unlicensed (LoRaWAN) and licensed (Narrowband IoT (NB-IoT)) Internet of Things (IoT) technologies as both feature distinct advantages regarding Quality of Service (QoS), cost and energy consumption. As demonstrated in [3], NB-IoT features higher QoS levels (including coverage, latency performance and payload size). However, LoRaWAN excels in both energy efficiency for small payloads and cost efficiency. Combining both NB-IoT and LoRaWAN in a single IoT node, enables dynamic switching between these IoT technologies depending on various circumstances. When combining multiple wireless IoT technologies for the purpose of coverage enhancement, the resulting service area is effectively the total of all individual service areas combined.

As bikes are often left behind in underground parking lots, coverage in these challenging environments is of paramount importance. We studied coverage levels of both LoRaWAN and NB-IoT in multiple underground parking lots in the city of Bruges (Belgium). Our findings are summarized in Table I. These indicate the superior performance of NB-IoT due to the variety in Coverage Enhancement (CE) level, resulting in a larger Maximum Coupling Loss (MCL). By boosting CE

TABLE I: Coverage performance comparison of LoRaWAN and NB-IoT in underground parking lots. Both Received Signal Strength Indicator (RSSI) and Reference Signals Received Power (RSRP) are signal level and quality indicators.

Level	LoRaWAN	NB-IoT
0	✓(SF 12, -113 dBm RSSI)	✓(CE 0, -61 dBm RSRP)
-1	✗	✓(CE 2, -127 dBm RSRP)
-2	✗	✓(CE 2, -118 dBm RSRP)
-3	✗	✓(CE 1, -120 dBm RSRP)
-4	✗	✓(CE 2, -133 dBm RSRP)
-5	✗	✓(CE 2, -134 dBm RSRP)

levels, transmit power and packet repetitions are increased.

By combining both LoRaWAN and NB-IoT, energy can be saved by using LoRaWAN connectivity when available. By using confirmed messages, an IoT node can discern whether LoRaWAN coverage is available. When no LoRaWAN coverage is available, the IoT node can switch to NB-IoT communication, to ensure successful delivery. In this manner, coverage is drastically improved by only a slight increase in energy consumption and cost: making the bike truly theft-proof.

REFERENCES

- [1] L. Zhang, J. Zhang, Z.-y. Duan, and D. Bryde, "Sustainable bike-sharing systems: characteristics and commonalities across cases in urban China," *Journal of Cleaner Production*, vol. 97, pp. 124–133, 2015.
- [2] D. Croce, D. Garlisi, F. Giuliano, A. L. Valvo, S. Mangione, and I. Tinnirello, "Performance of lora for bike-sharing systems," in *2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*. IEEE, 2019, pp. 1–6.
- [3] G. Leenders, G. Callebaut, G. Ottoy, L. Van der Perre, and L. De Strycker, "Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT," *IEEE Communications Magazine*, vol. 59, no. 12, pp. 98–104, 2021.

Extended Abstract: Embedded AI Enabled Air-Writing for a Post-COVID World

Koen Goedemondt, Jie Yang, and Qing Wang

Delft University of Technology, The Netherlands

Emails: {k.s.goedemondt@student.tudelft.nl, j.yang-3@tudelft.nl, qing.wang@tudelft.nl}

I. INTRODUCTION

Touchscreens and buttons had become a medium for virus transmission during the COVID-19 pandemic. We have seen in our daily life that people use tissues and keys to press buttons inside elevators, on public screens, etc. In the post-COVID world, *touch-free* interaction with public touchscreens and buttons may become more popular.

Motivated by the rise of visible light communication and sensing, we design a real-time embedded system to enable touch-free fingertip writing of the digits 0–9 with only *ambient light* and *simple photodiodes*. We propose an embedded deep learning model to learn the spatial and temporal patterns in the dynamic shadow for air-writing digits recognition. The model is devised with a lightweight convolutional architecture such that it can run on a resource-limited device. We evaluate our model using the LightDigit dataset [1] and report the results in terms of accuracy and inference time.

LightDigit dataset. It is a new air-writing digits dataset collected by a researcher going through 70000 images in the MNIST dataset [2] and replicating them with air-writing and ambient light to obtain time-series information. The dataset contains 20880 instances of air-writing digits 0–9. Each instance has $500 \times 9 = 4500$ samples (i.e., samples per photodiode \times number of photodiodes). For more details about the LightDigit dataset please refer to [1].

II. EMBEDDED AI ALGORITHM

Data processing. The classification principle of our proposed algorithm is image processing using a convolutional neural network. Each instance in the LightDigit dataset is compressed into a 50×9 image (see Figure 1 for illustrations). Irrelevant samples in each instance are stripped from the beginning and the end. A sample is considered relevant if the variation of light across channels lies above a predetermined threshold, i.e., a sample with all channels (almost) equally lit will be removed. This is done to correct for different writing speeds, as a user will generally not be writing for the entire sampling time. Then, the samples are downsampled either by averaging samples into one or by simply keeping equally spaced samples, and removing the rest. In both cases, 50 samples are retained to form a 50×9 image. Finally, the image is globally normalized, instead of each channel independently. This is essential to compensate for continuously lit or dark channel, which would otherwise significantly distort the image.

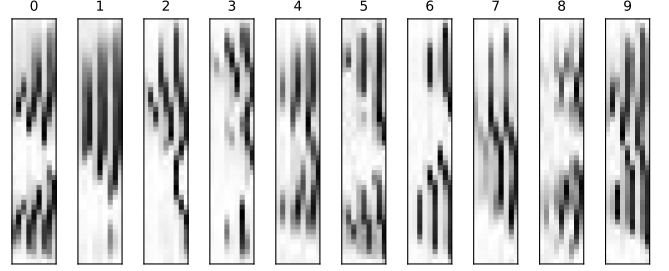


Fig. 1: Converting each air-writing digit to a 50×9 image.

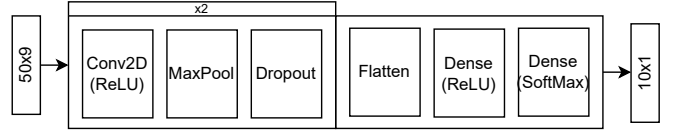


Fig. 2: Proposed model architecture which is optimized for various sizes. Note that dense softmax is the output layer.

Deep learning model. Our deep learning model is shown in Figure 2. It is based on the widely-used LeNet-5 architecture [3]. The goal is to keep the model as compact as possible while maintaining high accuracy. The final model contains two convolutional layers with ReLU activation followed by a max-pooling and dropout layer. The output of these layers is flattened and fed as input to a dense layer which then connects to the final output layer.

III. IMPLEMENTATION AND EVALUATION

We implement and run our embedded deep learning model on the NUCLEO-H743ZI2 STM32 board. This MCU board has an ARM-Cortex M7 CPU running at a maximum of 480 MHz, 1 MB SRAM and 2 MB flash. For detecting light, the system uses a 4×4 grid of OPT101 photodiodes, which are spaced 5 mm apart. They are sampled by the MCU through two MCP3008 ADCs at 100 Hz. We create the model in TensorFlow 2.0 and use TFLM [4] to port it the MCU. The model parameters are automatically quantized to 8-bit integer values, which decreases memory footprint as well as execution time. The model hyperparameters are optimized using the Hyperband algorithm [5] in keras tuner [6]. The amount of filters, kernel size and number of dense nodes were especially relevant. Rectangular kernels are found to perform best on this

TABLE I: Evaluation results of the within-subjects scenario.

Parameters	Dense nodes	Size (kB)	Accuracy	Inference time (s)	Inference time CMSIS-NN (s)
5k	96	9.9	0.885	0.72	0.08
8k	112	13.3	0.913	1.60	0.17
11k	80	16.2	0.936	1.48	0.16
14.7k	128	20.3	0.926	2.20	0.22

dataset. Both reference kernels¹ and CMSIS-NN [7] kernels were used when for determining inference time. CMSIS-NN is a deep learning library created by ARM consisting of highly optimized kernels specifically for Cortex M processors.

The evaluation results are presented in Table I. We consider a *within-subjects* scenario where we shuffle the data collected from 24 participants and split into training (80%) and test (20%). In addition, the training set is augmented with the simulated data from LightDigit. We observe that by converting the original time-series data from the LightDigit dataset to images and using a convolutional neural network with optimized hyperparameters, the amount of parameters could be reduced to 11k. After model quantization, this results in an embedded deep learning model of only 16 kB. The achieved accuracy is about 93.6% and the inference time using CMSIS-NN is only 0.16 seconds, running on the resource-limited ARM Cortex M-7.

IV. CHALLENGES AND FUTURE WORK

Through experimenting in various different light conditions, several major challenges were found which are listed below.

Clipping photodiodes. The OPT101 photodiodes are too sensitive when connected with the standard 1 M Ω feedback resistor and start clipping around 600 lux, depending on the spectrum of the captured light as the photodiodes respond different to red, green and blue light. In bright conditions this may cause the shadow area not to be dark enough, resulting in loss of information. The sensitivity of the photodiode can be reduced by using a smaller value feedback resistor.

Distorted shadows. Multiple light sources cause the shadow cast by the users' finger to become distorted. This is especially problematic since it is impossible to train the model for every possible configuration. We attempt to tackle this problem in two different ways. 1) An algorithm is proposed to extract hand movement from relative changes in the shadow, and train a new model on this data. The purpose of this algorithm is to more accurately model hand movement over the sensing area, avoiding the problem of brightness differences and light source distribution. 2) An autoencoder based deep learning approach in order to reconstruct distorted images. Autoencoders have been used successfully in image denoising to increase model robustness [8] and image restoration [9]. We intend to experiment with modifying images from the source dataset in such a way, they can be used to train an autoencoder. The hypothesis

is that this autoencoder can then be used to increase robustness in different lighting conditions.

Trigger sampling. For practical application, the system does not yet have way to start sampling automatically. This is intended to be solved by fitting the system with a APDS-9930 short range IR proximity sensor. When a user moves their hand over the sensing area, the sensor will send an interrupt to the MCU to trigger sampling.

V. CONCLUSION

LightDigit previously used a resource-intensive LSTM model for classification, which is too heavy to run on MCUs. By converting the time-series data to an image and using an optimized CNN, the amount of parameters could be reduced to 11k, resulting in a final model of 16 kB. Running on an ARM Cortex M-7 the inference time is 0.16 seconds using CMSIS-NN, while maintaining an accuracy of 93.6%. The inference time is 9 \times faster compared to reference kernels. Due to challenges resulting from variable light conditions, practical application of this system will require a more robust model. Since the inference time with current models is relatively fast, future work will include experimenting with larger models and more advanced preprocessing. We plan to experiment with denoising autoencoders and creating an improved algorithm to more precisely locate the finger of the user in space.

REFERENCES

- [1] T. Delft, "Lightdigit dataset," 2021. [Online]. Available: www.dropbox.com/s/lblt66mnun22g
- [2] L. Deng, "The MNIST database of handwritten digit images for machine learning research," *IEEE Signal Processing Magazine*, 2012.
- [3] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.
- [4] A. J. et. al., "Tensorflow lite for microcontrollers," <https://github.com/tensorflow/tflite-micro>, 2022.
- [5] L. Li and et. al., "Hyperband: A novel bandit-based approach to hyperparameter optimization," *Journal of Machine Learning Research*, 2018.
- [6] T. O'Malley, et., "Kerastuner," <https://github.com/keras-team/keras-tuner>, 2019.
- [7] L. Lai, N. Suda, and V. Chandra, "Cmsis-nn: Efficient neural network kernels for arm cortex-m cpus," 2018. [Online]. Available: <https://arxiv.org/abs/1801.06601>
- [8] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, "Extracting and composing robust features with denoising autoencoders," in *Proceedings of the 25th International Conference on Machine Learning*, ser. ICML '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 1096–1103. [Online]. Available: <https://doi.org/10.1145/1390156.1390294>
- [9] M. Suganuma, M. Özay, and T. Okatani, "Exploiting the potential of standard convolutional autoencoders for image restoration by evolutionary search," *CoRR*, vol. abs/1803.00370, 2018. [Online]. Available: <http://arxiv.org/abs/1803.00370>

¹In this context, kernel refers to the operations between tensors such as convolution.

Tensor-based Hemodynamic Response Estimation in Functional Ultrasound Data

Sofia-Eirini Kotti
Circuits and Systems, EEMCS
Delft University of Technology
Delft, The Netherlands
S.E.Kotti@tudelft.nl

Borbála Hunyadi
Circuits and Systems, EEMCS
Delft University of Technology
Delft, The Netherlands
B.Hunyadi@tudelft.nl

ABSTRACT

Functional ultrasound (fUS) is an emerging technique that provides high sensitivity imaging of cerebral blood volume (CBV) changes. As increased metabolic demand of active tissue induces changes in CBV, these changes reflect neuronal activity in the corresponding brain area. The main advantages of this technique are that it can image the entire brain with unprecedented spatial (50-500 μ m) and temporal resolution (10-100ms), and that it constitutes a potentially portable solution, as opposed to functional magnetic resonance imaging (fMRI), the currently dominant modality in functional brain imaging. The high resolution as well as the plane-wave illumination lead to a large amount of raw ultrasound data per acquisition.

The fundamental challenge is that fUS only provides an indirect measure of brain activity through the neurovascular coupling; this system is the link between the local neuronal activity and the resulting blood flow changes and has only partially known dynamic and nonlinear characteristics. Moreover, besides the activity of interest, fUS records a mixture of other ongoing brain activity, physiological artifacts and noise.

The goal of this research is to develop tensor-based source separation techniques in order to estimate the brain's hemodynamic response function (HRF) to stimuli and the activity of interest by learning its nonlinear coupling with the fUS signal. Tensors are a natural mathematical representation of the obtained fUS data; e.g. 2D images over time, or 3D images over time or across different subjects. The specific challenges to solve include:

- Characterizing the HRF in terms of a (non)linear parametric model,
- Adapting functional image processing techniques so that they can (a) act on high-dimensional data, exploiting the low-rank property of the images, (b) incorporate a parametric model of the HRF and (c) perform efficient joint decomposition of multiple images that are not acquired simultaneously but pairwise share spatial characteristics,
- Improving the preprocessing stage of the tensor data: current clutter-filtering techniques based on the singular value decomposition act on unfolded (matricized) data, destroying the spatial dependencies between neighboring voxels in the images.

Relative Kinematics Estimation Using Accelerometer Measurements

Anurodh Mishra

CAS Group, Department of Microelectronics
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
a.mishra@tudelft.nl

Raj Thilak Rajan

CAS Group, Department of Microelectronics
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
r.t.rajan@tudelft.nl

ABSTRACT

For a network of mobile nodes, the problem of estimation of relative kinematics, given pairwise distances between the nodes, has received limited attention in literature. In this context, relative kinematics includes relative position, relative velocity and other higher order kinematic parameters defined with respect to a common frame of reference within the network. For numerous application domains in engineering, the nodes are highly dynamic, making the estimation task much harder. To solve the estimation problem uniquely, conventional methods either require the positions of some nodes of the mobile network to be known [2] or impose rigid body constraints on the mobile network [3]. These conditions limit the scope of proposed methods. Given a network of mobile nodes and time-varying pairwise distance measurements, we introduce a time-varying Grammian-based data model under the assumption that the mobile nodes have polynomial trajectories. Using the results in [4] and [5], estimators are proposed to estimate the relative kinematic parameters. Furthermore, we consider a scenario where the nodes have on-board accelerometers and the mobile nodes are holonomic. Under such assumptions, the proposed data model is extended to include these accelerometer measurements, leading to improvements in relative kinematics estimation. We conduct simulations to showcase the performance of the proposed estimators, which show improvement against state-of-the-art methods.

Results and Discussion: Simulations are carried out for a network of 10 mobile nodes. In the comparison shown in Figure 1, the mobile nodes are assumed to be moving with constant velocity. The root-mean-square-error (RMSE) of the relative kinematic parameters show improvement against the state-of-the-art (SOTA) in [3] for varying number of data points used, denoted by K . Figure 2 shows the RMSE errors on the relative kinematic parameters when the mobile nodes are assumed to be moving with a constant acceleration and

This work is partially funded by the European Leadership Joint Undertaking (ECSEL JU), under grant agreement No 876019, the ADACORSA project - "Airborne Data Collection on Resilient System Architectures."
This work is submitted to EUSIPCO 2022 [1].

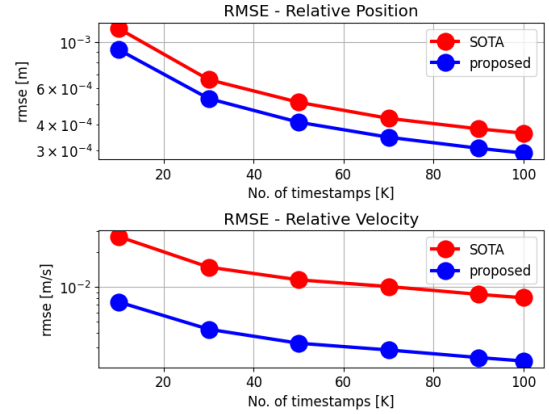


Fig. 1. Constant velocity case - RMSE on the relative kinematic estimates for varying K

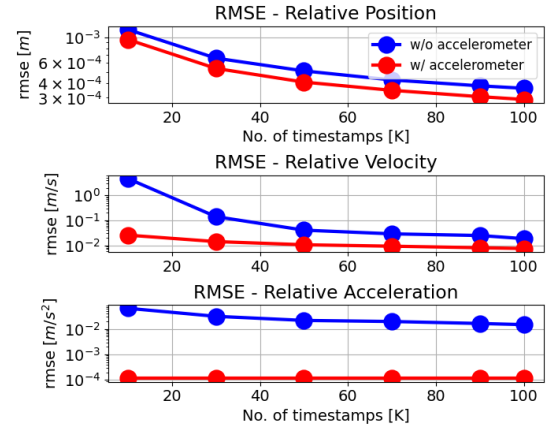


Fig. 2. Constant acceleration case - RMSE on the relative kinematic estimates for varying K with and without accelerometer measurements

each node is equipped with an accelerometer. The red curve shows the RMSE on the relative kinematics using the extended data model that fuses the accelerometer measurements with the originally proposed data model, shown in blue. The fusion of accelerometer measurements shows significant improvement in RMSE for the relative kinematic estimates.

REFERENCES

- [1] A. Mishra and R. T. Rajan, "Relative kinematics estimation using accelerometer measurements," <https://arxiv.org/pdf/2112.07307.pdf>, 2022.
- [2] P. Tabaghi, I. Dokmanić, and M. Vetterli, "Kinetic Euclidean distance matrices," *IEEE Transactions on Signal Processing*, vol. 68, 2020.
- [3] R. T. Rajan, G. Leus, and A.-J. van der Veen, "Relative kinematics of an anchorless network." *Signal Processing, Vol. 157, pp. 266-279, ISSN 0165-1684.*, 2019.
- [4] I. Borg and P. J. Groenen, *Modern multidimensional scaling: Theory and applications*. Springer Science & Business Media, 2005.
- [5] K.-W. E. Chu, "Symmetric solutions of linear matrix equations by matrix decompositions." *Linear Algebra Appl.*, vol. 119, pp. 35–50, 1989.

On the Integration of Acoustics and LiDAR: a Multi-Modal Approach to Acoustic Reflector Estimation

1st Ellen Riemens

Circuits and Systems (CAS) Group
Delft University of Technology
Delft, The Netherlands
E.H.J.riemens@tudelft.nl

2nd Pablo Martínez-Nuevo

Acoustics & Research
Bang & Olufsen
Struer, Denmark
PMN@bang-olufsen.dk

3rd Jorge Martinez

Circuits and Systems (CAS) Group
Delft University of Technology
Delft, The Netherlands
J.A.Martinez@tudelft.nl

4th Martin Møller

Acoustics & Research
Bang & Olufsen
Struer, Denmark
MIM@bang-olufsen.dk

5th Richard C. Hendriks

Circuits and Systems (CAS) Group
Delft University of Technology
Delft, The Netherlands
R.C.Hendriks@tudelft.nl

This work is accepted for EUSIPCO 2022.

Abstract—Loudspeakers are usually placed in an environment unknown to the loudspeaker designers. Having knowledge on the room acoustic properties, e.g., the location of acoustic reflectors, allows to better reproduce the sound field as intended. Current state-of-the-art methods for room boundary detection using microphone measurements typically focus on a two-dimensional setting, causing a model mismatch when employed in real-life scenarios. Detection of arbitrary reflectors in three dimensions encounters practical limitations, e.g., the need for a spherical array and the increased computational complexity. Moreover, loudspeakers may not have an omnidirectional directivity pattern, as usually assumed in the literature, making the detection of acoustic reflectors in some directions more challenging.

A smart loudspeaker system is considered, where a spherical microphone array is located on the loudspeaker as well as a computation module. It is possible to take advantage of the presence of other sensing modalities like LiDAR to detect walls more accurately. This could be done using point clouds that give direct depth information and can be used to detect planes.

In the proposed method, a LiDAR sensor is added to a smart loudspeaker to improve wall detection accuracy and robustness. This is done in two ways. First, the model mismatch introduced by horizontal reflectors can be resolved by detecting reflectors with the LiDAR sensor to enable elimination of their detrimental influence from the 2D problem in pre-processing. Second, a LiDAR-based method is proposed to compensate for the challenging directions where the directive loudspeaker emits little energy. We show via simulations that this multi-modal approach, i.e., combining microphone and LiDAR sensors, improves the robustness and accuracy of wall detection.

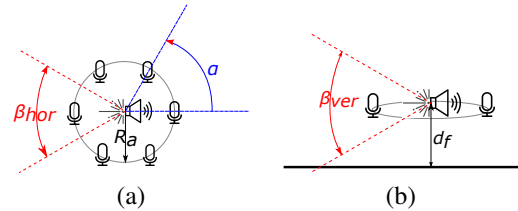


Fig. 1. The loudspeaker is modelled as a directive point source located at the origin where the front is positioned at $\alpha = 0^\circ$, i.e., in the positive horizontal direction. The LiDAR sensor is also located at the origin, but its front is directed towards the negative horizontal direction. We denote its Field-of-View (FOV) by $\beta_{\text{hor}} \times \beta_{\text{ver}}$. A UCA containing M microphones surrounds the loudspeaker and the LiDAR sensor at distance R_a . (a) Top view; (b) Side view.

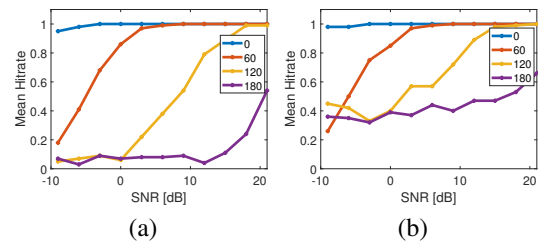


Fig. 2. (a) Acoustic reflector detection performance using acoustic information (Zaccà 2021) over 100 Monte-Carlo runs. For each angle α of the wall normal vector the mean hitrate is shown for several SNR values at fixed distance. (b) Acoustic reflector detection performance using the proposed method. For reflectors coinciding with the LiDAR FOV, i.e., at angles 120° and 180° , the detection rate at low SNR improves.

Extreme Precipitation Nowcasting using Deep Generative Models

Haoran Bi^{*§}, Maksym Kyryliuk^{*§}, Zhiyi Wang^{*§}, Cristian Meo^{*}, Yanbo Wang^{*},
Ruben Imhoff[†], Remko Uijlenhoet^{*} and Justin Dauwels^{*}

^{*}Delft University of Technology, Netherlands

[†]Deltares, Netherlands

Abstract—Extreme precipitation usually leads to substantial impacts. Floods in the Netherlands, Belgium and Germany in the summer of 2021 have caused loss of lives, destruction of infrastructures, and long-term effect on economics. To avoid such disasters, it is important to develop a reliable and accurate method to predict heavy rain.

Nowcasting is an observation-based method, which uses observations of the current state of the atmosphere to forecast future weather conditions, with statistical and optical-flow techniques, up to several hours in the future. Currently, there are two main pathways in nowcasting. The first are the conventional nowcasting methods, consisting of field-based methods, object-oriented methods and analogue-based methods. A number of these methods are included in PySTEPS, an open-source framework considered the state of the art in nowcasting [1]. Second, deep-learning models play a key role in the nowcasting field due to their strong regression ability. Various approaches to do nowcasting with Recurrent Neural Network (RNN) and Generative Adversarial Network (GAN) variants also lead to skilful predictions. Among them, DeepMind introduced a GANs network with two discriminators and convolution GRU as a generator [2]. This model can extract both spatial and temporal features and outperforms PySTEPS in overall performance. Nowcasting results from deep-learning models and PySTEPS show that deep-learning nowcasting methods lead to a lower bias and shorter processing time than PySTEPS. However, current nowcasting models are only sufficient for modelling normal weather conditions, but they are not suitable for extreme weather conditions due to the imbalance in the dataset. The imbalance originates from the skewed distribution of rainfall, which predominantly has zero rainfall and only few high-intensity amounts.

The focus of the study is on developing a deep generative model for nowcasting and incorporating extreme event-related conditions and constraints for better extreme rainfall forecasting. The proposed model was inspired by previous research in visual synthesis [3]. The model (shown in Figure 1) makes use of a two-stage structure: the first stage is a Vector Quantization Variational Autoencoder (VQ-VAE) which compresses the original input into a low-dimensional latent space. The second stage is an autoregressive transformer which predicts the future weather map’s latent space. For better modelling of extreme events, Extreme Value Loss (EVL) proposed in [4] is incorporated with the proposed model. In addition, a memory module is introduced for the transformer in the second stage to memorize historical extreme events that happened in particular catchments.

The model was tested and validated on the KNMI radar

[§]Equal contribution

dataset from 2008 to 2021, which includes 5-min precipitation accumulations over the Netherlands with a 1-km spatial resolution. The emphasis of the study is on 3-hour rainy events, and the extreme events are defined based on the precipitation intensity of 12 catchment areas across the Netherlands. Specifically, an event is labelled extreme if one of the catchments has a 3-hour precipitation amount that is among the top 1% of this catchment’s historical 3-hour precipitation sums. The model receives precipitation maps 30 minutes before the event as input to predict the precipitation maps for the following 3 hours, with a time interval of 30 minutes. The results are compared with PySTEPS, GAN and RNN models from the literature based on the Critical Success Index (CSI), Pearson Correlation Factor (PCF) and Fractions Skill Score (FSS). In addition, to identify whether extreme events are detected, the average precipitation of particular catchments is compared.

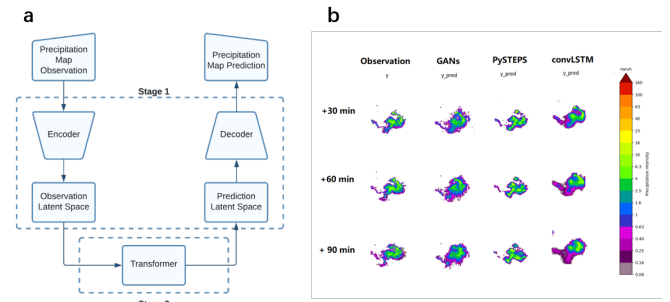


Fig. 1. (a) Proposed model structure. (b) Example prediction of precipitation intensity for 30, 60 and 90 min using nowcasting methods GAN, PySTEPS and convLSTM [1], [5], [6].

REFERENCES

- [1] S. Pulkkinen et al., “Pysteps: an open-source Python library for probabilistic precipitation nowcasting (v1.0),” *Geosci. Model Dev.*, vol. 12, no. 10, pp. 4185–4219, Oct. 2019.
- [2] S. Ravuri et al., “Skilful precipitation nowcasting using deep generative models of radar,” *Nature*, vol. 597, no. 7878, pp. 672–677, Sep. 2021.
- [3] C. Wu et al., “NUWA: Visual Synthesis Pre-training for Neural visUal World creAtion,” Nov. 2021.
- [4] D. Ding, M. Zhang, X. Pan, M. Yang, and X. He, “Modeling Extreme Events in Time Series Prediction,” in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 1114–1122.
- [5] J. R. Jing, Q. Li, X. Y. Ding, N. L. Sun, R. Tang, and Y. L. Cai, “AENN: A GENERATIVE ADVERSARIAL NEURAL NETWORK FOR WEATHER RADAR ECHO EXTRAPOLATION,” *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. XLII-3/W9, pp. 89–94, Oct. 2019.
- [6] X. Shi, Z. Chen, H. Wang, D.-Y. Yeung, W. Wong, and W. Woo, “Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting,” Jun. 2015.

Approximate quantum encryption with faster key expansion

Mehmet Hüseyin Temel and Boris Škorić

Eindhoven University of Technology

m.h.temel@tue.nl, b.skoric@tue.nl

Abstract

Perfect encryption of a qubit state using the Quantum One-Time Pad (QOTP) requires 2 classical key bits. More generally, perfect encryption of a 2^n -dimensional state requires $2n$ classical bits. However, *almost-perfect* encryption, with information-theoretic security, can be achieved with only little more than 1 key bit per qubit. It has been shown that key length $n + 2 \log \frac{1}{\varepsilon}$ suffices to encrypt n qubits in such a way that the cipherstate has trace distance $\leq \varepsilon$ from the fully mixed state. In this paper, we present a fast key expansion method to create a $2n$ -bit pseudorandom string which is then used as a QOTP key. In this expansion we make use of $2n$ bits of public randomness which are included as a classical part of the cipherstate. Our key expansion is a factor 2 faster than the previous fastest scheme, while achieving the shortest known key length $n + 2 \log \frac{1}{\varepsilon}$.

1 Introduction

1.1 Encryption of quantum states

An encryption scheme is called *perfect* if the ciphertext reveals no information whatsoever about the message that was encrypted. In the case of classical messages, the length of the key required to achieve perfect encryption is at least the Shannon entropy of the message. The Vernam cipher [Ver18] (also known as One-Time Pad, OTP) performs a bitwise **xor** of an n -bit message and an n -bit key; it achieves perfect encryption for any probability distribution of the message.

An equivalent of the Vernam cipher exists for the encryption of *quantum states* [AMTdW00, BR03, Leu02]. This is known as the quantum Vernam cipher, Quantum One-Time Pad (QOTP) or private quantum channel. In order to perfectly encrypt any n -qubit state, the necessary and sufficient key length is $2n$ bits. In its simplest form, QOTP encryption and decryption work by applying to each individual qubit a Pauli operation from the set $\{1, \sigma_x, \sigma_y, \sigma_z\}$. The choice of Pauli operations constitutes the key. For someone who does not know this key, the state after encryption equals the fully mixed state regardless of the original state.

It is possible to get ε -close to the fully mixed state by a randomization process that takes fewer than $2n$ key bits [HLSW04, AS04, DN06, Aub09, ŠdV17]. This is called *approximate randomization* or *almost-perfect encryption*. The ‘ ε -close’ property can be expressed as a distance with respect to different norms, e.g. the 1-norm (trace norm) or the ∞ -norm (maximum absolute eigenvalue). In this paper, we consider only the 1-norm, since it expresses the indistinguishability of states and it is a universally composable measure of security [Can01, BOHL⁺05, FS09]. Table 1 summarizes known results on approximate randomization, including this work, focusing on the 1-norm.

Approximate randomization is related to quantum encryption with *entropic security* [Des09, DD10]. Entropically secure encryption needs assumptions on the adversary’s prior knowledge about the plaintext. The approximate randomization scenario is the special case where it is known that Eve is not entangled with the plaintext state, but no other assumption is made. In the current paper, we will not consider entropic security in general.

Hayden et al. [HLSW04] showed that approximate randomization is possible with a key length of $n + \log n + 2 \log \frac{1}{\varepsilon}$ by using sets of random unitaries.¹ Random selection and storage of unitary matrices are very inefficient. Ambainis and Smith [AS04] introduced far more efficient schemes that work with a pseudorandom sequence that selects Pauli operators as in the QOTP. In one of them, they expand the

¹They also provide a result for the ∞ -norm, with key length $n + \log n + 2 \log \frac{1}{\varepsilon} + \log 134$; unitaries are drawn from the Haar measure. This was later improved to $n + 2 \log \frac{1}{\varepsilon} + \log 150$ by Aubrun [Aub09].

	Key length ℓ	Ciphertext length	Randomization process
[HLSW04]	$n + \log n + 2 \log \frac{1}{\varepsilon}$	n qubits	Random unitaries (non-Haar, e.g. Pauli)
[AS04]	$n + 2 \log n + 2 \log \frac{1}{\varepsilon}$	n qubits	Pseudorandom QOTP based on small-bias sets. Key expansion takes $\mathcal{O}(n^2)$ operations.
[AS04]	$n + 2 \log \frac{1}{\varepsilon}$	n qubits + $2n$ bits	Pseudorandom QOTP based on multiplication in $\text{GF}(2^{2n})$. Key expansion takes $\approx 6n \log_3 n$ operations.
[DN06]	$n + 2 \log \frac{1}{\varepsilon} + 4$	n qubits	Pseudorandom QOTP based on small-bias spaces. Key expansion takes $\mathcal{O}(n^2 \log n)$ operations.
[ŠdV17]	$n + 2 \log \frac{1}{\varepsilon}$	n qubits	Pseudorandom QOTP based on huge Common Reference String.
This paper	$n + 2 \log \frac{1}{\varepsilon}$	n qubits + $2n$ bits	Pseudorandom QOTP based on affine function in $\text{GF}(2^\ell)$. Key expansion takes $\approx 3n \log_3 n$ operations.

Table 1: *Results on almost-perfect encryption of n qubits, with security definition in terms of the trace distance: $\|\text{cipherstate} - \text{fully mixed state}\|_1 \leq \varepsilon$. The listed complexity for the finite field multiplications is based on the fastest known implementation and shows only the number of AND operations. (See Section 3.3).*

key using small-bias sets and achieve key length $n + 2 \log n + 2 \log \frac{1}{\varepsilon}$. This scheme is length-preserving, i.e. the cipherstate consists of n qubits. In another construction, they expand the key by multiplying it with a random binary string of length $2n$; this string becomes part of the cipherstate. The key length is reduced to $n + 2 \log \frac{1}{\varepsilon}$. Dickinson and Nayak [DN06] improved the small-bias based scheme of [AS04] and achieved key length $n + 2 \log \frac{1}{\varepsilon} + 4$. Škorić and de Vries [ŠdV17] described a pseudorandom QOTP scheme that has key length $n + 2 \log \frac{1}{\varepsilon}$, but they need an exponentially large common random string to be stored somewhere.

In all the schemes that expand the key, the expansion can be done efficiently, with time complexity $\mathcal{O}(n^2 \log n)$ or better, because these schemes are based on Galois field multiplication which takes $\mathcal{O}(n \log n)$ time (see e.g. Theorem 8.7 in [AHU74] and its corollary).

1.2 Contribution and outline

We modify the second scheme of Ambainis and Smith [AS04]. Instead of expanding the key by multiplying in $\text{GF}(2^{2n})$, we append to the key an affine function of the key. The two parameters of the affine function are drawn at random and become part of the cipherstate. The resulting encryption scheme still has key length $\ell = n + 2 \log \frac{1}{\varepsilon}$, which is the shortest length presented in the literature. The cipherstate consists of n qubits and $2n$ classical bits.² The key expansion is roughly twice as fast as [AS04] because we multiply in $\text{GF}(2^\ell)$ instead of $\text{GF}(2^{2n})$.

The outline of the paper is as follows. In Section 2.1 we introduce notation, and in Section 2.2 the desired ‘ ε -randomizing’ security property is specified. The QOTP is briefly recalled in Section 2.3. In Section 3 we give the details of our construction, the security proof and the complexity of the key expansion. We conclude with a brief discussion in Section 4.

2 Preliminaries

2.1 Notation

Expectation over a random variable X is written as \mathbb{E}_x . We denote the space of density matrices on Hilbert space \mathcal{H} as $\mathcal{D}(\mathcal{H})$. The single-qubit Hilbert space is \mathcal{H}_2 . A bipartite state comprising

²We do not consider the additional $2n$ bits to be costly. Classical storage and transmission are ‘for free’ compared to quantum resources.

subsystems ‘A’ and ‘B’ is written as $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The state of a subsystem is obtained by taking the partial trace over the other subsystem, e.g. $\rho^A = \text{tr}_B \rho^{AB}$. The identity operator on \mathcal{H} is denoted by $\mathbb{1}_{\mathcal{H}}$; we will simply write $\mathbb{1}$ when the Hilbert space is clear from the context. Similarly we write $\tau^{\mathcal{H}}$ for the fully mixed state $\mathbb{1}_{\mathcal{H}}/\dim(\mathcal{H})$, often omitting the superscript. Let M be an operator with eigenvalues λ_i . The Schatten 1-norm of M is given by $\|M\|_1 = \text{tr} \sqrt{M^\dagger M} = \sum_i |\lambda_i|$. The induced ‘trace’ distance between states ρ, σ is $\|\rho - \sigma\|_1$.

2.2 Security definitions

We use standard definitions of encryption and ε -randomization.

Definition 2.1 (Encryption scheme) *An encryption scheme with classical key space \mathcal{K} , quantum message space \mathcal{H} and quantum ciphertext space \mathcal{H}' consists of a pair (Enc, Dec) . Here $\text{Enc}: \mathcal{K} \times \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}')$ is a (possibly randomized) algorithm that takes as input a classical key $k \in \mathcal{K}$ and a quantum state $\varphi \in \mathcal{D}(\mathcal{H})$, and outputs a quantum state $\omega = \text{Enc}(k, \varphi) \in \mathcal{D}(\mathcal{H}')$ called the ciphertext. $\text{Dec}: \mathcal{K} \times \mathcal{D}(\mathcal{H}') \rightarrow \mathcal{D}(\mathcal{H})$ is an algorithm that takes as input a key $k \in \mathcal{K}$ and a state $\omega \in \mathcal{D}(\mathcal{H}')$, and outputs a state $\text{Dec}(k, \omega) \in \mathcal{D}(\mathcal{H})$. It must hold that $\forall_{k \in \mathcal{K}, \varphi \in \mathcal{D}(\mathcal{H})} \text{Dec}(k, \text{Enc}(k, \varphi)) = \varphi$.*

Note that Def. 2.1 allows the ciphertext space to be larger than the plaintext space, $\dim \mathcal{H}' > \dim \mathcal{H}$. We will be working with the special case where the ciphertext consists of a quantum state of the same dimension as the input (n qubits), accompanied by classical information.

The effect of the encryption, with the key unknown to the adversary, can be described as a completely positive trace preserving (CPTP) map $R: \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}')$ as follows,

$$R(\varphi) = \sum_{k \in \mathcal{K}} \frac{1}{|\mathcal{K}|} \text{Enc}(k, \varphi). \quad (1)$$

Definition 2.2 (ε -Randomizing) *Let $\varepsilon \geq 0$. A CPTP linear operator $R: \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}')$ is said to be ε -randomizing with respect to a norm $\|\cdot\|$ if*

$$\forall_{\varphi \in \mathcal{D}(\mathcal{H})} \quad \left\| R(\varphi) - \tau^{\mathcal{H}'} \right\| \leq \varepsilon. \quad (2)$$

We say that R is completely randomizing if $\varepsilon = 0$.

Def. 2.2 is a slight modification of Def. 1.1 in [DN06]; the difference is that we allow $\dim \mathcal{H}' \neq \dim \mathcal{H}$.

It is important to note that randomization as specified in Def. 2.2 implies that $R(\varphi)$ is practically independent of any Eve who is correlated only *classically* with φ . Let $\rho^{E\Phi}$ denote the bipartite state of Eve and the quantum ‘plaintext’ state. We write $\varphi = \rho^\Phi = \text{tr}_E \rho^{E\Phi}$. Without entanglement between the E and Φ subsystems, the state is separable, $\rho^{E\Phi} = \sum_k p_k \rho_k^E \otimes \varphi_k$. We write $\tau = \tau^{\mathcal{H}'}$. Furthermore Φ' denotes the result of the operation R on the Φ subsystem, and we write $\varphi' = R(\varphi)$. Repeated use of the triangle inequality, followed by (2) yields $\|\rho^{E\Phi'} - \rho^E \otimes \varphi'\| = \|\sum_k p_k \rho_k^E \otimes (\varphi_k - \varphi')\| \leq \sum_k p_k \|\varphi_k - \varphi'\| = \sum_k p_k \|\varphi_k - \tau + \tau - \varphi'\| \leq \sum_k p_k \|\varphi_k - \tau\|_1 + \sum_k p_k \|\tau - \varphi'\| \leq 2\varepsilon$.

Just as the earlier works [HLSW04, AS04, DN06, ŠdV17] we will use Def. 2.2 (with the 1-norm) as our security definition.

2.3 The Quantum One Time Pad (QOTP)

Let \mathcal{H}_2 denote the Hilbert space of a qubit. Let Z and X be single-qubit Pauli operators, in the standard basis given by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. For QOTP encryption of one qubit, the key consists of two bits $s, t \in \{0, 1\}$. The encryption of a state $\varphi \in \mathcal{D}(\mathcal{H}_2)$ is given by $X^s Z^t \varphi Z^t X^s$. Decryption is the same operation as encryption. For someone who does not know the key, the state after encryption is $\frac{1}{4} \sum_{s, t \in \{0, 1\}} X^s Z^t \varphi Z^t X^s = \mathbb{1}/2$ for any φ . Hence the QOTP is completely randomizing.

The simplest way to encrypt an n -qubit state $\varphi \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ is to encrypt each qubit independently. The key is $\beta = (\beta_1, \dots, \beta_n) \in \{0, 1\}^{2n}$, with $\beta_i = (s_i, t_i)$. In the rest of the paper we will use the following shorthand notation for the QOTP ciphertext,

$$F_\beta(\varphi) = U_\beta \varphi U_\beta^\dagger \quad \text{where } U_\beta = \bigotimes_{i=1}^n X^{s_i} Z^{t_i}. \quad (3)$$

It holds that $2^{-2n} \sum_{\beta \in \{0, 1\}^{2n}} F_\beta(\varphi) = \mathbb{1}/2^n$ for any $\varphi \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$.

3 Our result on approximate randomization

3.1 The construction

We encrypt an n -qubit state $\varphi \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ using a key $k \in \{0, 1\}^\ell$ where $\ell > n$, and ℓ is an even integer. We construct a pseudorandom sequence $b \in \{0, 1\}^{2n}$ by expanding $k \in \{0, 1\}^\ell$ as follows. Two strings $u \in \{0, 1\}^\ell$, $v \in \{0, 1\}^{2n-\ell}$ are drawn at random. They are interpreted as elements of $\text{GF}(2^\ell)$. Note that $2n - \ell < n$. The string b is constructed by concatenating k with an affine function of k ,

$$b(k, u, v) = k \parallel (uk + v)_{\text{lsb}}. \quad (4)$$

The subscript ‘lsb’ (Least Significant Bits) stands for taking the last $2n - \ell$ bits of the string; in the finite field representation, this corresponds to taking a polynomial in x modulo $x^{2n-\ell}$. In (4) the multiplication and addition are operations in $\text{GF}(2^\ell)$. Instead of $(uk + v)_{\text{lsb}}$ we can also write $(uk)_{\text{lsb}} + v$. The cipherstate is given by

$$\text{Enc}(k, \varphi) = \left(u, v, F_{b(k, u, v)}(\varphi) \right) \quad (5)$$

with F the QOTP encryption as defined in (3) and $b(\cdot, \cdot, \cdot)$ as defined by (4). The parameters u, v are a *classical* part of the cipherstate.

3.2 Security proof

Eve sees the parameters u, v but she does not know k . From her point of view the state of the qubits is

$$R_{uv}(\varphi) \stackrel{\text{def}}{=} \frac{1}{2^\ell} \sum_{k \in \{0, 1\}^\ell} F_{b(k, u, v)}(\varphi). \quad (6)$$

Lemma 3.1 *It holds that*

$$\mathbb{E}_{uv} R_{uv}(\varphi) = \tau. \quad (7)$$

Proof: We write $\mathbb{E}_{uv} R_{uv}(\varphi) = \mathbb{E}_u [\mathbb{E}_{kv} F_{b(k, u, v)}(\varphi)]$. Next, $\mathbb{E}_{kv} F_{b(k, u, v)}(\varphi) = \mathbb{E}_{\beta \in \{0, 1\}^{2n}} F_\beta(\varphi) = \tau$. The first equality follows from the fact that for any fixed u , the k and v together can create any string in $\{0, 1\}^{2n}$ in precisely one way. The second equality is due to the fact that the QOTP is completely randomizing. \square

Lemma 3.2 *Let f be any (possibly operator valued) function acting on $\{0, 1\}^{2n}$. It holds that*

$$\mathbb{E}_{kk'uv} f(b(k, u, v)) f(b(k', u, v)) = 2^{-\ell} \mathbb{E}_\beta f(\beta) f(\beta) + \mathbb{E}_{\beta\beta'} f(\beta) f(\beta') - 2^{-\ell} \mathbb{E}_{kgg'} f(k \parallel g) f(k \parallel g'). \quad (8)$$

Here $\beta, \beta' \in \{0, 1\}^{2n}$, and \mathbb{E}_β stands for $2^{-2n} \sum_\beta$. Similarly, $g, g' \in \{0, 1\}^{2n-\ell}$ and \mathbb{E}_g stands for $2^{\ell-2n} \sum_g$.

Proof: We first look at the summation terms with $k' \neq k$. We write $b(k, u, v) = k \parallel g$ and $b(k', u, v) = k' \parallel g'$. Consider k, k' fixed. For every combination (g, g') there are exactly $2^{2\ell-2n}$ values of (u, v) that yield $(uk)_{\text{lsb}} + v = g$, $(uk')_{\text{lsb}} + v = g'$.³ This allows us to rewrite the summations as

$$\sum_{kk': k' \neq k} \sum_{uv} f(b(k, u, v)) f(b(k', u, v)) = 2^{2\ell-2n} \sum_{kk': k' \neq k} \sum_{gg'} f(k \parallel g) f(k' \parallel g') \quad (9)$$

$$= 2^{2\ell-2n} \left(\sum_{kgg'} f(k \parallel g) f(k' \parallel g') - \sum_{kgg'} f(k \parallel g) f(k \parallel g') \right). \quad (10)$$

Next we look at the $k' = k$ terms. The summation over k and v spans all the possible β 's. Hence we can write

$$\sum_k \sum_{uv} f(b(k, u, v)) f(b(k, u, v)) = \sum_u \sum_\beta f(\beta) f(\beta). \quad (11)$$

³When the two equations are added the v disappears and we get $[u(k+k')]_{\text{lsb}} = g+g'$, which has $2^\ell/2^{2n-\ell}$ solutions u . Then, at fixed k, k', g, g', u the solution for v is unique.

Combining the $k' = k$ and $k' \neq k$ parts we get

$$\sum_{kk'uv} f(b(k, u, v))f(b(k', u, v)) = 2^\ell \sum_{\beta} f(\beta)f(\beta) + 2^{2\ell-2n} \sum_{\beta\beta'} f(\beta)f(\beta') - 2^{2\ell-2n} \sum_{kgg'} f(k\|g)f(k\|g'). \quad (12)$$

In order to go from summations to expectations we divide (12) by a factor $(2^\ell)^3 2^{2n-\ell} = 2^{2\ell+2n}$. \square

Theorem 3.3 *The randomizing map $R_{uv} : \mathcal{D}(\mathcal{H}_2^{\otimes n}) \rightarrow \mathcal{D}(\mathcal{H}_2^{\otimes n})$ as described in (6) satisfies*

$$\forall_{\varphi \in \mathcal{D}(\mathcal{H}_2^{\otimes n})} \quad \mathbb{E}_{uv} \|R_{uv}(\varphi) - \tau\|_1 < \sqrt{2^{n-\ell}}. \quad (13)$$

Proof: For any φ we have

$$\mathbb{E}_{uv} \|R_{uv}(\varphi) - \tau\|_1 = \mathbb{E}_{uv} \text{tr} \sqrt{(R_{uv}(\varphi) - \tau)^2} \quad (14)$$

$$\stackrel{\text{Jensen}}{\leq} \text{tr} \sqrt{\mathbb{E}_{uv} (R_{uv}(\varphi) - \tau)^2} \quad (15)$$

$$\stackrel{\text{Lemma 3.1}}{=} \text{tr} \sqrt{\mathbb{E}_{uv} [R_{uv}(\varphi)]^2 - \tau^2} \quad (16)$$

$$= \text{tr} \sqrt{\mathbb{E}_{uv} \mathbb{E}_{kk'} F_{b(k,u,v)}(\varphi) F_{b(k',u,v)}(\varphi) - \tau^2} \quad (17)$$

$$\stackrel{\text{Lemma 3.2}}{=} \text{tr} \sqrt{2^{-\ell} \mathbb{E}_{\beta} F_{\beta}(\varphi) F_{\beta}(\varphi) - 2^{-\ell} \mathbb{E}_k [\mathbb{E}_g F_{k\|g}(\varphi)] [\mathbb{E}_{g'} F_{k\|g'}(\varphi)]}. \quad (18)$$

In the last step we used $\mathbb{E}_{\beta\beta'} F_{\beta}(\varphi) F_{\beta'}(\varphi) = \tau^2$. Next we use $F_{\beta}(\varphi) F_{\beta}(\varphi) = F_{\beta}(\varphi^2)$ and $\mathbb{E}_{\beta} F_{\beta}(\varphi^2) = \tau \text{tr}(\varphi^2)$, yielding

$$\mathbb{E}_{\beta} F_{\beta}(\varphi) F_{\beta}(\varphi) = \tau \text{tr}(\varphi^2). \quad (19)$$

Furthermore we write $\varphi = \sum_{abcd} \varphi_{abcd} |e_a^L e_b^R\rangle \langle e_c^L e_d^R|$ where the index ‘L’ stands for the first $\ell/2$ qubits⁴ and ‘R’ stands for the final $n - \ell/2$ qubits; e^L is a basis for the L subsystem and likewise e^R for R. The marginal state of the L-subsystem is given by $\varphi^L = \text{tr}_R \varphi = \sum_{ac} (\sum_{bd} \varphi_{abcd}) |e_a^L\rangle \langle e_c^L|$. We note that $\mathbb{E}_g F_{k\|g}(\varphi) = F_k(\varphi^L) \otimes \tau^R$, which gives

$$\mathbb{E}_k [\mathbb{E}_g F_{k\|g}(\varphi)] [\mathbb{E}_{g'} F_{k\|g'}(\varphi)] = \mathbb{E}_k F_k(\varphi^L) F_k(\varphi^L) \otimes (\tau^R)^2 = \tau^L \otimes (\tau^R)^2 \text{tr}_L((\varphi^L)^2). \quad (20)$$

We substitute (19) and (20) into (18). Since the operator under the square root is diagonal, the $\text{tr} \sqrt{\dots}$ is readily computed and gives

$$\mathbb{E}_{uv} \|R_{uv}(\varphi) - \tau\|_1 \leq \sqrt{2^{n-\ell} \text{tr} \varphi^2 - 2^{-\ell/2} \text{tr}(\varphi^L)^2} \quad (21)$$

$$\leq \sqrt{2^{n-\ell} - 2^{-\ell}} \quad (22)$$

$$< \sqrt{2^{n-\ell}}. \quad (23)$$

In (22) we used $\text{tr} \varphi^2 \leq 1$ and $\text{tr}(\varphi^L)^2 \geq 2^{-\ell/2}$. \square

Theorem 3.4 *Our scheme is ε -randomizing (Def. 2.2) with respect to the 1-norm when the key length is set to $\ell = n + 2 \log \frac{1}{\varepsilon}$.*

Proof: From the adversary’s point of view the cipherstate is $\mathbb{E}_{uv} |uv\rangle \langle uv| \otimes R_{uv}(\varphi)$. We have to prove that this is ε -close to the fully mixed state on the *whole* output space, i.e. to $\mathbb{E}_{uv} |uv\rangle \langle uv| \otimes \tau$. We get

$$\left\| \mathbb{E}_{uv} |uv\rangle \langle uv| \otimes [R_{uv}(\varphi) - \tau] \right\|_1 = \mathbb{E}_{uv} \|R_{uv}(\varphi) - \tau\|_1 \stackrel{\text{Th. 3.3}}{\leq} \sqrt{2^{n-\ell}}. \quad (24)$$

Substituting $\ell = n + 2 \log \frac{1}{\varepsilon}$ into the final expression yields ε . \square

⁴Here we use that ℓ is even.

3.3 Complexity of the key expansion

We briefly comment on the complexity of our key expansion compared to [AS04]. Multiplication in $\text{GF}(2^n)$ has time complexity $\mathcal{O}(n \log n)$ [AHU74, Can89] whereas addition (subtraction) consists of n XOR operations. Mateer [Mat08] introduced an improved version of Schönhage’s multiplication algorithm [Sch77]. If m is of the form 3^κ and κ is a power of two, then multiplication of two elements in $\text{GF}(2^{2^m})$ requires $\frac{17}{3}m \log_3 m$ bit-AND operations and at least $\frac{52}{5}m \log m \log(\log m) + \frac{3}{2}m \log m - \frac{3}{2}m + \frac{11}{2}\sqrt{m}$ bit-XORs. If κ is not a power of two, then the number of ANDs slightly increases to $6m \log_3 m$ while the bound on the XORs stays the same.

Our key expansion consists of one multiplication in $\text{GF}(2^\ell)$ and one addition in $\text{GF}(2^{2n-\ell})$ or, since ℓ asymptotically almost equals n , roughly speaking one multiplication and one addition in $\text{GF}(2^n)$. With Mateer’s multiplication for general κ , this yields a total cost of $3n \log_3 n - 3n \log_3 2$ ANDs and $\geq n \log n \{ \frac{26}{5} \log \log \frac{n}{2} + \frac{3}{4} \} - n \{ \frac{26}{5} \log \log \frac{n}{2} + \frac{1}{2} \} + \mathcal{O}(\sqrt{n})$ XORs for our key expansion.

In [AS04] the ℓ -bit key k is multiplied by a string $\alpha \in \{0,1\}^{2n}$, and the multiplication is in $\text{GF}(2^{2n})$. If we write $\alpha = L||R$ and take $\ell \approx n$ then this can be reorganized into the following steps: (i) a polynomial multiplication $k \cdot R$ without modular reduction; (ii) a polynomial multiplication $k \cdot L$ shifted by n positions, resulting in a polynomial of degree at most $3n$, followed by $\text{GF}(2^{2n})$ modular reduction; (iii) addition of the two above contributions. As we count two XORs per monomial that needs to be reduced⁵, we see that the addition in step (iii) precisely compensates the missing reduction in step (i). Furthermore the number of monomials that needs reducing in step (ii) is n , which is the same as in $\text{GF}(2^n)$ multiplication. Hence the cost of computing $k \cdot \alpha$ equals the cost of two $\text{GF}(2^n)$ multiplications. Since in $\text{GF}(2^n)$ multiplication is much more expensive than addition, we see that our key expansion is a factor 2 cheaper than [AS04].

4 Discussion

We get the same shortest key length $\ell = n + 2 \log \frac{1}{\epsilon}$ reported in other studies, but with a key expansion that is twice as efficient as the fastest one [AS04] in the literature. It is interesting to note that the security proof in [AS04] uses Fourier analysis and δ -biased families, and invokes Cayley graphs for intuition, whereas our proof is more straightforward.

A small improvement to our scheme could be to draw the parameter u from $\{0,1\}^{2n-\ell}$ instead of $\{0,1\}^\ell$.

It would be interesting to see how our scheme behaves regarding *entropic security* [Des09, DD10]. This is left for future work.

Acknowledgements

We thank Tanja Lange and Dan Bernstein for discussions on multiplication complexity. Part of this work was supported by the Dutch Startimpuls NAQT KAT-2 and NGF Quantum Delta NL KAT-2.

References

- [AHU74] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The design and analysis of computer algorithms*. Addison-Wesley series in computer science and information processing. Addison-Wesley Pub. Co, 1974.
- [AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.
- [AS04] A. Ambainis and A. Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 249–260. Springer, 2004.

⁵With $m = 3^\kappa$ it is possible to use the trinomial $x^{2^m} + x^m + 1$ as the irreducible polynomial, which allows for efficient reduction. If we depart from the 3^κ form, irreducible polynomials of degree 5 may become necessary, which leads to more costly modular reduction. It has been shown [BCP19] that irreducible pentanomials can be chosen such that no more than *three* XORs are required per monomial reduction.

- [Aub09] G. Aubrun. On almost randomizing channels with a short Kraus decomposition. *Communications in mathematical physics*, pages 1103–1116, 2009.
- [BCP19] G. Banegas, R. Custódio, and D. Panario. A new class of irreducible pentanomials for polynomial-based multipliers in binary fields. *Journal of Cryptographic Engineering*, 9(4):359–373, 2019.
- [BOHL⁺05] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference*, pages 386–406. Springer, 2005.
- [BR03] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.
- [Can89] D.G. Cantor. On arithmetical algorithms over finite fields. *Journal of Combinatorial Theory, Series A*, 50(2):285–300, 1989.
- [Can01] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.
- [DD10] S.P. Desrosiers and F. Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*, 56(7):3455–3464, 2010.
- [Des09] S.P. Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8(4):331–345, 2009.
- [DN06] P.A. Dickinson and A. Nayak. Approximate randomization of quantum states with fewer bits of key. In *Quantum computing: back action*, volume 864, pages 18–36. AIP, 2006.
- [FS09] S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference*, pages 350–367. Springer, 2009.
- [HLSW04] P. Hayden, D. Leung, P.W. Shor, and A. Winter. Randomizing quantum states: constructions and applications. *Commun. Math. Phys.*, 250:371–391, 2004.
- [Leu02] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.
- [Mat08] T. Mateer. *Fast Fourier transform algorithms with applications*. PhD thesis, Clemson University, 2008.
- [Sch77] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica*, 7(4):395–398, 1977.
- [ŠdV17] B. Škorić and M. de Vries. Quantum Key Recycling with 8-state encoding (The Quantum One-Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 15(03):1750016, 2017.
- [Ver18] G.S. Vernam. Secret signaling system, 1918. US Patent 1310719.

Multi-Objective Game Theory for Multi-User OFDM Integrated Radar Waveform Design

Guillaume Thiran
ICTEAM UCLouvain
Louvain-la-Neuve, Belgium
guillaume.thiran@uclouvain.be

Ivan Stupia
ICTEAM UCLouvain
Louvain-la-Neuve, Belgium
ivan.stupia@uclouvain.be

Luc Vandendorpe
ICTEAM UCLouvain
Louvain-la-Neuve, Belgium
luc.vandendorpe@uclouvain.be

I. RESEARCH GOAL AND CONTEXT

Differently from previous generations, future networks will connect a massive number of nodes requiring several metrics to be characterised accurately. Due to the multiplicity of nodes and metrics, allocating the radio resources is a challenging problem, and the information exchange required by centralised approaches might be incompatible with large scale networks. Instead, each node can be modelled as a selfish player optimising its own objectives, considering the impact of the other players as fixed. The coupling between the optimisation problems gives rise to interactions between players, which will be studied to determine whether an equilibrium point exists, and to design an algorithm reaching it while being compatible with autonomous nodes.

II. STATE-OF-THE-ART

Stemming from Multi-Objective Optimisation (MOO) and Game Theory (GT), Multi-Objective Game Theory (MOGT) provides a framework to study the above problem. On the one hand, it builds on MOO to study the equilibria of a multi-objective game, named Pareto-Nash Equilibria (PNE), by scalarising for each player their several objectives into a unique one. Under convexity assumptions, such scalarised objective is defined as the weighted sum of the objectives [1], the weights translating the players preferences. On the other hand, in the single-objective case, GT comes up with sufficient conditions ensuring the existence of an equilibrium, named Nash Equilibrium (NE), as well as its unicity. It also provides sufficient convergence conditions for an algorithm named the asynchronous Best Response Dynamics (BRD) [2] which benefits from an extremely low signalling burden and is therefore fully compatible with autonomous nodes. What is lacking however is an equivalent of the single-objective GT sufficient conditions for multi-objective games, valid whatever the player preferences.

III. CONTRIBUTIONS

Filling the above gap, our work enables to study the properties of the scalarised game NE, equivalent to the PNE of the multi-objective one, from a family of single-objective games named the *underlying games*. These latter are obtained by selecting for each player only one of its objective, the whole family being build by considering all possible selections.

Guillaume Thiran is a Research Fellow of the Fonds de la Recherche Scientifique – FNRS.

It is first shown that if all underlying games satisfy the existence conditions of [2], then any weighted sum scalarisation of the multi-objective game also benefits from this property, whatever the weights. Secondly, the equivalence between the fulfilment of underlying games unicity conditions and the fulfilment of the scalarised game unicity conditions whatever the weights is obtained. Finally, studying the convergence of the BRD, a similar statement is obtained: all underlying games satisfy the convergence conditions if and only if this is the case for the scalarised one whatever the scalarisation weights.

The above results enable to move from complicated weighted sum objectives with a continuum of scalarisation weights to a finite number of single-objective games. Moreover, many communication games have already been studied, and one can thus benefit from this literature.

IV. COMPETITIVE RADCOM WAVEFORM DESIGN

To highlight the benefits of our approach, an OFDM multi-user communication system with an integrated radar function is considered, as represented in Figure 1. Each player has two objectives, the communication throughput and the mutual information between the radar echo and the target impulse response. In this setting, we obtain conditions ensuring that whatever the preferences of the players between the two objectives, the BRD converges to a unique NE. These conditions translate into limits on the communication and radar interferences received from and emitted by players.

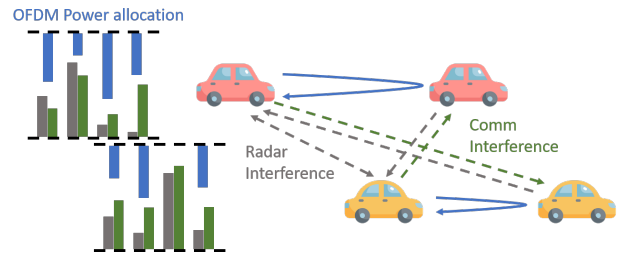


Fig. 1. OFDM integrated radar communication system. Both the communication and radar interferences of the first car are functions of the power allocation of the second car.

REFERENCES

- [1] A. Zapata, A. Mármol, L. Monroy, and M. Caraballo, "A maxmin approach for the equilibria of vector-valued games," *Group Decision and Negotiation*, vol. 28, no. 2, pp. 415–432, 2019.
- [2] G. Scutari, F. Facchinei, J.-S. Pang, and D. P. Palomar, "Real and complex monotone communication games," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 4197–4231, 2014.

Unconditional tamper evidence from short keys

(extended abstract)

Bart van der Vecht, Xavier Coiteux-Roy, Boris Škorić

Abstract

Storing data on an external server with information-theoretic security, while using a key shorter than the data itself, is impossible. As an alternative, we propose a scheme that achieves information-theoretically secure tamper evidence: The server is able to obtain information about the stored data, but not while staying undetected. Moreover, the client only needs to remember a key whose length is much shorter than the data.

We provide a security proof for our scheme, based on an entropic uncertainty relation, similar to QKD proofs. Our scheme works if Alice is able to (reversibly) randomise the message to almost-uniformity with only a short key. By constructing an explicit attack we show that short-key unconditional tamper evidence cannot be achieved without this randomisability.

1 Introduction

1.1 Delegated Storage

We look at the problem of *Delegated Storage*. Alice needs to store a large amount of data securely, but she does not have enough storage capacity herself. The typical solution is to encrypt the data and then store it on a remote (‘cloud’) server Eve. Since Alice has to remember the encryption key, this key is necessarily smaller than the data (otherwise Alice could have just stored the data herself). It is well known that information-theoretic security is possible only when the key is at least as large as the entropy of the data. Hence it is obvious that in Delegated Storage the confidentiality of the data cannot be guaranteed unconditionally, not even using quantum physics. A computationally unbounded Eve will always be able to extract information about the data from the (quantum) ciphertext.

We show that, somewhat surprisingly, it *is* possible in Delegated Storage to get information-theoretic guarantees for a security property other than confidentiality: tamper evidence (tampering detection). We present a quantum Delegated Storage scheme for classical data which makes it impossible for Eve to learn anything about Alice’s data without alerting Alice, even if Eve has unbounded powers of (quantum) computation, measurement, storage etc. Our scheme is close in spirit to QKD, and in fact it is useful to imagine Delegated Storage as a sort of QKD where Bob is ‘future Alice’ who retrieves and decrypts the stored cipherstate, and storage on the server corresponds to travelling qubits. There are some subtle differences with QKD, however, namely (i) the short encryption key, (ii) the availability of the ciphertext at the moment when Eve attacks the qubits, and (iii) Bob’s inability to send any message to Alice. These subtle differences conspire to necessitate a security proof that differs nontrivially from QKD security proofs, though many well known ingredients can be re-used.

1.2 Related work

Several works have appeared on the topic of provable deletion of remotely stored data. Coiteux-Roy and Wolf [1] introduced the task of Delegated Storage and provable deletion with a short-key requirement for both tasks. However, they did not settle the question whether unconditional tamper evidence is achievable. Independently, Broadbent and Islam [2] achieved information-theoretic security for provable deletion using keys that are as long as the message.

Lütkenhaus, Marwah and Touchette [3] use a form of Delegated Storage to store a fully-randomised bit commitment on temporarily trusted servers, with the possibility of recall. They don't require a short key in their definition and use a key as long as the message in their protocol.

The verification process in Delegated Storage involves the measurement of a quantum state by the verifier; the prover has to send this quantum state to the verifier. This is different from Provable Deletion protocols and from Molina, Vidick and Watrous's tickets variant [4] of Wiesner's quantum money, where the stored data is quantum but the communication between the prover and the verifier is classical during the verification phase.

1.3 Contributions

We define *Correctness*, *Security* and *Usefulness* for Delegated Storage. Correctness means that, in case of low disturbance of the stored quantum states, Alice should not get alerted and should be able to recover the message. Security means that Eve cannot learn a non-negligible amount of information about the stored message without alerting Alice. (This definition *does* allow Eve to learn the full message while alarming Alice.) Usefulness means that Alice's locally stored data is smaller than the remotely stored message.

Let M be the data that serves as input to the protocol; M' the data returned by Eve; $\Omega \in \{0, 1\}$ a flag that indicates if Alice notices disturbance (with $\Omega = 1$ meaning that everything looks fine). Let E denote Eve's quantum ancilla. By $\rho_{[\omega=1]}$ we mean the (sub-normalised) part of ρ that corresponds to $\omega = 1$.

ε -Correctness:

$$\text{Eve behaves honestly} \implies \Pr[\Omega = 1 \wedge \hat{M} = M] \geq 1 - \varepsilon. \quad (1)$$

ε -Security:

$$\left\| \rho_{[\omega=1]}^{MTT'E} - \mathbb{E}_m |m\rangle\langle m| \otimes \rho_{[\omega=1]}^{TT'E} \right\|_1 \leq \varepsilon. \quad (2)$$

Eq.(2) can be read as: "If $\Pr[\Omega = 1]$ is negligible then we are making no demands. If $\Pr[\Omega = 1]$ is non-negligible then we demand that M is decoupled from Eve". Note that security properties formulated in terms of the 1-norm (or trace norm) are *composable* [5, 6, 7, 8] with other (sub-)protocols.

Usefulness.

Let the message space be \mathcal{M} and the key space \mathcal{K} . We define the *usefulness* parameter $Y \leq 1$ as $Y = \frac{|\mathcal{M}| - |\mathcal{K}|}{|\mathcal{M}|}$. A positive usefulness means that the amount of data that Alice has to store locally is less than the message size.

We present CAN'TTOUCHTHIS, our Delegated Storage scheme. As a first step Alice derives, in a reversible way, an almost-uniform string M from the message μ . Our scheme requires that this randomisation step is possible without the introduction of long keys; hence the entropy of μ must be sufficiently high to allow for using an extractor, or Alice must know the distribution of μ with sufficient accuracy in order to apply compression-based randomisation techniques. Then, Alice extracts a one-time pad from a random string x ; the x is encoded into qubits. She computes a ciphertext by masking m with the one-time pad. She stores the ciphertext and the qubits on the server. In between the qubits that contain x there are 'trap' qubits in random positions. When Alice recovers the stored data, she inspects these trap states to see if they have changed.

We prove that our scheme satisfies the Correctness and Security properties. If ℓ is the message length and β_0 the bit error rate of the quantum channel, then asymptotically $n = \frac{\ell}{1-h(\beta_0)}$ qubits are required¹, and Alice has to remember a syndrome of (asymptotic) size $\ell \frac{h(\beta_0)}{1-h(\beta_0)}$; the syndrome is the main 'key' that she has to store locally. CAN'TTOUCHTHIS allows the message to be longer than the key only when $1 - 2h(\beta_0) > 0$. This inequality is familiar in Quantum Key Distribution, where it represents the condition for having positive key rate without two-way communication.

¹ h is the binary entropy function.

We propose a method for recursively applying CAN'T TOUCH THIS. The syndrome is not stored locally, but using CAN'T TOUCH THIS. The effect is that Alice has to remember a shorter key; asymptotically the number of qubits stored on the server is $n \rightarrow \frac{\ell}{1-2h(\beta_0)}$. This expression too is familiar from QKD, where it stands for the number of qubits required to generate a key of length ℓ . Our scheme needs a preprocessing step to reversibly transform the message μ into an almost-uniform string m which then serves as the ‘message’ in the quantum part of the protocol. We show that this need for a uniform input is not a deficiency of our scheme or our proof technique, but in fact a fundamental requirement. We introduce an attack called SUPPORT which tries to determine one bit: whether the plaintext is the one with the highest a-priori probability. We consider delegated storage in general *without preprocessing* and lowerbound the advantage that SUPPORT yields as a function of the key length and the min-entropy of the plaintext. This lower bound serves as a kind of ‘no go’ theorem: In the case of a low min-entropy distribution that is not known to Alice, our bound implies that the Security property cannot be achieved with a short key.

For details we refer to the full paper [9].

References

- [1] X. Coiteux-Roy and S. Wolf. Proving erasure. In *IEEE International Symposium on Information Theory (ISIT) 2019*, pages 832–836, 2019.
- [2] A. Broadbent and R. Islam. Quantum encryption with certified deletion. In *Theory of Cryptography Conference (TCC) 2020*, volume 12552 of *LNCS*, pages 92–122, 2020.
- [3] N. Lütkenhaus, A.S. Marwah, and D. Touchette. Erasable bit commitment from temporary quantum trust. *IEEE Journal on Selected Areas in Information Theory*, 1(2):536–554, 2020.
- [4] A. Molina, T. Vidick, and J. Watrous. Optimal counterfeiting attacks and generalizations for Wiesner’s quantum money. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 45–64. Springer, 2012.
- [5] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.
- [6] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference*, pages 386–406. Springer, 2005.
- [7] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.
- [8] S. Fehr and C. Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference*, pages 350–367. Springer, 2009.
- [9] B. van der Vecht, X. Coiteux-Roy, and B. Škorić. Can’t Touch This: unconditional tamper evidence from short keys. *Quantum Information and Computation*, 2022. <https://arxiv.org/abs/2006.02476>.

Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Standardization Process Finalists

Corentin Verhamme
ICTEAM, Crypto Group
UCLouvain
Louvain-la-Neuve, Belgium
corentin.verhamme@student.uclouvain.be

Gaëtan Cassiers
ICTEAM, Crypto Group
UCLouvain
Louvain-la-Neuve, Belgium
gaetan.cassiers@uclouvain.be

François-Xavier Standaert
ICTEAM, Crypto Group
UCLouvain
Louvain-la-Neuve, Belgium
francois-xavier.standaert@uclouvain.be

***Index Terms*—Side-Channel Attack, Masking Countermeasure, Lightweight Cryptography, Leakage resilience**

Security against side-channel attacks has been explicitly mentioned by the NIST as a target in the ongoing standardization process for lightweight cryptography. In this talk, we will analyze the leakage resistance of 9 out of the 10 candidates selected as finalists of the competition.

Our analysis follows two main steps:

First, we use a framework introduced by Bellizia et al. in order to evaluate the high-level leakage properties of the candidates' modes of operations [1].¹ This high-level analysis allows us to observe that 6 candidates can only/mostly rely on (expensive) implementation-level countermeasures. By contrast, 3 candidates (namely Ascon, ISAP and Romulus-T) have leakage-resistant features enabling so-called leveled implementations, where different parts of the implementations require different (more or less expensive) implementation-level countermeasures.

Second, we investigate the hardware performances of these 3 leakage-resistant modes of operation and evaluate their leveled implementation. For Ascon and Romulus-T, we protect the Key Derivation Function (KDF) and Tag Generation Function (TGF) against Differential Power Analysis (DPA) with Hardware Private Circuits (HPC), a state-of-the-art masking scheme that jointly provides resistance against physical defaults and composability [2], [3]. For ISAP, the KDF and KGF are based on a leakage-resilient PRF that embeds a fresh re-keying mechanism such that they only require security against Simple Power Analysis (SPA). The latter is natively (and efficiently) obtained thanks to parallelism in hardware.

Gaëtan Cassiers and François-Xavier Standaert are respectively research fellow and senior research associate of the Belgian fund for scientific research (FNRS- F.R.S.). This work has been funded in parts by European Union via the ERC project 724725 (acronym SWORD).

¹ Excluding Grain-128AEAD, which cannot be captured with such a mode vs. primitive granularity.

For all 3 candidates, the bulk of the computation contains and internal re-keying mechanism. Hence SPA security (again achieved with hardware parallelism) guarantees confidentiality with leakage. This part of the implementation can even leak in an unbounded manner if only integrity with leakage is required.

We conclude that more than the quantitative comparison of the finalists, the main criteria that should guide the NIST in selecting a lightweight cryptography standard (if leakage is deemed important) are qualitative. The limited relevance of quantitative comparisons at this stage of the competition follows from two facts. For ciphers that rely on comparable countermeasures (like Ascon and Romulus-T), the performance gap is limited and predictable from simple proxies (and both are easier to protect than the AES). For ciphers that rely on different countermeasures (like ISAP), we currently lack (both theoretical and practical) tools that would allow a definitive comparison (e.g., with masking). By contrast, these three ciphers have different quantitative features, leading to at least two clear questions that could (and we think, should) guide the final selection:

- *Is confidentiality with decryption leakage wanted?* Ascon, ISAP and Romulus-T all reach the top of the hierarchy in [4] for integrity with leakage (coined CIML2). The leveled implementation of Ascon only provides confidentiality with encryption leakages and misuse-resilience (coined CCAmL1). The leveled implementations of ISAP and Romulus-T can additionally provide confidentiality with decryption leakages and misuse-resilience (coined CCAmL2) at the cost of being two-pass (and can reach CCAmL1 in a single pass).
- *Flexibility or simplicity for the KDF and KGF?* Ascon and Romulus-T require DPA countermeasures like masking to protect their KDF and TGF. Implementing masking securely is a sensitive process that requires expertise. But it comes with a lot of flexibility: countermeasures do not

always have to be deployed, different security vs. performance tradeoffs can be considered and one can have different security levels in encryption and decryption. ISAP relies on a re-keying mechanism so that only SPA security is needed for the whole implementation, which is easy to obtain in hardware. But it has no flexibility (the overheads of the leakage-resilient PRF have to be paid even if side-channel security is not a concern).²

A slightly longer-term question relates to the choice between permutations and Tweakable Block Ciphers (TBCs). While the same leakage-resistant features can be obtained at somewhat similar costs from permutations and sponges, these two building blocks come with some differences. On the one hand, TBC-based designs seem more amenable to security analyzes in the standard model [7], [8], while permutations currently require idealized assumptions [9], [10]. On the other hand, TBC-based schemes enable performing an inverse-based tag verification that can leak in full [11] while permutation-based schemes require masking [12] or additional computations [13] for securing this part of their design against leakage.

REFERENCES

- [1] D. Bellizia, O. Bronchain, G. Cassiers, V. Grosso, C. Guo, C. Momin, O. Pereira, T. Peters, and F. Standaert, “Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle,” in *CRYPTO (1)*, ser. Lecture Notes in Computer Science, vol. 12170. Springer, 2020, pp. 369–400.
- [2] G. Cassiers, B. Grégoire, I. Levi, and F. Standaert, “Hardware private circuits: From trivial composition to full verification,” *IEEE Trans. Computers*, vol. 70, no. 10, pp. 1677–1690, 2021.
- [3] G. Cassiers and F. Standaert, “Provably secure hardware masking in the transition- and glitch-robust probing model: Better safe than sorry,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 2, pp. 136–158, 2021.
- [4] C. Guo, O. Pereira, T. Peters, and F. Standaert, “Authenticated encryption with nonce misuse and physical leakage: Definitions, separation results and first construction - (extended abstract),” in *LATINCRYPT*, ser. Lecture Notes in Computer Science, vol. 11774. Springer, 2019, pp. 150–172.
- [5] O. Bronchain and F. Standaert, “Breaking masked implementations with many shares on 32-bit software platforms or when the security order does not matter,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 3, pp. 202–234, 2021.
- [6] M. J. Kannwischer, P. Pessl, and R. Primas, “Single-trace attacks on keccak,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 3, pp. 243–268, 2020.
- [7] F. Berti, C. Guo, O. Pereira, T. Peters, and F. Standaert, “Tedt, a leakage-resist AEAD mode for high physical security applications,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 1, pp. 256–320, 2020.
- [8] F. Berti, C. Guo, T. Peters, and F. Standaert, “Efficient leakage-resilient macs without idealized assumptions,” in *ASIACRYPT (2)*, ser. Lecture Notes in Computer Science, vol. 13091. Springer, 2021, pp. 95–123.
- [9] C. Dobraunig and B. Mennink, “Leakage resilience of the duplex construction,” in *ASIACRYPT (3)*, ser. Lecture Notes in Computer Science, vol. 11923. Springer, 2019, pp. 225–255.
- [10] C. Guo, O. Pereira, T. Peters, and F. Standaert, “Towards low-energy leakage-resistant authenticated encryption from the duplex sponge construction,” *IACR Trans. Symmetric Cryptol.*, vol. 2020, no. 1, pp. 6–42, 2020.
- [11] F. Berti, O. Pereira, T. Peters, and F. Standaert, “On leakage-resilient authenticated encryption with decryption leakages,” *IACR Trans. Symmetric Cryptol.*, vol. 2017, no. 3, pp. 271–293, 2017.
- [12] O. Bronchain, C. Momin, T. Peters, and F. Standaert, “Improved leakage-resistant authenticated encryption based on hardware AES coprocessors,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 3, pp. 641–676, 2021.
- [13] C. Dobraunig and B. Mennink, “Leakage resilient value comparison with application to message authentication,” in *EUROCRYPT (2)*, ser. Lecture Notes in Computer Science, vol. 12697. Springer, 2021, pp. 377–407.

² Security in low-end embedded software implementations is unclear both for masking and re-keying, which can both be the target of strong attacks in low-noise contexts: see [5] for masking and [1], [6] for re-keying. We believe the understanding of low-noise leakages is not stable enough for being used as a guiding criteria.

Adaptation of Simultaneous Orthogonal Matching Pursuit for Cooperative Spectrum Sensing

Adelin Roty
BEAMS-embedded electronics
Université Libre de Bruxelles
1050 Brussels, Belgium
adelin.roty@ulb.be

Jean-François Determe
BEAMS-embedded electronics
Université Libre de Bruxelles
1050 Brussels, Belgium
jean-francois.determe@ulb.be

Abstract—Efficient spectrum occupancy measurement campaigns mainly rely on wideband spectrum sensing capacities. This paper focuses on the performance of compressive sensing (CS) applied to spectrum sensing. We study a system comprising several sensors endowed with CS-based measurement front-ends installed in the area whose spectrum is to be monitored. Sensors send their measurements to a central node that processes them jointly to estimate global spectrum occupancy. Our main contribution is to study the impact of a newly developed adaptation of Simultaneous Orthogonal Matching Pursuit (SOMP). This adaptation essentially assumes and leverages a common structure shared by all signals seen by sensors, which is stronger than that generally assumed by SOMP. We also study to what extent the spatial distribution of sensors affects the reliability of spectrum recovery. Our results show a significant increase in the probability of correct recovery in comparison to using the basic, canonical SOMP algorithm.

Index Terms—wideband spectrum sensing, sparse signal recovery, simultaneous orthogonal matching pursuit

Adaptive Optimizer Design for Constrained Variational Inference

Alp Sari
TU Eindhoven
Eindhoven, Netherlands
a.sari@student.tue.nl

Semih Akbayrak
TU Eindhoven
Eindhoven, Netherlands
s.akbayrak@tue.nl

İsmail Şenöz
TU Eindhoven
Eindhoven, Netherlands
i.senoz@tue.nl

Bert de Vries
TU Eindhoven
Eindhoven, Netherlands
bert.de.vries@tue.nl

Abstract—This paper addresses the problem of implementing robust and hyperparameter-free natural gradient variational inference. Natural gradient methods are often employed in variational inference strategies, which maximize a variational lower bound on the model evidence. Generally, gradient-based optimization algorithms require the user to pre-specify values for hyperparameters such as step size and number of iterations. Optimal values for these hyperparameters are problem-specific and may significantly affect the algorithm’s performance. We propose a model-aware optimizer that adaptively adjusts its step size parameter. The proposed optimizer determines the necessary number of iterations and evaluates the accuracy of the variational approximation, compared to the actual posterior distribution, using convergence diagnostics. We verify in this paper that the proposed adaptive optimizer alleviates the fine tuning problem with no manually initialized step size and a number of iterations. The performance of the optimization results is reported using the convergence diagnostics implemented within the proposed optimizer.

Index Terms—Bayesian Diagnostics, Constrained Bayesian Inference, Exponential-family Distributions, Hyper-parameter Free Optimization, Natural Gradient Variational Inference, Stochastic Gradients

I. INTRODUCTION

WE address the problem of implementing robust and hyper-parameter free natural gradient variational inference. When exact Bayesian inference to find a posterior distribution of a parameter is not tractable, an approximate distribution for the posterior estimate is searched. Finding this approximate posterior using optimization and through variational calculus is known as variational inference [1]. Conjugate-computation variational inference (CVI) is a variational inference algorithm that uses stochastic gradients on the non-conjugate term whereas using efficient conjugate computations on the conjugate term [2]. CVI is highly dependent on the choice of hyper parameters, such as the step size and the number of iterations. The optimal choice of these hyper-parameters differs for each problem, so it requires fine tuning, which is time consuming. This paper focuses on developing an automatized optimizer by making modifications to the CVI algorithm with already existing methods on the variational inference literature and adding more heuristics to the approaches when necessary. In this paper we will show:

- Limitations of vanilla implementations of the CVI algorithm in Sec. II-C and how to address them in Sec. III.

- Methods to automate the inference process by automatically determining proper step size and number of iterations to prevent manual fine tuning in Sec. III-B and Sec. III-C, respectively.
- How to evaluate the accuracy of our variational approximation in Sec. III-D.

II. CONJUGATE COMPUTATION VARIATIONAL INFERENCE

A. Variational Objective

In Bayesian inference, a model is specified as joint distribution:

$$p(y, z) = p(y|z)p(z) \quad (1)$$

where y stands for observations and z stands for latent variables of the model. Having observed y , we can use the Bayes rule to calculate the posterior distribution of latent variables z as:

$$p(z|y) = \frac{p(y|z)p(z)}{\int p(y|z)p(z) dz} \quad (2)$$

The problem is, the marginal likelihood term ($\int p(y|z)p(z) dz$) might be intractable. This usually happens when the prior term is not a *conjugate prior* to the likelihood.. $p(z)$ is called a *conjugate prior* for the likelihood $p(y|z)$ if the posterior $p(z|y)$ is in the same probability distribution family as the prior distribution $p(z)$ [3, Ch. 2].

A workaround would be to introduce another distribution $q(z)$ that will approximate the exact posterior $p(z|y)$ [1]. Then the marginal likelihood term can be rewritten as:

$$p(y) = \int p(y|z)p(z) dz = \int \frac{p(y|z)p(z)}{q(z)} q(z) dz \quad (3)$$

Using Jensen’s inequality [4], we obtain a lower bound on the log-likelihood function, also known as the evidence lower bound ELBO, given by the expression:

$$\mathcal{L}[q] \triangleq \int \log \left(\frac{p(y, z)}{q(z)} \right) q(z) dz = \mathbb{E}_q \left[\log \left(\frac{p(y, z)}{q(z)} \right) \right]. \quad (4)$$

Our objective is to maximize $\mathcal{L}[q]$ with respect to our approximate variational distribution $q(z)$.

Note that ELBO $\mathcal{L}[q]$ is a *functional*, a function of functions, in this setting, without further assumptions on $q(z)$. In variational inference, we further assume a fixed-form variational approximation $q_\lambda(z)$, parametrized by λ . Then, functional

maximization problem reduces to maximization of a function $\mathcal{L}(\lambda)$ with respect to its parameters. Thus, we are trying to find optimal values for the parameters λ by the following optimization problem:

$$\begin{aligned} \max_{\lambda \in \Omega} \mathcal{L}(\lambda) &= \mathbb{E}_q \left[\log \left(\frac{p(y|z)p(z)}{q_\lambda(z)} \right) \right] \\ &= \mathbb{E}_q \left[\log(p(y|z)) - \log \left(\frac{q_\lambda(z)}{p(z)} \right) \right] \end{aligned} \quad (5)$$

where Ω is the space of valid parameters [1].

B. CVI Algorithm

CVI method utilizes conjugate computations on the conjugate part of the model, whereas it computes the natural gradients on the non-conjugate part of the model [2]. For CVI, the variational approximation is chosen to be in the minimal exponential family of distributions. A distribution $q_\lambda(z)$ in the exponential family with natural parameters λ has the probability density function of the following form:

$$q_\lambda(z) = h(z) \exp(\phi(z)^T \lambda - A(\lambda)) \quad (6)$$

where $h(z)$ is the base measure, $\phi(z)$ is the sufficient statistics vector and the $A(\lambda)$ is the log-partition function. An exponential family representation is called minimal if the components of the sufficient statistics vector are linearly independent [5, Ch. 3]. We would assume that our prior distribution $p_{\lambda_p}(z)$ is in the same minimal exponential family as the variational approximation, with natural parameters λ_p . Thus, the conjugate part is the prior term $p_{\lambda_p}(z)$, and the non-conjugate term is the log-likelihood term $p(y|z)$. CVI algorithm updates the parameters using a natural gradient descent approach:

$$\lambda \leftarrow \lambda + \beta \hat{g} \quad (7)$$

The natural gradient of the ELBO $\hat{g} \triangleq \nabla_m \mathcal{L}$ is the Euclidean gradient with respect to the expectation parameters $m \triangleq \mathbb{E}_q[\phi(z)]$ and can also be computed as $m = \nabla_\lambda A(\lambda)$ for minimal exponential family distributions. Calculating natural gradients also give rise to local exponential-family approximations of the non-conjugate terms. Then, combining (5) and (7), the natural gradient update for the CVI algorithm becomes:

$$\lambda \leftarrow \lambda + \beta [\nabla_m \mathbb{E}_q[\log(p(y|z))] + \lambda_p - \lambda] \quad (8)$$

using the property that:

$$\nabla_m \left(\mathbb{E}_q \left[\log \left(\frac{p_{\lambda_p}(z)}{q_\lambda(z)} \right) \right] \right) = \lambda_p - \lambda. \quad (9)$$

For more details about the derivation of (8), we refer the interested reader to [2].

C. Considerations Using CVI

In CVI, the parameters of $q_\lambda(z)$ are updated using natural gradients to optimize ELBO. Using such an approach comes with practical considerations, such as:

- The update scheme does not take into account the constraints of the parameters by default. For example, the precision parameter of a Gaussian distribution must be

positive-definite. Since there are no constraints on the values of step size or the natural gradient vector can take, this constraint may be violated in (8). The constraints are addressed in Sec. III-A.

- Convergence of gradient-based methods are dependent on the hyper-parameters, which are step size and the number of iterations, and the optimal choice of these parameters differ for different model specifications. CVI algorithm does not offer any specification for these parameters. Finding appropriate parameters for the step size and the number of iterations are addressed in Sec. III-B and Sec. III-C, respectively.
- After a given number of iterations, CVI algorithm does not give information about the convergence of the parameters. A metric to evaluate the posterior approximation is given in Sec. III-D.

III. ADAPTIVE OPTIMIZER DESIGN FOR CONSTRAINED CVI

Our proposed optimizer addresses the problems mentioned in Sec. II-C. We propose a modification to the CVI update using existing methods in the variational inference literature and adding more heuristics to the approaches when necessary. The proposed optimizer is capable of initializing and updating the hyper-parameters of the inference process, adapting to the given model.

A. Handling Positive Definite Constraints of the Parameters

A modified version of the CVI update (8) is proposed in [6], which is called the improved Bayesian Learning Rule (iBLR). This update scheme handles the positive-definite constraints of the valid parameter space when the approximation $q_\lambda(z)$ attains a certain parameterization, which the authors call *block-coordinate natural parameterization* (BCN). This modification allows us to freely choose the step size parameter β_t . For the sake of completeness, we briefly summarize iBLR approach below.

Let BCN parameters are denoted with λ and λ contains blocks of parameters as $\lambda = \{\lambda^{[1]}, \dots, \lambda^{[n]}\}$. Let λ^{a_i} denote the parameter at a -th entry of the i -th block parameter $\lambda^{[i]}$, \hat{g}^{c_i} denote the c -th entry of natural gradient \hat{g}^i with respect to $\lambda^{[i]}$. Then, modified gradient ascent update takes the form:

$$\lambda^{c_i} \leftarrow \lambda^{c_i} + \beta_t \hat{g}^{c_i} - \frac{\beta_t^2}{2} \sum_{a_i} \sum_{b_i} \Gamma_{a_i b_i}^{c_i} \hat{g}^{a_i} \hat{g}^{b_i} \quad (10)$$

where each summation is to sum over all entries of the i -th block, $\Gamma_{a_i b_i}^{c_i} := \frac{1}{2} \partial_{m_{c_i}} \partial_{\lambda^{a_i}} \partial_{\lambda^{b_i}} A(\lambda)$ and m_{c_i} is the c -th entry of the expectation parameter $m_{[i]} := \nabla_{\lambda^{[i]}} A(\lambda)$.

Note that (10) only differs from CVI update by the last term $-\frac{\beta_t^2}{2} \sum_{a_i} \sum_{b_i} \Gamma_{a_i b_i}^{c_i} \hat{g}^{a_i} \hat{g}^{b_i}$, which is to take the curvature information in a Riemannian manifold into account. For some of the BCN parameterizations, such as for the Gaussian distribution, (10) can be efficiently applied. For the list of BCN parameterizations in the exponential family of distributions, their simplified update rules and the detailed derivation of their update rules, see [6].

B. Determining Step Size

In this section, a fast heuristic approach and an adaptive method are presented to find an appropriate step size parameter β_t .

1) *Inexact Line Search to Determine Step Size*: To determine the step size, our optimizer uses an inexact line search method, which is a heuristic approach. Note that inexact line search inequality conditions used in Euclidean spaces cannot be utilized directly since our parameter space induces a Riemannian manifold. An adaptation of line search methods to manifolds can be utilized, but the study of it is left for future work.

Our heuristic approach searches for an appropriate step size only for the first iteration to be computationally efficient. Found step size is kept fixed throughout the optimization.

2) *Adaptive Step Size*: Adaptive step size approach is based on [7], which is developed for stochastic variational inference. Stochastic variational inference is used to scale variational inference to models with large data sets by instead of computing a batch gradient, a sample data from the data set is used to calculate the gradient for its computational efficiency. The proposed method determines the step size β_t such that it minimizes the expected distance between updated parameters λ_{t+1} , where the update from λ_t to λ_{t+1} is the CVI update given in (7), and the updated parameters using the whole batch λ_* , by minimizing the expectation of the following cost function:

$$J(\beta_t) = (\lambda_{t+1}(\beta_t) - \lambda_*)^T (\lambda_{t+1}(\beta_t) - \lambda_*) \quad (11)$$

The cost function J is a function of step size β_t through λ_{t+1} term and is a random variable since update from λ_t to λ_{t+1} includes the natural gradient term \hat{g}_t in (7). Thus, the minimization is done for its expectation value $\mathbb{E}[J|\lambda_t]$, given the current iterate λ_t . Minimizing the expectation yields the optimal step size as:

$$\beta_t^* = \frac{\mathbb{E}[\hat{g}_t]^T \mathbb{E}[\hat{g}_t]}{\mathbb{E}[\hat{g}_t^T \hat{g}_t]} \quad (12)$$

and the expectations can be calculated using moving average windows and they can be plugged in (12), to calculate β_t at each time step t . For the detailed derivation of the result, see [7].

C. Determining the Number of Iterations

Convergence of CVI optimization scheme is highly dependent on the number of iterations. Doing too many iterations might result in unnecessary increase in the computation time, whereas small number of iterations might result in premature termination of the optimization process before convergence. Unfortunately, there does not exist a specified number of iterations, which is optimal for any optimization problem. But, if the convergence of the parameters can be checked using some diagnostics, we can come up with a stopping criteria which will be used to terminate the optimization process. In our proposed optimizer, a method based on tracking the

relative change of the variational objective $\mathcal{L}(\lambda)$, to determine the stopping criterion is implemented.

This stopping criteria is similar to the Automatic Variational Inference in Stan algorithm [8]. For a (optional) specified number $k \in \mathbb{Z}^+$, the variational objective and the relative change of variational objective is calculated. If one iteration index at which the calculation occurred is T , then the relative change for that step is calculated as:

$$\Delta\mathcal{L}_T = 100 \cdot \left| \frac{\mathcal{L}(\lambda_T) - \mathcal{L}(\lambda_{T-k})}{\mathcal{L}(\lambda_{T-k})} \right| \quad (13)$$

$$\mathcal{L}_T = \mathbb{E}_q \left[\log(p(y|z)) - \log\left(\frac{q_{\lambda_T}(z)}{p(z)}\right) \right], \quad (14)$$

and stored in a vector $\Delta\mathcal{L}_{vect} = [\dots, \Delta\mathcal{L}_{T-k}, \Delta\mathcal{L}_T]$. Then, the running mean and median of this vector is calculated and compared to a threshold and the algorithm is terminated when either of the criteria are satisfied.

Downside of this algorithm is that it can prematurely end the optimization algorithm. This is shown with a simulated example displayed in Fig. 1. The variational objective is Free Energy, which is calculated as the negative of ELBO. As we are using the relative change in the free energy, this algorithm will be referred as ΔFE . Since there are no guarantees to reduce the free energy in each step with a given step size, simulated scenario involves an increase in the free energy at first then it converges to a lower value after considerable amount of iterations. The convergence algorithm ΔFE calculates the relative change in the free energy and compares the running mean and median to the threshold, which is set as 3%. Then, the algorithm would terminate prematurely, where the termination point is shown with red dashed line in Fig. 1.

To solve this problem, we have defined a burn-in period where the algorithm would not look for convergence until a specified number of iterations are carried out or the initial free energy decreases until a certain amount. With the latter condition, the algorithm will not search for convergence before the free energy decreases compared to the initial value, thus skipping the points where the vanilla implementation would prematurely terminate the optimization process.

D. Evaluating Variational Inference Using Generalized Pareto Distribution

A diagnostic which can be used to assess the goodness of the fit of variational distribution $q_\lambda(z)$ is fitting a generalized pareto distribution to the largest importance ratios and looking at the shape parameter k of the fitted distribution [9]. The motivation to use such a diagnostic comes from importance sampling literature [10, Ch. 9].

We treat our variational approximation $q_\lambda(z)$ as if it were a proposal distribution in importance sampling. When the proposal distribution $q_\lambda(z)$ is a poor approximation to the target distribution $p(z|y)$, the distribution of importance ratios can have a heavy right tail [11]. Thus, checking if distribution of importance ratios having a heavy tailed would indicate the accuracy of our variational approximation.

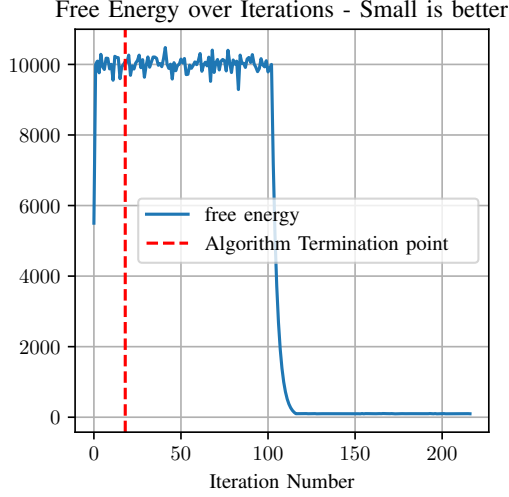


Fig. 1: A simulated example where ΔFE algorithm would result in premature termination. The threshold is set as 3% and the dashed line shows the termination point. Premature termination prevents the algorithm to converge to a lower free energy than the initial free energy.

A distribution used to model tails of another distribution is generalized Pareto distribution. A generalized Pareto distribution with a shape parameter k has finite moments up to the order $1/k$. If the fitted importance ratios have more than 2 finite moments, the convergence rate of the estimator improves [11], then if we have $k < 0.5$, it can be concluded that the variational distribution is close enough to the true posterior. Empirical studies show the number of samples you would need to have reliable estimators increases drastically after $k > 0.7$ [11]. Thus, for the fitted values of $0.5 < k < 0.7$, the variational distribution can still be practically useful.

This diagnostic is used as follows in our optimizer: After updating $q_\lambda(z)$ after a certain number of iterations, which can be fixed or determined by a stopping criterion, S samples from variational distribution are obtained and importance ratios are calculated as:

$$r_s(z) = \frac{p(y|z_s)p(z_s)}{q_\lambda(z_s)} \quad (15)$$

where $z_s \sim q_\lambda(z_s), i = 1, \dots, S$. Then, a generalized Pareto distribution is fitted to M largest importance ratios, where M is a function of S and fitted shape parameter k is reported. If $k > 0.7$, the user is warned that the variational inference may not have converged. For the negative values of k , it is predicted that the importance ratios are bounded from above. For detailed explanation of how to fit the generalized Pareto distribution, we refer the interested reader to [12], and for more details about the convergence properties of the generalized Pareto distribution, we refer the interested reader to [11] and [9].

E. Overall Algorithm

We have addressed the practical considerations of the vanilla implementation of the CVI algorithm mentioned in Sec. II-C, with the methods given in Sec. III. Using these methods, we propose our adaptive optimizer in Algorithm 1 which finds the appropriate step size using an adaptive step size algorithm and tracks the relative change of the variational objective to terminate the algorithm. Finally, the accuracy of the approximation is diagnosed by fitting a generalized Pareto distribution to the largest importance ratios.

Algorithm 1 Adaptive Optimizer for Constrained CVI using Relative Change of Variational Objective

Define: Number of iterations of burn-in period: τ

Define: Mean threshold ϵ_1

Define: Median threshold ϵ_2

Define: Window size to evaluate the variational objective W

Require: $\tau, \epsilon_1, \epsilon_2, W$

$check = false$

$\Delta \mathcal{L}_{vect} = []$

for $t=1, \dots, T_{max}$ **do**

if $t = 1$ **then**

 Compute $F_{thr} = \mathcal{L}(\lambda_0)$

end if

 Compute $\hat{g} = \nabla_m \mathcal{L}$

 Compute β via (12)

 Compute λ_t via (10)

$\lambda \leftarrow \lambda_t$

if $t \leq \tau$ **then**

$continue$

 ▷ First additional heuristic

else if $t \bmod W = 0$ **then**

 Compute $\mathcal{L}(\lambda_t)$

if $check = false$ and $\mathcal{L}(\lambda_t) \geq F_{thr}$ **then**

$check = true$ ▷ Second additional heuristic

end if

if $check = true$ **then**

 Compute $\Delta \mathcal{L}_t$ via Eq 13

 Append $\Delta \mathcal{L}_{vect} = [\Delta \mathcal{L}_{vect}, \Delta \mathcal{L}_t]$

 Compute mean m_1 and median m_2 of $\Delta \mathcal{L}_{vect}$

end if

if $m_1 \leq \epsilon_1$ or $m_2 \leq \epsilon_2$ **then**

$break$

end if

end if

end for

Sample $z_s, s = 1, \dots, S$ from $q_\lambda(z)$

Compute importance ratios $r_s, s = 1, \dots, S$ via Eq 15

Fit generalized Pareto distribution to M largest importance ratios and return shape parameter estimate \hat{k}

if $\hat{k} > 0.7$ **then**

 Warn user that variational inference may not have converged.

end if

return λ

IV. EXPERIMENTS

In this section, the experiment results on simulated examples which investigate how the choice of step size and the number of iterations affect the convergence of the variational distribution are shown. Motivation of using simulated examples is to observe the behavior of the current algorithms with arbitrary nonlinearities/functions to test their robustness.

A. First Experiment: Nonlinear Measurement Model

In the first experiment, the effect of the step size parameter and the number of iterations is studied. The prior distribution of the latent variable z is the Gaussian distribution. Observations y are also Gaussian distributed with known precision γ and the mean parameter is a non-linear function $g(\cdot)$ of latent variables z . The model is given as:

$$p(y | z) = \mathcal{N}(y | g(z), \gamma^{-1}) \quad (16a)$$

$$p(z) = \mathcal{N}(z | \mu_p, S_p^{-1}) \quad (16b)$$

The Gaussian prior and the measurement precision are set as:

$$\mu_p = 0, S_p^{-1} = 0.01, \gamma^{-1} = 0.01,$$

respectively.

The nonlinear expression $g(\cdot)$ is given as:

$$g(z) = -z^3 \cdot \exp(-0.005 \cdot |z|) \quad (17)$$

A measurement $\hat{y} = g(120) + \epsilon, \epsilon \sim \mathcal{N}(0, 1)$ is observed and a variational approximation $q_\lambda(z)$, which is a Gaussian distribution, of the true posterior $p(z|\hat{y})$ is calculated. The selected variational objective to find $q_\lambda(z)$ is the free energy, defined as the negative of the ELBO. Non-linearity $g(z)$ is selected such that $g(120)$ evaluates to a large number, which also tests numerical stability of the algorithms. For the given nonlinearity $g(\cdot)$, the likelihood $p(\hat{y}|z)$ has two local optima, around $z \approx 120$ and $z \approx 1716$. Having a weak prior $p(z)$, the local variational approximation should converge to a Gaussian distribution with mean around either of the local optima. The posterior with mean value of 120 is the global optimum, since it is closer to the prior, which has lower free energy than the posterior with mean value of 1716, but the noisy estimate of the expectation of the log-likelihood term makes it impossible to distinguish the global optimum.

The parameters of variational approximation $q_\lambda(z)$ are optimized using both the CVI update rule with gradient descent and Adam optimizers and the iBLR update rule. All optimization schemes are tested with various number of iterations and step size hyper-parameters. Step size parameters are set as $ss_i = 10^{-i}, i = 0, 1, \dots, 10$, number of iterations are set as $itr_j = 10^j, j = 1, 2, \dots, 6$ to cover a variety of hyperparameter combinations. Then, for each point (ss_i, itr_j) in the hyper-parameter space for all three update rules, we perform the experiment with the same hyper-parameter configuration 10 times, and report the median value of 10 experiments.

Fig. 2 and Fig. 3 show the estimated posterior mean parameter of the variational distribution $q_\lambda(z)$ using the iBLR algorithm and the CVI algorithm with Descent optimizer,

respectively. Only the results that are in the vicinity of the true posterior mean are shown in the figures, as failed cases have arbitrarily large values and cannot be plotted on the same graph. The results using CVI algorithm with Adam optimizer are not shown since none of the 66 different configurations of hyper-parameters yield a close approximation to the true posterior mean.

As seen in Fig. 2 and Fig. 3, both iBLR and CVI algorithm with Descent converge only for the cases where the step size parameter is less than a certain threshold, which is 10^{-6} for the iBLR case and 10^{-7} for the CVI case. Moreover, if the user selects smaller step sizes, then the optimal number of iterations varies.

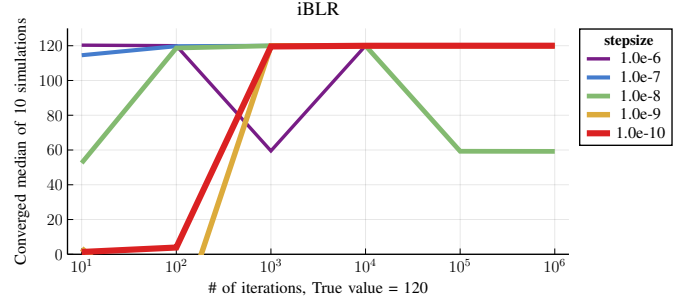


Fig. 2: Hyper-parameter sweep results using iBLR algorithm. It is observed that using stepsizes larger than 10^{-6} yield in algorithm to fail, whereas a certain number of iterations are necessary if one uses very small step sizes, such as 10^{-10} .

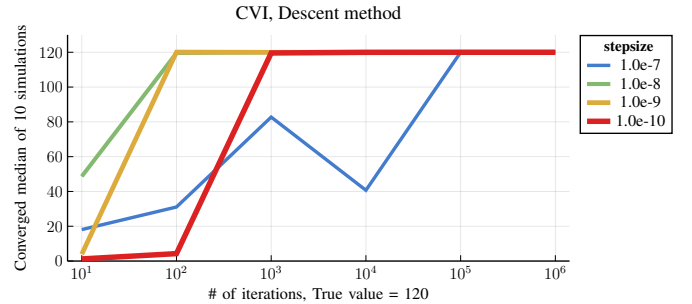


Fig. 3: Hyper-parameter sweep results using CVI algorithm with Descent optimizer. It is observed that using step sizes larger than 10^{-7} yield in algorithm to fail, whereas a certain number of iterations are necessary if one uses very small step sizes, such as 10^{-10} .

Fig. 4 shows the comparison of 3 optimization schemes with a fixed step size of 10^{-7} . It is observed that ADAM needs too many samples for this problem to converge, which is more than a million samples, whereas you would need much less samples for the iBLR case and at least 100000 samples for the CVI case to converge.

Fig. 2, Fig. 3 and Fig. 4 show how hyper-parameters affect the inference performance. The optimal parameters varies with every design choice, and finding suitable parameters requires

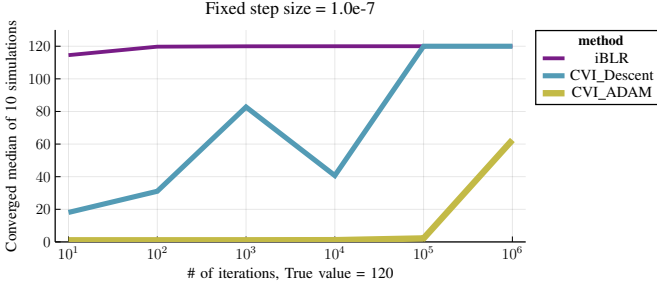


Fig. 4: Comparison of three optimization schemes. It is observed that the optimal number of iterations also changes greatly depending on the optimization algorithm chosen.

tedious work. Our proposed optimization scheme relieves the user of choosing step sizes and the number of iterations. We used our proposed optimizer given in Algorithm 1 for the given problem without any specifications on the initial step size or how many iterations to perform. The step size is selected to be determined by the heuristic based on the inexact line search method in Sec III-B1 to see if the optimizer can propose an appropriate step size for the problem. Initial step size is determined as $7.62 \cdot 10^{-6}$, which is an appropriate step size according to the results of Fig 2, and the algorithm terminated itself after 90000 iterations, converging to the value 120, which is the mean parameter value minimizing the current variational objective.

B. Second Experiment: Variational Message Passing

In the second example, variational message passing(VMP) example introduced in [13] is studied. The model in [13] can be formed using the same factorization in Eq. 16 with two differences. First, the non-linear function $g(\cdot)$ is changed to identity mapping, i.e., $g(z) = z$ and we put a Gamma prior on the measurement precision γ with the shape parameter a and the rate parameter β . VMP example in [13] approximates the posterior $p(x, \gamma | y)$ with a variational approximation $q(x, \gamma)$. If we also assume mean-field factorization $q(x, \gamma) = q_x(x)q_\gamma(\gamma)$, the model is conditionally conjugate and VMP algorithm updates the posterior parameters analytically. 5 observations are generated as:

$$y_n = 15 + \epsilon, \epsilon \sim \mathcal{N}(0, 1), n = 1, \dots, 5 \quad (18)$$

Using VMP on the given problem setting resulted in the posterior mean of z as $\mu_z = 14.938$. We will take this result as the ground truth and test our gradient-based algorithm's performance.

In the first experiment in Sec. IV-A, we have used our heuristic line-search-based approach to find an appropriate step size. In this example, we let our optimizer decide the step size using adaptive step size algorithm mentioned in Section III-B2.

500 Monte Carlo simulations were performed and we calculated the mean and variance of the estimate as $\hat{\mu}_z = 14.90$ and $\sigma_{\hat{\mu}_z}^2 = 0.40$, respectively. As expected, the mean is in the vicinity of the ground truth with a small variance value.

We also ran the algorithm using a fixed step size of 0.5 and 10^{-6} and we observe that even though we only needed 20 iterations using a step size of 0.5, we needed at least 10^6 iterations for the step size of 10^{-6} . Even if the VMP model is simple, it still shows how important the hyper-parameters are for performance of the algorithm.

V. CONCLUSION

We illustrated the practical considerations of implementing a natural gradient based variational inference optimization and what can be done in order to automatize the hyper-parameter tuning process, with their limitations. We proposed an automated optimizer for conjugate computation variational inference, which determines the initial step size, adaptation of step size over the iterations and when to terminate the inference procedure, along with diagnosing the accuracy of the posterior approximation to the true posterior. Its working principle can be improved by careful design of heuristics and implementing more robust solutions from the literature. This paper paves the way for a novel approach of gradient based variational inference algorithms which has its own robust convergence diagnostics and adaptive to the different types of non-conjugate terms in the generative model.

REFERENCES

- [1] D. M. Blei, A. Kucukelbir, and J. D. McAuliffe, "Variational Inference: A Review for Statisticians," *Journal of the American Statistical Association*, vol. 112, pp. 859–877, Apr. 2017. arXiv: 1601.00670.
- [2] M. E. Khan and W. Lin, "Conjugate-Computation Variational Inference : Converting Variational Inference in Non-Conjugate Models to Inferences in Conjugate Models," arXiv:1703.04265 [cs], Mar. 2017.
- [3] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer-Verlag New York, Inc., 2006.
- [4] M. Jordan, Z. Ghahramani, T. Jaakkola, and L. Saul, "An Introduction to Variational Methods for Graphical Models," *Machine Learning*, vol. 37, pp. 183–233, Jan. 1999.
- [5] M. Wainwright and M. Jordan, "Graphical Models, Exponential Families, and Variational Inference," *Foundations and Trends in Machine Learning*, vol. 1, pp. 1–305, Jan. 2008.
- [6] W. Lin, M. Schmidt, and M. E. Khan, "Handling the Positive-Definite Constraint in the Bayesian Learning Rule," arXiv:2002.10060 [cs, stat], Oct. 2020.
- [7] R. Ranganath, C. Wang, B. David, and E. Xing, "An Adaptive Learning Rate for Stochastic Variational Inference," in *Proceedings of the 30th International Conference on Machine Learning*, pp. 298–306, PMLR, May 2013. ISSN: 1938-7228.
- [8] A. Kucukelbir, R. Ranganath, A. Gelman, and D. M. Blei, "Automatic Variational Inference in Stan," arXiv:1506.03431 [stat], June 2015.
- [9] Y. Yao, A. Vehtari, D. Simpson, and A. Gelman, "Yes, but Did It Work?: Evaluating Variational Inference," arXiv:1802.02538 [stat], July 2018.
- [10] O. Art B., *Monte Carlo theory, methods and examples*. 2013.
- [11] A. Vehtari, D. Simpson, A. Gelman, Y. Yao, and J. Gabry, "Pareto Smoothed Importance Sampling," arXiv:1507.02646 [stat], Feb. 2021.
- [12] J. Zhang and M. A. Stephens, "A New and Efficient Estimation Method for the Generalized Pareto Distribution," *Technometrics*, vol. 51, no. 3, pp. 316–325, 2009. Publisher: [Taylor & Francis, Ltd., American Statistical Association, American Society for Quality].
- [13] J. Winn and C. M. Bishop, "Variational Message Passing," *Journal of Machine Learning Research*, vol. 6, no. 23, pp. 661–694, 2005.

Collusion-resistant fingerprinting of parallel content channels

Basheer Joudeh

Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, the Netherlands
b.joudeh@tue.nl

Boris Škorić

Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, the Netherlands
b.skoric@tue.nl

Abstract—The fingerprinting game is analysed when the coalition size k is known to the tracer, but the colluders can distribute themselves across L TV channels. The collusion channel is introduced and the extra degrees of freedom for the coalition are made manifest in our formulation. We introduce a payoff functional that is analogous to the single TV channel case, and is conjectured to be closely related to the fingerprinting capacity. For the binary alphabet case under the marking assumption, and the restriction of access to one TV channel per person per segment, we derive the asymptotic behavior of the payoff functional. We find that the value of the maximin game for our payoff is asymptotically equal to $L^2/k^2 2 \ln 2$, with optimal strategy for the tracer being the arcsine distribution, and for the coalition being the interleaving attack across all TV channels, as well as assigning an equal number of colluders across the L TV channels.

Index Terms—information hiding, information theory, security

I. INTRODUCTION

A. Collusion resistant fingerprinting

Fingerprinting, also known as forensic watermarking, is a technique for tracing the origin and distribution of digital content. Before distribution, the content is modified by embedding an imperceptible watermark, which is unique for each recipient. When an unauthorized copy of the content is released, the watermark in this copy reveals information about the identities of those who created the copy. A tracing algorithm (also called a decoder) outputs a list of suspicious users. This procedure is known as forensic watermarking or traitor tracing.

The most powerful attack against watermarking is the *collusion attack*, where multiple users (the ‘coalition’) combine their differently watermarked versions of the same content; the detected differences partly reveal the locations of the hidden marks and allow for an informed attack. Various collusion-resistant codes have been developed, most notably the class of *bias-based* codes, introduced by G. Tardos in 2003 [1], [2]. For each watermarking symbol position the tracer first generates a bias $w \in (0, 1)$ drawn from a distribution f_W and then assigns to each user a watermark symbol ‘1’ with probability w and ‘0’ with probability $1 - w$. Work on bias-based codes

includes improved analyses [3]–[9], code modifications [10]–[12], advanced decoders [13]–[19] and generalizations [20]–[23]. Bias-based codes achieve the asymptotically optimal relationship $n \propto k^2$, where n is the sufficient code length, and k is the coalition size.

An important result was finding the asymptotic *saddlepoint* of the information-theoretic maximin game [10], [24], [25] in the case of the Restricted Digit Model¹ and joint decoding.

The saddlepoint is a pair (bias distribution f_W , attack strategy) such that it is disadvantageous for either party to depart from their strategy. With increasing k , the solution of the max-min game for the binary fingerprinting alphabet gets closer to the combination² ($f_W = \frac{1}{\pi \sqrt{w(1-w)}}$, attack = Interleaving). In the Interleaving attack the colluders output the symbol of one colluder chosen uniformly at random.

Knowing the location of the saddlepoint allows the tracer to build a *universal* decoder that works optimally against the saddlepoint attack and that works well against all other attacks too. What is usually not considered in studies of forensic watermarking is that most pirate decoder boxes observed in practice give access to multiple TV channels in parallel. Hence, attackers have an additional degree of freedom that has not yet been explored in the academic literature: which TV channel to collude on at which point in time. The information-theoretic maximin game has not yet been studied for multiple TV channels attacks.

B. Contributions and outline

We study the information-theoretic maximin game for the binary fingerprinting scenario with multiple parallel TV channels which are being attacked simultaneously by a set of colluders under the Restricted Digit Model. We consider the *static* case, as opposed to *dynamic* traitor tracing, i.e. we do not allow the parties to adapt their strategy as a function of symbols observed previously. We assume that each attacker can tune into merely one channel, and furthermore we consider only attack strategies in which the colluders take equal risk, and all TV channels are treated as being equally important.

¹In the Restricted Digit Model, colluders must output a symbol that has been received by at least one of them.

²This f_W is known as the arcsine distribution, $f_W(w)dw = \frac{1}{\pi} d \arcsin(2w - 1)$.

This work has been accepted for publication by the 10th ACM Workshop on Information Hiding and Multimedia Security IH&MMSEC’22.

Under these restrictions we study the mutual information $I(\hat{Y}; \hat{Z}, \hat{C} | \hat{W})$, which is a straightforward generalisation of the single-channel figure of merit $I(Y; M | W)$. Here the hat indicates a vector in which each entry comes from one TV channel; the Y is the colluders' output, the M stands for the coalition's symbol tally in the single TV channel case, while (\hat{Z}, \hat{C}) represent the coalition's symbol tally in the multiple TV channel case, and W is the bias. Although the generalised figure of merit looks simple, the multiple TV channel maximin game is more complicated than the single TV channel case. If a pirate is active in one TV channel, then this excludes the possibility that they are active in another TV channel. This exclusion causes a nontrivial dependence between the TV channels, which complicates the analysis: it is not a priori clear if the multi-channel attack can be treated as a set of independent single-channel attacks.

- We find the solution of the maximin game for the $k \rightarrow \infty$ limit of the payoff function $I(\hat{Y}; \hat{Z}, \hat{C} | \hat{W})$, using the same technique as Huang and Moulin [25]. The optimal bias distribution for the tracer is the arcsine distribution, and the optimal colluder strategy within each channel is Interleaving. Moreover, it is optimal for the attackers to spread evenly over the channels. Although the result is far from surprising, the proof is less simple than one would have hoped for. The proof needs some careful handling of expressions with different orders in $1/k$ that arise from different attack strategies for spreading out over the channels.
- We present an alternative payoff functional, namely the mutual information $I(\hat{Y}; \hat{X}_{\mathcal{K}} | \hat{W})$. Here $\hat{X}_{\mathcal{K}}$ stands for the part of the code matrices in all the TV channels that can potentially be tuned into by the coalition \mathcal{K} . We argue that the two payoffs have the same maximin game asymptotically, and this leads us to conjecture that the optimal strategies old for $I(\hat{Y}; \hat{X}_{\mathcal{K}} | \hat{W})$ as well, and that the fingerprinting capacity asymptotically behaves like $L^2/(k^2 2 \ln 2)$.

In Section II we introduce the multiple TV channels model and the payoff function. In Section III we derive the maximin solution for the asymptotic payoff. We discuss the alternative payoff and fingerprinting capacity in Section IV. We summarize and suggest future work in Section V. Before we proceed, we introduce common notations used throughout the manuscript.

C. Notation

Let m be the number of users; $\mathcal{M} \triangleq \{1, 2, \dots, m\}$ the index set for all users; $\mathcal{X} \triangleq \{0, 1, \dots, q-1\}$ denote the q -ary fingerprinting alphabet; n denote the code length; $\mathcal{K} \triangleq \{j_1, \dots, j_K\} \subset \mathcal{M}$ the index set of the coalition, where K is the number of colluders; k is the nominal coalition size³; L the number of TV channels; $\mathcal{L} \triangleq \{1, 2, \dots, L\}$ the index set for all TV channels; \tilde{L} the number of TV channels a user can

tune in to simultaneously; $(\cdot)_{\mathcal{K}} \triangleq \{(\cdot)_j : j \in \mathcal{K}\}$; vectors are denoted by boldface letters; L -tuples are denoted by $(\hat{\cdot}) \triangleq ((\cdot)^1, \dots, (\cdot)^L)$; $|\cdot|$ denotes the L^1 -norm of a vector or the cardinality of a set, depending on the argument. We denote the Kronecker delta by $\delta(i, j)$, which is equal to 1 when $i = j$, and 0 otherwise. We use the following notation for asymptotic relations: Let $f(k)$ and $g(k)$ be two functions defined on the real numbers. $f(k) = O(g(k))$ if $\exists c > 0, k^* > 0$ such that $f(k) \leq cg(k), \forall k \geq k^*$. $f(k) = o(g(k))$ if $f(k)/g(k)$ tends to 0. $f(k) = w(g(k))$ if $f(k)/g(k)$ tends to ∞ . $f(k) \sim g(k)$ if $f(k)/g(k)$ tends to a non-zero constant. $f(k) \rightarrow g(k)$ if $f(k)/g(k)$ tends to 1.

II. CHANNEL MODEL

A. Channel law

In the single channel case [25], the tracer produces codewords for m users in a random fashion. This is achieved as follows: for each of the n segments a bias vector \mathbf{W} is drawn from a distribution $f_{\mathbf{W}}$ chosen by the tracer, and $X_j \in \{0, 1, \dots, q-1\}$ is assigned for user j according to a categorical distribution with parameters $\{W_i\}_{i=0}^{q-1}$:

$$\mathbb{P}(X_j = x | \mathbf{W} = \mathbf{w}) = w_x. \quad (1)$$

The users are assigned their codewords independently by the tracer, and hence we also have:

$$\mathbb{P}(X_1 = x_1, \dots, X_m = x_m | \mathbf{W} = \mathbf{w}) = \prod_{j=1}^m w_{x_j}. \quad (2)$$

Note that we do not include a segment index since this procedure is repeated for all segments independently, hence producing the codewords $\{\mathbf{X}_j\}_{j=1}^m$, where $\mathbf{X}_j = (X_{j,1}, \dots, X_{j,n})$.

We now describe an analogous procedure for producing the codewords of m users in the case of multiple TV channels. We adopt the same notation as in the case of a single TV channel, and one can recover the single TV channel description by setting $L = 1$ in what follows. The tracer produces codewords $\{\hat{\mathbf{X}}_1, \dots, \hat{\mathbf{X}}_m\}$ with $\mathbf{X}_j^l \in \{0, 1, \dots, q-1\}^n$ denoting the l -th codeword for user j . This is done by choosing L i.i.d bias vectors at each segment, and each segment is independent of other segments. That is, let $\hat{\mathbf{W}}_i$ be the bias vectors at segment i , then:

$$\begin{aligned} f_{\hat{\mathbf{W}}_1, \dots, \hat{\mathbf{W}}_n}(\hat{\mathbf{w}}_1, \dots, \hat{\mathbf{w}}_n) &= \prod_{i=1}^n f_{\hat{\mathbf{W}}_i}(\hat{\mathbf{w}}_i) \\ &= \prod_{i=1}^n \prod_{l=1}^L f_{\mathbf{W}_i^l}(\mathbf{w}_i^l) = \prod_{i=1}^n \prod_{l=1}^L f_{\mathbf{W}}(\mathbf{w}_i^l), \end{aligned} \quad (3)$$

For any $l \in \{1, \dots, L\}$ and $i \in \{1, \dots, n\}$, $\{X_{j,i}^l\}_{j=1}^m$ are i.i.d and drawn from a categorical distribution:

$$\mathbb{P}(X_{1,i}^l = x_1, \dots, X_{m,i}^l = x_m | \mathbf{W}_i^l = \mathbf{w}) = \prod_{j=1}^m w_{x_j}. \quad (4)$$

The pirates receive codewords $\hat{\mathbf{X}}_{\mathcal{K}}$, and produce the output $\hat{\mathbf{Y}}$, where $\mathbf{Y}^l \in \mathcal{Y}^n$ (we assume an RDM setting, i.e. $\mathcal{Y} = \mathcal{X}$),

³In this work, we do not make a distinction between K and k , i.e. we assume the real number of colluders is known to the tracer.

according to a pmf $p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}$, where $\{\hat{S}_i\}_{i=1}^n$ is the assignment of pirates to channels at each segment, i.e. S_i^l is a random subset of \mathcal{K} that we assume is independent of $X_{\mathcal{K},i}^l$. Let \tilde{L} be the maximum number of channels a single user can simultaneously tune in to⁴, then for any segment i and TV channel l , a realization s_i^l is an assignment

$$s_i^l : l \mapsto 2^{\mathcal{K}}, \quad (5)$$

that respects the following:

$$s_i^l \neq \emptyset, \quad (6)$$

$$\bigcup_{l=1}^L s_i^l = \mathcal{K}, \quad (7)$$

$$\bigcap_{l \in \tilde{\mathcal{L}}} s_i^l = \emptyset, \forall \tilde{\mathcal{L}} \subseteq \mathcal{L}, |\tilde{\mathcal{L}}| > \tilde{L}. \quad (8)$$

Equation (8) states that a single pirate can not be assigned to more than \tilde{L} TV channels. We further assume memorylessness and no feedback of the collusion channel, which implies:

$$p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}(\hat{\mathbf{y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}) = \prod_{i=1}^n p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}(\hat{y}_i|\hat{x}_{\mathcal{K},i},\hat{s}_i), \quad (9)$$

and in what follows, we drop the segment index on random variables. In this work, we restrict to the case of each user having access to only one of the TV channels at each segment, i.e. $\tilde{L} = 1$ (and so $K \geq L$). In this case $\{s^l\}_{l=1}^L$ form a partition of \mathcal{K} , or more precisely, \hat{s} defines a weak ordering of \mathcal{K} where pirates assigned to the same TV channel are tied. The size of the support for \hat{S} (denoted by $\hat{\mathcal{S}}$) is then given by⁵:

$$|\hat{\mathcal{S}}| = L! \left\{ \begin{matrix} K \\ L \end{matrix} \right\}, \quad (10)$$

where $\left\{ \begin{matrix} a \\ b \end{matrix} \right\}$ denotes Stirling numbers of the second kind. If we instead disregard the identity of the colluders assigned to each channel, and only keep their numbers, the support size would shrink to⁶ $\binom{K-1}{L-1}$. Furthermore, if we also disregard the TV channel labels, the support size would become $P(K, L)$, which is the number of partitions of K into exactly L parts. It is common in the literature to assume colluder symmetry, i.e. all pirates share the risk equally. Furthermore, it is logical to assume TV channel symmetry, i.e. all L TV channels are equally important. Therefore in practice, finding an optimal distribution over $\{\hat{s}\}$ is the same as finding an optimal distribution over $P(K, L)$ partitions. Since $\tilde{L} = 1$, i.e. $\{s^l\}_{l=1}^L$ are disjoint, then we can simplify equation (9) by writing:

$$p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}(\hat{\mathbf{y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}) = \prod_{i=1}^n \prod_{l=1}^L p_{Y^l|X_{S^l}^l,S^l}(y_i^l|x_{s_i^l,i}^l,s_i^l), \quad (11)$$

⁴We assume pirates have the same accessibility constraints as normal users, i.e. access to the same hardware.

⁵ $\left\{ \begin{matrix} K \\ L \end{matrix} \right\}$ counts the number of ways we can partition \mathcal{K} into L non-empty subsets, while the $L!$ factor orders them across TV channels. Otherwise, it can be viewed as putting K distinguishable balls into L distinguishable bins.

⁶It can be viewed as putting K indistinguishable balls into L distinguishable bins, which can be easily proved using stars and bars.

i.e. colluders on different TV channels do not communicate after being assigned. Applying TV channel symmetry to (11), i.e. removing any bias towards a particular TV channel in the pirates' strategy (it is true for the tracer, i.e. $\{X_{\mathcal{K}}^l\}_{l=1}^L$ are i.i.d.), then we can write:

$$p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}(\hat{\mathbf{y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}) = \prod_{i=1}^n \prod_{l=1}^L p_{Y^l|X_{S^l}^l,S^l}(y_i^l|x_{s_i^l,i}^l,s_i^l). \quad (12)$$

Given x_s (a realization of X_S), we define the tally vector \mathbf{m} as the following:

$$\mathbf{m} \triangleq (m_0, \dots, m_{q-1}), \quad (13)$$

$$m_\alpha \triangleq |\{j \in s : x_j = \alpha\}|. \quad (14)$$

Imposing colluder symmetry, we can write:

$$p_{\hat{\mathbf{Y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}}(\hat{\mathbf{y}}|\hat{\mathbf{x}}_{\mathcal{K}},\hat{\mathbf{s}}) = \prod_{i=1}^n \prod_{l=1}^L p_{Y^l|\mathbf{M}^l}(y_i^l|\mathbf{m}_i^l), \quad (15)$$

where \mathbf{m}_i^l is the tally vector received by the pirates assigned to the l -th TV channel at segment i , and we assume $p_{Y^l|\mathbf{M}^l}$ abides by the marking assumption. Note that unlike the single TV channel⁷ case ($L = 1$), $|\mathbf{M}^l| = |S^l| \triangleq C^l$ is a random variable, which is the number of colluders assigned to attack TV channel l . Another implication of the TV channel symmetry condition is the following:

$$p_{C^l}(c^l) = p_C(c^l), \quad (16)$$

i.e. the number of pirates assigned to attack different TV channels must be identically distributed. This follows since $p_{\hat{C}}$ together with $p_{Y|\mathbf{M}}$ form the pirates' strategy. Figure 1 showcases the process of producing the colluders outputs across the L TV channels. Note that from colluder symmetry, $p_{\hat{S}|\hat{C}}$ is specified by the rule:

$$p_{\hat{S}|\hat{C}}(\hat{s}|\hat{c}) = \begin{cases} \frac{1}{\binom{K}{c^1, c^2, \dots, c^L}}, & |s^l| = c^l, \forall l \in \mathcal{L} \\ 0, & \text{otherwise} \end{cases}, \quad (17)$$

where $\binom{K}{c^1, c^2, \dots, c^L}$ is the multinomial coefficient.

Lemma 1. $\{\mathbf{M}^l\}_{l=1}^L$ are identically distributed.

*Proof.*⁸

$$\begin{aligned} p_{\mathbf{M}^l}(\mathbf{m}) &= \sum_{\mathbf{w}} p_{\mathbf{M}^l|\mathbf{w}^l}(\mathbf{m}|\mathbf{w}) f_{\mathbf{w}}(\mathbf{w}) \\ &= \sum_c \sum_{\mathbf{w}} p_{C^l}(c) p_{\mathbf{M}^l|\mathbf{w}^l, C^l}(\mathbf{m}|\mathbf{w}, c) f_{\mathbf{w}}(\mathbf{w}) \\ &= \sum_c \sum_{\mathbf{w}} p_C(c) p_{\mathbf{M}^l|\mathbf{w}^l, C^l}(\mathbf{m}|\mathbf{w}, c) f_{\mathbf{w}}(\mathbf{w}) \\ &\stackrel{(a)}{=} \sum_c \sum_{\mathbf{w}} p_C(c) p_{\mathbf{M}|\mathbf{w}, C}(\mathbf{m}|\mathbf{w}, c) f_{\mathbf{w}}(\mathbf{w}) = p_{\mathbf{M}}(\mathbf{m}), \end{aligned} \quad (18)$$

⁷In the single channel case this would be equal to K , which is usually unknown but constant.

⁸Summations over \mathbf{w} can be appropriately replaced by integrals in the case of $f_{\mathbf{w}}$ being a density.

where in (a) we used the fact that $p_{\mathbf{M}^l|\mathbf{W}^l, C^l}$ is a multinomial distribution regardless of l . \square

Lemma 2. $\{Y^l\}_{l=1}^L$ are identically distributed.

Proof.

$$\begin{aligned} p_{Y^l}(y^l) &= \sum_{\mathbf{m}^l} p_{Y^l|\mathbf{M}^l}(y^l|\mathbf{m}^l) p_{\mathbf{M}^l}(\mathbf{m}^l) \\ &= \sum_{\mathbf{m}^l} p_{Y|\mathbf{M}}(y^l|\mathbf{m}^l) p_{\mathbf{M}}(\mathbf{m}^l) = p_Y(y^l), \end{aligned} \quad (19)$$

where the equalities follow from Lemma 1 and TV channel symmetry ($p_{Y|\mathbf{M}}$ is part of the pirates' strategy). \square

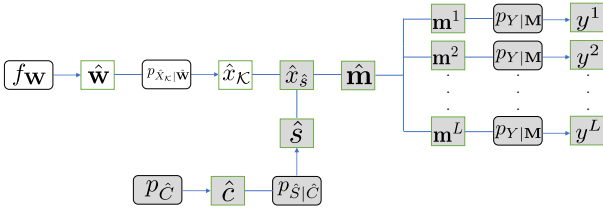


Fig. 1: A schematic diagram that shows the watermarking/collusion process. Arrows indicate drawing realizations from a pmf, while straight lines indicate use of those realizations. White boxes correspond to the tracer, while grey boxes correspond to the coalition.

B. Payoff functional

For any $l \in \{1, \dots, L\}$, we define the single channel payoff as:

$$\begin{aligned} \frac{I(Y^l; \mathbf{M}^l | C^l = c, \mathbf{W}^l)}{c} &= \frac{I(Y; \mathbf{M} | C = c, \mathbf{W})}{c} \\ &\triangleq \mathcal{I}_c(\mathbf{W}, p_{Y|\mathbf{M}, C=c}), \end{aligned} \quad (20)$$

where equality follows from Lemma 1, Lemma 2, and $\{\mathbf{W}^l\}_{l=1}^L$ being i.i.d. In analogy to the single channel case [25], we define the multi channel payoff as the following:

$$J_{k,L}[f_{\mathbf{W}}, p_{Y|\mathbf{M}}, p_{\hat{C}}] \triangleq \frac{I(\hat{Y}; \hat{\mathbf{M}} | \hat{\mathbf{W}})}{k}. \quad (21)$$

From here on, we restrict our attention to the binary alphabet case $\mathcal{X} = \{0, 1\} = \mathcal{Y}$, and we wish to evaluate $J_{k,L}[f_{\mathbf{W}}, p_{Y|\mathbf{M}}, p_{\hat{C}}]$ for this case. We define the random variables $\{Z^l\}_{l=1}^L$ by:

$$Z^l \triangleq \sum_{j \in S^l} X_j^l, \quad (22)$$

which counts the number of 1s received by the pirates assigned to the l -th TV channel. Equation (16) and Lemma 1 imply that $\{Z^l\}_{l=1}^L$ and $\{C^l\}_{l=1}^L$ are sets of identically distributed random variables. Therefore, we can talk about Z and C with no reference to a TV channel label. We also use the scalar bias

W instead of \mathbf{W} , which is the probability of assigning a user the symbol 1. Using this notation, we define the following:

$$\begin{aligned} p_{Z|C,W}(z|c, w) &\triangleq \alpha_z(w, c) \\ &= \begin{cases} \binom{c}{z} w^z (1-w)^{c-z}, & 0 \leq z \leq c \\ 0, & \text{otherwise} \end{cases}, \end{aligned} \quad (23)$$

$$\begin{aligned} p_{Z,C|W}(z, c|w) &= p_{C|W}(c|w) p_{Z|C,W}(z|c, w) \\ &= p_C(c) \alpha_z(c, w), \end{aligned} \quad (24)$$

$$\pi_{z,c} \triangleq p_{Y|Z,C}(1|z, c), \quad 0 \leq z \leq c. \quad (25)$$

Note that (Z^l, C^l) is a sufficient statistic for determining Y^l , while (W^l, C^l) is a sufficient statistic for determining Z^l , therefore we have the following (keeping in mind that $\{W^l\}_{l=1}^L$ are i.i.d.):

$$\begin{aligned} p_{\hat{Y}|\hat{Z}, \hat{C}, \hat{W}}(\hat{y}|\hat{z}, \hat{c}, \hat{w}) &= \prod_{l=1}^L p_{Y^l|Z^l, C^l}(y^l|z^l, c^l) \\ &= \prod_{l=1}^L p_{Y^l|Z^l, C^l, W^l}(y^l|z^l, c^l, w^l) \\ &= \prod_{l=1}^L p_{Y|Z,C,W}(y^l|z^l, c^l, w^l), \end{aligned} \quad (26)$$

$$\begin{aligned} p_{\hat{Z}|\hat{C}, \hat{W}}(\hat{z}|\hat{c}, \hat{w}) &= \prod_{l=1}^L p_{Z^l|C^l, W^l}(z^l|c^l, w^l) = \prod_{l=1}^L \alpha_{z^l}(w^l, c^l). \end{aligned} \quad (27)$$

Lemma 3. $p_{\hat{Y}|\hat{C}, \hat{W}}(\hat{y}|\hat{c}, \hat{w}) = \prod_{l=1}^L p_{Y|C,W}(y^l|c^l, w^l)$.

Proof. See Appendix A \square

Lemma 4.

$$\begin{aligned} I(\hat{Y}; \hat{Z} | \hat{C} = \hat{c}, \hat{W}) &= \sum_{l=1}^L c^l \mathcal{I}_{c^l}(W, \pi_{c^l}), \\ \pi_c &\triangleq (\pi_{0,c}, \dots, \pi_{c,c}). \end{aligned}$$

Proof. See Appendix B \square

Lemma 5. $\mathcal{I}_c(W, \pi_c)$ coincides with the single channel payoff for c pirates as defined in [25].

Proof. The pirate strategy consists of $p_{\hat{C}}$, as well as the vectors $\{\pi_{c'}\}_{c'=1}^{k-L+1}$. Note that $\mathcal{I}_c(W, \pi_c)$ is independent of $p_{\hat{C}}$ and all $\{\pi_{c'} : c' \neq c\}$, i.e. it only depends on f_W and π_c . \square

Lemma 6. $2 \ln 2 c^2 \mathcal{I}_c(W, \pi_c) \geq 4 \left[\int_0^1 \frac{dw}{f_W(w) w (1-w)} \right]^{-1}$.

Proof. This follows from Theorem 7 in [25]. \square

III. ASYMPTOTIC THEOREM

We wish to obtain the asymptotic behavior of the payoff given in equation (21) (for $q = 2, \tilde{L} = 1$), as well as the solution to the asymptotic maximin game in analogy to the single TV channel case. For the single TV channel case [25], this is referred to as the asymptotic saddle point value, which is the limit of the maximin value of the payoff as the number

of pirates is sent to infinity. This is also accompanied by the asymptotic optimal strategies for both tracer and pirates, which are the asymptotic solutions to the maximin game. However, as this makes logical sense in terms of taking the limit of the maximin game, this is usually not solved in the same way as it is formulated. Instead of taking the limit of a sequence of optimal payoffs (and optimal strategies), which is not possible given no closed form solution exists for either, the payoff is approximated for large number of pirates and solved in the limit. This can be justified if the optimal payoff converges uniformly in the limit, which is usually glossed over in the literature. Nevertheless, we shall adopt the same approach and write down an expansion of our payoff function. In analogy to the single channel case, we make the following regularity assumptions:

- For any $c \in \{1, \dots, k - L + 1\}$, there exists a bounded, twice differentiable function $g_c(x)$ for $x \in [0, 1]$ with $g(0) = 0$ and $g(1) = 1$ such that:

$$\pi_{z,c} = g_c\left(\frac{z}{c}\right), \quad \forall z \in \{0, \dots, c\}, \quad (28)$$

$$\lim_{k \rightarrow \infty} g_c(x) \triangleq g(x), \quad c \in w(1). \quad (29)$$

Lemma 7. Let

$$G[g_c(w)] \triangleq \arccos[1 - 2g_c(w)], \quad (30)$$

$$\mathcal{J}[g_c(w)] \triangleq w(1 - w) [G'(w)]^2, \quad (31)$$

$$\bar{\mathcal{J}}[g_c(W)] \triangleq \mathbb{E}_{f_W} [\mathcal{J}[g_c(W)]], \quad (32)$$

where the derivative is w.r.t w , then we can write:

$$\mathcal{I}_c(W, \pi_c) = \frac{1}{c^2 \ln 2} \bar{\mathcal{J}}[g_c(W)] + o\left(\frac{1}{c^2}\right). \quad (33)$$

Proof. This follows from Theorem 8 in [25]. \square

Lemma 8. $\bar{\mathcal{J}}[g(W)] \geq \pi^2 \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1}$, with equality iff $g(w) = g_{\text{opt}}(w)$ given by:

$$g_{\text{opt}}(w) = \frac{1}{2} \left[1 - \cos \left(\frac{\pi \int_0^w \frac{dv}{f_W(v)v(1-v)}}{\int_0^1 \frac{dv}{f_W(v)v(1-v)}} \right) \right]. \quad (34)$$

Proof. This is Lemma 7 in [25]. \square

For $q = 2, \tilde{L} = 1$, we can rewrite equation (21) as:

$$\begin{aligned} J_{k,L}[f_W, p_{Y|Z,C}, p_C] &= k^{-1} I(\hat{Y}; \hat{Z} | \hat{C}, \hat{W}) + k^{-1} I(\hat{Y}; \hat{C} | \hat{W}) \\ &= k^{-1} \sum_{\hat{c}} p_{\hat{C}}(\hat{c}) \sum_{l=1}^L c^l \mathcal{I}_{c^l}(W, \pi_{c^l}) + k^{-1} I(\hat{Y}; \hat{C} | \hat{W}) \\ &= k^{-1} L \sum_c p_C(c) c \mathcal{I}_c(W, \pi_c) + k^{-1} I(\hat{Y}; \hat{C} | \hat{W}), \end{aligned} \quad (35)$$

where the second equality follows from Lemma 4, and the third equality follows from $\{C^l\}_{l=1}^L$ having the same marginal, as dictated by $p_{\hat{C}}$ being symmetric under permutations (TV

channel symmetry), i.e. C denotes the number of pirates assigned to any TV channel.

Lemma 9. Let

$$\tilde{J}_{k,L}[f_W, p_{Y|Z,C}, p_C] \triangleq \sum_c p_C(c) \frac{c}{k} \mathcal{I}_c(W, \pi_c), \quad (36)$$

then an asymptotically optimal⁹ p_C for \tilde{J} must obey:

$$\lim_{k \rightarrow \infty} \frac{p_C(c) k^\alpha}{c^\alpha} < \infty, \quad (37)$$

for some $\alpha \geq 1$, and \tilde{J} optimally decays like $1/k^2$.

Proof. We know that c can at most grow as a fraction of k , that is, the value $q \triangleq c/k$ can only belong to $[0, 1]$ in the limit. That is, we can divide the summation in \tilde{J} as follows:

$$\begin{aligned} \tilde{J} &= \sum_{c \sim k} p_C(c) \frac{c}{k} \left(\frac{1}{c^2 \ln 2} \bar{\mathcal{J}}[g_c(W)] + o\left(\frac{1}{c^2}\right) \right) \\ &\quad + \sum_{c \in w(1) \cap o(k)} p_C(c) \frac{c}{k} \left(\frac{1}{c^2 \ln 2} \bar{\mathcal{J}}[g_c(W)] + o\left(\frac{1}{c^2}\right) \right) \\ &\quad + \sum_{c \in O(1)} p_C(c) \frac{c}{k} \mathcal{I}_c(W, \pi_c), \end{aligned} \quad (38)$$

where note that $\bar{\mathcal{J}}$ is bounded in the limit. For non-decaying measure $p_C(c)$, we can see from (38) that the first term decays like $1/k^2$, the second term decays like $1/kc$ where c is sub-linear in k , and the last term decays like $1/k$. Therefore if $p_C(c)$ in the last two terms is not small enough in the limit, the payoff will decay slower than $1/k^2$. Any strategy that assigns asymptotically small enough measure in the last two terms will hence produce a lower value for the payoff given large enough k , nevertheless, the first term will always decay like $1/k^2$. \square

Lemma 10. $\mathbb{E}_{p_C} \left[\frac{C}{k} \right] = \frac{1}{L}$.

Proof.

$$\begin{aligned} \sum_c p_C(c) \frac{c}{k} &= \frac{1}{L} \sum_{l=1}^L \sum_c p_C(c) \frac{c}{k} = \frac{1}{L} \sum_{l=1}^L \sum_{c^l} p_C(c^l) \frac{c^l}{k} \\ &= \frac{1}{L} \sum_{c^1, \dots, c^L} p_{C^1, \dots, C^L}(c^1, \dots, c^L) \frac{c^1 + \dots + c^L}{k} = \frac{1}{L}. \end{aligned} \quad (39)$$

Lemma 11. $\sum_c p_C(c) \frac{k}{c} \geq L$, with equality iff $p_C(k/L) = 1$.

Proof.

$$\mathbb{E}_{p_C} \left[\frac{k}{C} \right] = k \mathbb{E}_{p_C} \left[\frac{1}{C} \right] \geq k \frac{1}{\mathbb{E}_{p_C}[C]} = \frac{1}{\mathbb{E}_{p_C} \left[\frac{C}{k} \right]} = L, \quad (40)$$

⁹An asymptotically optimal sequence of strategies for the pirates is one that produces the lowest value for the payoff in the limit.

which is an application of Jensen's inequality to a strictly convex function. \square

Lemma 12. Let $\alpha \geq 1$, then $\sum_{c \sim k} p_C(c) \frac{k}{c} \geq L + \dots$, where terms in ellipsis go to zero in the limit $k \xrightarrow{c} \infty$.

Proof. See Appendix C. \square

Lemma 13. For $\alpha = 1$, $\tilde{p}_C(c) \triangleq \frac{p_C(c)k}{c}$, and up to $o(1/k^2)$, we have the following lower bound for \tilde{J} :

$$\tilde{J}_{\alpha=1} \geq \frac{\pi^2 L}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \cdot \left(1 + L^{-1} \sum_{c \in w(1) \cap o(k)} \tilde{p}_C(c) + \frac{4L^{-1}}{\pi^2} \sum_{c \in O(1)} \tilde{p}_C(c) \right). \quad (41)$$

Proof. For $\alpha = 1$, all terms in \tilde{J} become of order $1/k^2$, and we can write:

$$\begin{aligned} \tilde{J}_{\alpha=1} &= \sum_{c \sim k} \tilde{p}_C(c) \left(\frac{1}{k^2 2 \ln 2} \tilde{\mathcal{J}}[g_c(W)] + o\left(\frac{1}{k^2}\right) \right) \\ &+ \sum_{c \in w(1) \cap o(k)} \tilde{p}_C(c) \left(\frac{1}{k^2 2 \ln 2} \tilde{\mathcal{J}}[g_c(W)] + o\left(\frac{1}{k^2}\right) \right) \\ &+ \sum_{c \in O(1)} \tilde{p}_C(c) \frac{c^2}{k^2} \mathcal{I}_c(W, \pi_c) \\ &= \frac{1}{k^2 2 \ln 2} \left(\sum_{c \sim k} \tilde{p}_C(c) \tilde{\mathcal{J}}[g_c(W)] \right. \\ &+ \sum_{c \in w(1) \cap o(k)} \tilde{p}_C(c) \tilde{\mathcal{J}}[g_c(W)] \\ &+ \left. \sum_{c \in O(1)} \tilde{p}_C(c) 2 \ln 2 c^2 \mathcal{I}_c(W, \pi_c) \right) + o\left(\frac{1}{k^2}\right), \end{aligned} \quad (42)$$

where note that $\tilde{p}_C(c) = \frac{p_C(c)k}{c}$ is bounded in the limit. We can replace $\tilde{\mathcal{J}}[g_c(W)]$ in the first two terms by $\tilde{\mathcal{J}}[g(W)]$, and the remainder will still decay faster than $1/k^2$. That is, up to

$o(1/k^2)$, we have the following:

$$\begin{aligned} &\frac{1}{k^2 2 \ln 2} \left(\sum_{c \sim k} \tilde{p}_C(c) \tilde{\mathcal{J}}[g(W)] + \sum_{c \in w(1) \cap o(k)} \tilde{p}_C(c) \tilde{\mathcal{J}}[g(W)] \right. \\ &+ \left. \sum_{c \in O(1)} \tilde{p}_C(c) 2 \ln 2 c^2 \mathcal{I}_c(W, \pi_c) \right) \\ &= \frac{1}{k^2 2 \ln 2} \left(\tilde{\mathcal{J}}[g(W)] \sum_{c \in w(1)} \tilde{p}_C(c) \right. \\ &+ \left. \sum_{c \in O(1)} \tilde{p}_C(c) 2 \ln 2 c^2 \mathcal{I}_c(W, \pi_c) \right) \geq \\ &\frac{1}{k^2 2 \ln 2} \left(\pi^2 \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \sum_{c \in w(1)} \tilde{p}_C(c) \right. \\ &+ \left. 4 \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \sum_{c \in O(1)} \tilde{p}_C(c) \right) \\ &= \frac{1}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \pi^2 \cdot \\ &\left(\sum_{c \in w(1)} \tilde{p}_C(c) + \frac{4}{\pi^2} \sum_{c \in O(1)} \tilde{p}_C(c) \right), \end{aligned} \quad (43)$$

where the inequality follows from Lemma 6 and Lemma 8. Finally, applying Lemma 12, we obtain the desired bound. \square

Lemma 14. For $\alpha > 1$, we have the following lower bound for \tilde{J} :

$$\tilde{J}_{\alpha>1} \geq \frac{L}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \pi^2 + o\left(\frac{1}{k^2}\right), \quad (44)$$

with conditions for equality being:

$$g(w) = g_{\text{opt}}(w), \quad (45)$$

$$\lim_{k \rightarrow \infty} p_C(k/L) = 1, \quad (46)$$

where $g_{\text{opt}}(w)$ is given by equation (34).

Proof. Note that in equation (42), for any choice of $\alpha > 1$, the second two terms will decay faster than $1/k^2$, while the first term will dominate since it decays as $1/k^2$ for any value of α . Therefore choosing $\alpha > 1$ makes the contribution from $c \sim k$ negligible in the limit, and so repeating the same steps as in the proof of Lemma 13, we obtain:

$$\begin{aligned} \tilde{J}_{\alpha>1} &\geq \frac{\pi^2}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \sum_{c \sim k} p_C(c) \frac{k}{c} + o\left(\frac{1}{k^2}\right) \\ &\geq \frac{\pi^2 L}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} + o\left(\frac{1}{k^2}\right). \end{aligned} \quad (47)$$

Conditions for equality follow from Lemma 8 and Lemma 11. \square

Lemma 15. $\alpha > 1$, $g_{\text{opt}}(w)$ and $p_C^*(c) \triangleq \delta(c, k/L)$ are asymptotically optimal for \tilde{J} .

Proof. This follows directly from Lemma 9, Lemma 13, and Lemma 14. Note that the lower bound for $\tilde{J}_{\alpha=1}$ given in Lemma 13 is asymptotically larger than the lower bound for $\tilde{J}_{\alpha>1}$ given in Lemma 14, and since $g_{\text{opt}}(w)$ and $p_C^*(c)$ achieve this lower bound for $\tilde{J}_{\alpha>1}$, we conclude that the optimal sequence of pirate strategies must have $\alpha > 1$ with its limit being $(g_{\text{opt}}(w), p_C^*)$. \square

Lemma 16.

$$\left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \pi^2 \leq 1, \quad (48)$$

with equality iff f_W is the arcsine distribution: $f_W^*(w) \triangleq \left(\pi \sqrt{w(1-w)} \right)^{-1}$.

Proof. This is Lemma 4 in [25]. \square

Lemma 17. f_W^* is asymptotically optimal for \tilde{J} .

Proof. From Lemma 14 and Lemma 15, the asymptotically optimal f_W is the maximiser of

$$\frac{L}{k^2 2 \ln 2} \left[\int_0^1 \frac{dw}{f_W(w)w(1-w)} \right]^{-1} \pi^2,$$

which is f_W^* by Lemma 16. \square

Lemma 18. The payoff function $\tilde{J}_{k,L}$ has the following asymptotic behavior:

$$\max_{f_W} \min_{\{\pi\}, p_C} \tilde{J}_{k,L} \rightarrow \frac{L^2}{k^2 2 \ln 2}, \quad (49)$$

with asymptotically optimal strategies being (f_W^*, g^*, p_C^*) , where $g^*(w) \triangleq w$ is the interleaving attack.

Proof. This follows directly from Lemma 14, Lemma 15, and Lemma 17. \square

We are now in a position to present the main result of the work, concerning the asymptotic behavior of our payoff function as defined in equation (35). To this end, we define the following degenerate distribution:

$$p_C^*(\hat{c}) \triangleq \prod_{l=1}^L \delta(c^l, k/L) = \begin{cases} 1, & \hat{c} = (k/L, k/L, \dots, k/L) \\ 0, & \text{otherwise} \end{cases}, \quad (50)$$

which corresponds to the strategy where the pirates equally populate the L TV channels.

Theorem 1. The payoff function in equation (35) has the following asymptotic behavior:

$$\max_{f_W} \min_{\{\pi\}, p_C} J_{k,L} \rightarrow \frac{L^2}{k^2 2 \ln 2}, \quad (51)$$

with asymptotically optimal strategies being (f_W^*, g^*, p_C^*) .

Proof. From equation (35), we can see that

$$J = L\tilde{J} + k^{-1}I(\hat{Y}; \hat{C}|\hat{W}),$$

and the minimum of $I(\hat{Y}; \hat{C}|\hat{W})$ is zero. For any f_W and g , this is achieved when \hat{C} is deterministic, i.e. as in p_C^* . Optimality of (f_W^*, g^*, p_C^*) follows from Lemma 18, as well as the asymptotic value. \square

IV. ALTERNATIVE PAYOFF AND FINGERPRINTING CAPACITY

The maximin game of our payoff given by equation (21) (or equation (35) for the binary alphabet case) is a direct generalization of the single TV channel payoff in [25], i.e. if we set $L = 1$ for the maximin game, we recover the single TV channel payoff that defines the fingerprinting capacity, which is asymptotically equal to $(k^2 2 \ln 2)^{-1}$ in the binary alphabet case [25]. Nevertheless, this is not the only generalization that reduces to the single TV channel payoff when setting $L = 1$. If we consider the payoff $R_{k,L} \triangleq k^{-1}I(\hat{Y}; \hat{X}_K|\hat{\mathbf{W}})$, the maximin game will also reduce to the single TV channel case when $L = 1$. This payoff is generally smaller than our payoff $J_{k,L}$, and the difference term (up to k) is $I(\hat{Y}; \hat{S}|\hat{X}_K) = I(\hat{Y}; \hat{\mathbf{M}}|\hat{X}_K)$, i.e. we can write:

$$\begin{aligned} I(\hat{Y}; \hat{X}_K|\hat{\mathbf{W}}) &= kJ_{k,L} - I(\hat{Y}; \hat{S}|\hat{X}_K) \\ &= kJ_{k,L} - I(\hat{Y}; \hat{\mathbf{M}}|\hat{X}_K) = I(\hat{Y}; \hat{\mathbf{M}}|\hat{\mathbf{W}}) - I(\hat{Y}; \hat{\mathbf{M}}|\hat{X}_K). \end{aligned} \quad (52)$$

$R_{k,L}$ could possibly have different asymptotic behavior compared to $J_{k,L}$. However, since it can not be larger than $J_{k,L}$, we can write (in the binary alphabet case):

$$\max_{f_W} \min_{\{\pi\}, p_C} R_{k,L} \rightarrow \frac{N^2}{k^2 2 \ln 2}, \quad (53)$$

for some $N \leq L$. It is plausible that N is in fact equal to L , and the asymptotic maximin games for both $R_{k,L}$ and $J_{k,L}$ are identical. This is motivated by the fact that the difference term $I(\hat{Y}; \hat{S}|\hat{X}_K)$ extracts information about the choice of pirates assigned to the different TV channels from their outputs \hat{Y} , and asymptotically we expect likely realizations of \hat{X}_K to be insensitive to who the pirates choose to assign for the different TV channels. That is, as long as they choose large enough numbers of pirates to populate the TV channels, we expect that knowing \hat{S} will not be significant if we already know \hat{X}_K . This of course hinges on the argument that the pirates should assign large numbers to all L TV channels, which is also in line of what one would expect. This leads us to the following conjecture:

Conjecture 1. For the binary alphabet case, and $\tilde{L} = 1$, the payoff functional $R_{k,L}$ given by:

$$R_{k,L} = J_{k,L} - \frac{1}{k}I(\hat{Y}; \hat{S}|\hat{X}_K) \quad (54)$$

has the following asymptotic behavior:

$$\max_{f_W} \min_{\{\pi\}, p_C} R_{k,L} \rightarrow \frac{L^2}{k^2 2 \ln 2}, \quad (55)$$

with optimal strategies

$$\begin{aligned} f_W^*(w) &= \left(\pi \sqrt{w(1-w)} \right)^{-1}, \\ g^*(w) &= w, \\ p_C^*(\hat{c}) &= \prod_{l=1}^L \delta(c^l, k/L). \end{aligned}$$

The payoffs $J_{k,L}$ and $R_{k,L}$ are the most natural generalizations of the single TV channel payoff in [25]. Assuming Conjecture 1 holds, then by Theorem 1, and Corollary 7 in [25], the asymptotic maximin value for both $J_{k,L}$ and $R_{k,L}$ is the same as the asymptotic fingerprinting capacity in the single TV channel case ($L = 1$). This prompts the question of whether this holds also for any L , i.e. if our payoff defines the fingerprinting capacity for multiple TV channels. Since the pirates choose \hat{S} independently of the watermarking procedure, and once \hat{S} is known the problem reduces to L independent single TV channels that abide by the assumptions used in [25], our direct generalization of the single TV channel payoff can very possibly define the capacity (in the limit $k \rightarrow \infty$) in this case as its maximin value, and this leads us to the following conjecture:

Conjecture 2. *The binary fingerprinting capacity in the multiple TV channels scenario (with $\tilde{L} = 1$) $C_{\text{fp}}^{\text{binary}}(k, L)$ has the asymptotic behavior:*

$$\max_{f_W} \min_{\{\pi\}, p_C} C_{\text{fp}}^{\text{binary}}(k, L) \rightarrow \frac{L^2}{k^2 2 \ln 2} \quad (56)$$

with optimal strategies

$$\begin{aligned} f_W^*(w) &= \left(\pi \sqrt{w(1-w)} \right)^{-1}, \\ g^*(w) &= w, \\ p_C^*(\hat{c}) &= \prod_{l=1}^L \delta(c^l, k/L). \end{aligned}$$

V. DISCUSSION

We have shown that when k colluders attack L TV channels simultaneously, the maximin value of the payoff defined in equation (35) has the asymptotic value $((k/L)^2 2 \ln 2)^{-1}$ with asymptotically optimal strategies being

$$\begin{aligned} f_W^*(w) &= \left(\pi \sqrt{w(1-w)} \right)^{-1}, \\ g^*(w) &= w, \\ p_C^*(\hat{c}) &= \prod_{l=1}^L \delta(c^l, k/L). \end{aligned}$$

This is exactly the same as having L independent single TV channels [25] with k/L colluders on each TV channel. This is expected as the payoff is independent of the identity of the pirates assigned to the TV channels, i.e. it is only sensitive to the number of colluders assigned to the different TV channels. The identity dependence is present in $I(\tilde{Y}; \hat{X}_K | \hat{W})$, namely in the difference term $I(\tilde{Y}; \hat{S} | \hat{X}_K)$, which possibly lowers

the value of the payoff by virtue of allowing the identity of the pirates assigned to a TV channel to be chosen uniformly randomly given they know the numbers $\{c^l\}_{l=1}^L$.

We have presented arguments that strongly suggest that this liberty the pirates enjoy, although it can be significantly advantageous for finite k , does become of less value asymptotically and the asymptotic maximin games of $I(\tilde{Y}; \hat{X}_K | \hat{W})$ and $I(\tilde{Y}; \hat{Z}, \hat{C} | \hat{W})$ are the same. It remains an open question to prove Conjecture 1, which is left for future work. Furthermore, we have argued that our payoff does predict how the fingerprinting capacity behaves asymptotically, and that it is indeed plausible that its maximin value can be replaced by the fingerprinting capacity in Theorem 1.

It is important to note that we have not used any saddle point property of the payoff (c.f. [25]) as it is simply not needed. That is, we make no claims of the maximin game yielding the same value for the payoff as the minimax game (applicability of Sion's theorem) for any of the payoffs discussed in this work. Although this is very possible, i.e. the strategies we found could be an equilibrium point, one still needs to show that the payoff considered is jointly convex in the pirates' strategies, e.g. if future directions require solving the maximin game numerically.

As other potential follow-up work, there remains the generalization to non-binary alphabet, the case where users can tune in to more than one TV channel simultaneously, i.e. $\tilde{L} \neq 1$, dynamic tracing, and perhaps most practically useful, the study of decoders and score functions suitable for multiple TV channel attacks. Furthermore, it would be also interesting to consider relaxing the TV channel symmetry assumption as one or more content channels might be of more of value to the coalition.

ACKNOWLEDGMENT

Part of this work was supported by NWO grant CS.001 (Forwardt).

REFERENCES

- [1] G. Tardos, "Optimal probabilistic fingerprint codes," in *ACM Symposium on Theory of Computing (STOC) 2003*, 2003, pp. 116–125.
- [2] —, "Optimal probabilistic fingerprint codes," *J. ACM*, vol. 55, no. 2, pp. 1–24, 2008.
- [3] O. Blayer and T. Tassa, "Improved versions of Tardos' fingerprinting scheme," *Designs, Codes and Cryptography*, vol. 48, no. 1, pp. 79–103, 2008.
- [4] T. Furon, A. Guyader, and F. C  rou, "On the design and optimization of Tardos probabilistic fingerprinting codes," in *Information Hiding 2008*, ser. LNCS, vol. 5284. Springer, 2008, pp. 341–356.
- [5] T. Furon, L. P  rez-Freire, A. Guyader, and F. C  rou, "Estimating the minimal length of Tardos code," in *Information Hiding 2009*, ser. LNCS, vol. 5806, 2009, pp. 176–190.
- [6] T. Laarhoven and B. de Weger, "Optimal symmetric Tardos traitor tracing schemes," *Designs, Codes and Cryptography*, pp. 1–21, 2012.
- [7] A. Simone and B.   kori  , "Accusation probabilities in Tardos codes: beyond the Gaussian approximation," *Designs, Codes and Cryptography*, vol. 63, no. 3, pp. 379–412, 2012.
- [8] B.   kori  , T. Vladimirova, M. Celik, and J. Talstra, "Tardos Fingerprinting is Better Than We Thought," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3663–3676, 2008.
- [9] B.   kori   and J.-J. Oosterwijk, "Binary and q-ary Tardos codes, revisited," *Designs, Codes, and Cryptography*, July 2013.

- [10] Y.-W. Huang and P. Moulin, "Capacity-achieving fingerprint decoding," in *IEEE Workshop on Information Forensics and Security (WIFS) 2009*, 2009, pp. 51–55.
- [11] K. Nuida, "Short collusion-secure fingerprint codes against three pirates," in *Information Hiding 2010*, ser. LNCS, vol. 6387. Springer, 2010, pp. 86–102.
- [12] K. Nuida, S. Fujitsu, M. Hagiwara, T. Kitagawa, H. Watanabe, K. Ogawa, and H. Imai, "An improvement of discrete Tardos fingerprinting codes," *Designs, Codes, and Cryptography*, vol. 52, no. 3, pp. 339–362, 2009.
- [13] E. Amiri and G. Tardos, "High rate fingerprinting codes and the fingerprinting capacity," in *SODA 2009*, 2009, pp. 336–345.
- [14] A. Charpentier, F. Xie, C. Fontaine, and T. Furon, "Expectation maximization decoding of Tardos probabilistic fingerprinting code," in *SPIE Media Forensics and Security 2009*, 2009, p. 72540.
- [15] P. Meerwald and T. Furon, "Towards Joint Tardos Decoding: The 'Don Quixote' Algorithm," in *Information Hiding 2011*, 2011, pp. 28–42.
- [16] J. Oosterwijk, B. Škorić, and J. Doumen, "Optimal suspicion functions for Tardos traitor tracing schemes," in *ACM Information Hiding and Multimedia Security Workshop (IH&MMSec) 2013*, 2013, pp. 19–28.
- [17] T. Furon and M. Desoubreaux, "Tardos codes for real," in *IEEE Workshop on Information Forensics and Security (WIFS) 2014*, 2014.
- [18] B. Škorić, "Tally-based simple decoders for traitor tracing and group testing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1221–1223, 2015.
- [19] B. Škorić and W. de Groot, "Generalized tally-based decoders for traitor tracing and group testing," in *IEEE Workshop on Information Forensics and Security (WIFS) 2015*, 2015.
- [20] A. Charpentier, C. Fontaine, T. Furon, and I. Cox, "An asymmetric fingerprinting scheme based on Tardos codes," in *Information Hiding 2011*, ser. LNCS, vol. 6958. Springer, 2011, pp. 43–58.
- [21] B. Škorić, S. Katzenbeisser, and M. Celik, "Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes," *Designs, Codes and Cryptography*, vol. 46, no. 2, pp. 137–166, 2008.
- [22] B. Škorić, S. Katzenbeisser, H. Schaathun, and M. Celik, "Tardos Fingerprinting Codes in the Combined Digit Model," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 906–919, 2011.
- [23] F. Xie, T. Furon, and C. Fontaine, "On-off keying modulation and Tardos fingerprinting," in *Multimedia & Security (MM&Sec) 2008*. ACM, 2008, pp. 101–106.
- [24] Y. Huang and P. Moulin, "On fingerprinting capacity games for arbitrary alphabets and their asymptotics," in *IEEE International Symposium on Information Theory (ISIT) 2012*, 2012, pp. 2571–2575.
- [25] —, "On the saddle-point solution and the large-coalition asymptotics of fingerprinting games," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 160–175, 2012.

APPENDIX A PROOF OF LEMMA 3

$$\begin{aligned}
p_{\hat{Y}|\hat{C},\hat{W}}(\hat{y}|\hat{c},\hat{w}) &= \sum_{\hat{z}} p_{\hat{Y}|\hat{C},\hat{Z},\hat{W}}(\hat{y}|\hat{c},\hat{z},\hat{w}) p_{\hat{Z}|\hat{C},\hat{W}}(\hat{z}|\hat{c},\hat{w}) = \\
&= \sum_{z^1} \cdots \sum_{z^L} \prod_{l=1}^L p_{Y^l|Z^l,C^l,W^l}(y^l|z^l,c^l,w^l) p_{Z^l|C^l,W^l}(z^l|c^l,w^l) \\
&= \sum_{z^1} \cdots \sum_{z^L} \prod_{l=1}^L p_{Y,Z|C,W}(y^l,z^l|c^l,w^l) \\
&= \prod_{l=1}^L p_{Y|C,W}(y^l|c^l,w^l).
\end{aligned} \tag{57}$$

APPENDIX B PROOF OF LEMMA 4

$$\begin{aligned}
I(\hat{Y}; \hat{Z}|\hat{C} = \hat{c}, \hat{W} = \hat{w}) &\stackrel{(a)}{=} H(\hat{Y}|\hat{C} = \hat{c}, \hat{W} = \hat{w}) - H(\hat{Y}|\hat{Z}, \hat{C} = \hat{c}, \hat{W} = \hat{w}) \\
&\stackrel{(b)}{=} H(\hat{Y}|\hat{C} = \hat{c}, \hat{W} = \hat{w}) \\
&\quad - \sum_{\hat{z}} p_{\hat{Z}|\hat{C},\hat{W}}(\hat{z}|\hat{c},\hat{w}) H(\hat{Y}|\hat{Z} = \hat{z}, \hat{C} = \hat{c}, \hat{W} = \hat{w}) \\
&\stackrel{(c)}{=} \sum_{l=1}^L H(Y|C = c^l, W = w^l) - \\
&\quad \sum_{\hat{z}} \prod_{l'=1}^L p_{Z|C,W}(z^{l'}|c^{l'},w^{l'}) \sum_{l=1}^L H(Y|Z = z^l, C = c^l, W = w^l) \\
&\stackrel{(d)}{=} \sum_{l=1}^L H(Y|C = c^l, W = w^l) \\
&\quad - \sum_{l=1}^L \sum_{z^l} p_{Z|C,W}(z^l|c^l,w^l) H(Y|Z = z^l, C = c^l, W = w^l) \\
&\stackrel{(e)}{=} \sum_{l=1}^L I(Y; Z|C = c^l, W = w^l),
\end{aligned} \tag{58}$$

where (a) and (b) follow from the definitions of conditional mutual information and conditional entropy; (c) follows from equations (26), (27), and Lemma 3; (d) follows by direct computation; (e) follows from the definition of conditional mutual information. Finally, it is straightforward to confirm that

$$I(\hat{Y}; \hat{Z}|\hat{C} = \hat{c}, \hat{W} = \hat{w}) = \sum_{l=1}^L I(Y; Z|C = c^l, W = w^l). \tag{59}$$

APPENDIX C PROOF OF LEMMA 12

$$\left[\sum_{c' \sim k} p_C(c') \right]^{-1} \sum_{c \sim k} p_C(c) \frac{c}{k} = \frac{1}{L} \left[\sum_{c' \sim k} p_C(c') \right]^{-1} \tag{60}$$

and so applying Jensen's inequality, we get:

$$\begin{aligned}
&\left[\sum_{c' \sim k} p_C(c') \right]^{-1} \sum_{c \sim k} p_C(c) \frac{k}{c} \geq \\
&\left[\frac{1}{L} \left[\sum_{c' \sim k} p_C(c') \right]^{-1} - \left[\sum_{c' \sim k} p_C(c') \right]^{-1} \sum_{c \sim k} p_C(c) \frac{c}{k} \right]^{-1},
\end{aligned} \tag{61}$$

and if we multiply both sides by $\sum_{c' \sim k} p_C(c')$, we arrive at:

$$\sum_{c \sim k} p_C(c) \frac{k}{c} \geq \left[\frac{1}{L} \left[\sum_{c' \sim k} p_C(c') \right]^{-2} - \left[\sum_{c' \sim k} p_C(c') \right]^{-2} \sum_{c \not\sim k} p_C(c) \frac{c}{k} \right]^{-1} \quad (62)$$

or simply:

$$\begin{aligned} \sum_{c \sim k} p_C(c) \frac{k}{c} &\geq L \frac{[\sum_{c' \sim k} p_C(c')]^2}{1 - L \sum_{c \not\sim k} p_C(c) \frac{c}{k}} \\ &= L \frac{[1 - \sum_{c' \not\sim k} p_C(c')]^2}{1 - L \sum_{c \not\sim k} p_C(c) \frac{c}{k}} \\ &= L \frac{\left[1 - \sum_{c' \not\sim k} \bar{p}_C(c') \left(\frac{c}{k}\right)^\alpha\right]^2}{1 - L \sum_{c \not\sim k} \bar{p}_C(c) \left(\frac{c}{k}\right)^{\alpha+1}}, \end{aligned} \quad (63)$$

where we write $\bar{p}_C(c) \triangleq p_C(c) \frac{k^\alpha}{c^\alpha}$, which is bounded in the limit. For $\alpha \geq 1$ and $c \not\sim k$, we have $c^\alpha/k^\alpha \rightarrow 0$.

A Distributed Adaptive Signal Fusion Framework for Spatial Filtering within a Wireless Sensor Network

Cem Ates Musluoglu, Charles Hovine and Alexander Bertrand

KU Leuven, Department of Electrical Engineering (ESAT),

STADIUS Center for Dynamical Systems, Signal Processing and Data Analytics, Belgium

{cemates.musluoglu, charles.hovine, alexander.bertrand}@esat.kuleuven.be

Abstract—The emergence of wireless sensor networks (WSNs) created the possibility to collect data and retrieve information in a way that was previously unfeasible or impractical. Fundamentally, WSNs consist of a multitude of spatially distributed sensor nodes which are able to locally process and communicate their measured data. Their usage has been adopted in a wide range of fields, such as health monitoring, acoustics and environmental studies among many others.

A specific task of interest is to find a filter which optimally fuses the signals over the network through a linear combination, i.e., spatial filtering. The filter is typically obtained as a result of an optimization problem involving the sensor signal statistics, e.g., a least squares problem or a (generalized) eigenvalue decomposition of the spatial covariance matrix of the sensor signals. Although a centralized setting – in which all the data acquired in the network is sent to a central node for processing – could be considered as a straightforward solution, it would create energy and communication bandwidth requirements which are too burdensome for many practical settings, implying the necessity of a fully distributed approach. Various algorithms have been proposed describing distributed approaches for signal processing, such as diffusion [1], incremental strategies [2] and consensus [3]. However, most of these existing methods for distributed signal processing make the assumption that the objective function f of the problem can be written as $\sum_k f_k$, where f_k only depends on the data of node k , which is not satisfied in various settings and especially in the case of spatial filtering. Instead, the common attribute between different spatial filtering problems is that the objective depends on the optimization variable X solely through the fusion/filtering expression $X^T \mathbf{y} = \sum_k X_k^T \mathbf{y}_k$, where \mathbf{y}_k corresponds to the signal measured at node k , while X_k is the block of X filtering node k 's signal. An illustrative example of the difference between the setting of our problems of interest and the one of existing distributed signal processing algorithms is given in Figure 1.

We propose the distributed adaptive signal fusion (DASF) algorithmic framework for signal fusion and spatial filtering problems in a distributed context. The main result is a generic iterative algorithm which reduces the energy and communication requirements in the WSN by only allowing the nodes of the network to communicate fused (and hence compressed) signals between each other. When spreading out the iterations over time (i.e., over different data batches), the algorithm becomes adaptive to small changes in the statistics of the observed signals and can therefore be used in tracking applications as well. We show that the algorithm converges to the optimal filter that corresponds to the solution of the centralized filter design problem. This generic algorithm covers a wide span of well-known spatial filter design principles as special cases, includ-

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 802895). The authors also acknowledge the financial support of the FWO (Research Foundation Flanders) for project G.0A49.18N, and the Flemish Government under the "Onderzoeksprogramma Artificial Intelligence (AI) Vlaanderen" programme.

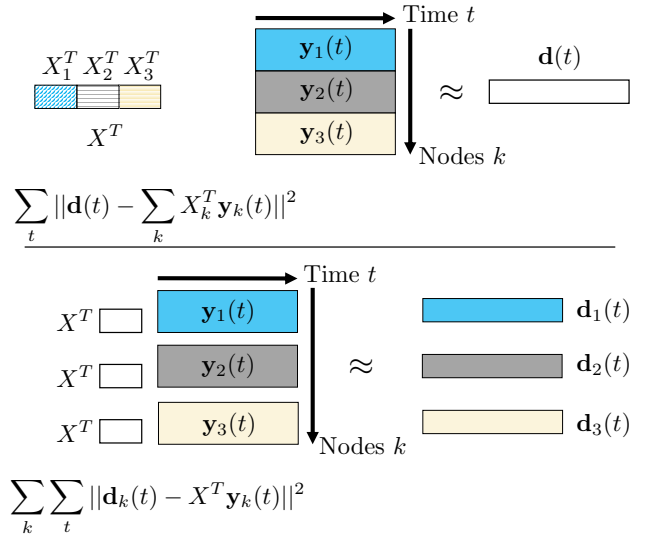


Fig. 1. Comparison of the DASF framework setting for a 3-node network (top) and the traditional consensus-type setting with separable objectives (bottom) with corresponding example objective functions for the case of least squares estimation.

ing principal component analysis (PCA), minimum variance beamforming, least squares regression, multi-channel Wiener filtering, canonical correlation analysis (CCA), generalized eigenvectors, trace ratio optimization, and more. The DASF framework covers several existing distributed algorithms for such problems such as for linearly constrained minimum variance beamforming [4] or PCA [5].

REFERENCES

- [1] J. Chen and A. H. Sayed, "Diffusion adaptation strategies for distributed optimization and learning over networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 8, pp. 4289–4305, 2012.
- [2] D. P. Bertsekas, "A new class of incremental gradient methods for least squares problems," *SIAM Journal on Optimization*, vol. 7, no. 4, pp. 913–926, 1997.
- [3] R. Olfati-Saber and J. S. Shamma, "Consensus filters for sensor networks and distributed sensor fusion," in *Proceedings of the 44th IEEE Conference on Decision and Control*. IEEE, 2005, pp. 6698–6703.
- [4] A. Bertrand and M. Moonen, "Distributed LCMV beamforming in a wireless sensor network with single-channel per-node signal transmission," *IEEE Transactions on Signal Processing*, vol. 61, no. 13, pp. 3447–3459, 2013.
- [5] —, "Distributed adaptive estimation of covariance matrix eigenvectors in wireless sensor networks with application to distributed PCA," *Signal Processing*, vol. 104, pp. 120–135, 2014.

Compressed Sensing in Wireless Acoustic Sensor Networks

Chesney Buyle, Bert Cox, Tuur Baele, Laura Monteyne and Lieven De Strycker
KU Leuven, WaveCore, Department of Electrical Engineering (ESAT), Ghent Technology Campus
 Ghent, Belgium
 first.lastname@kuleuven.be

Abstract—In this paper, we compare several compressed sensing reconstruction algorithms on acoustic data for potential implementation on Wireless Acoustic Sensor Network (WASN) nodes with limited energy budget. The energy consumption of four data driven energy conservation methods are tested on a RISC microprocessor. Our results demonstrate that the CSRec approach maintains high accuracy while the processing time is low, that local compressed sensing is possible but currently not feasible on WASN nodes and that one time random sampling is three times more energy efficient than other convenient methods.

Index Terms—Acoustic Monitoring, Compressed Sensing, Low-Power Electronics, Microcontrollers, System Testing

I. INTRODUCTION

The rise of compact micro electromechanical system (MEMS) microphones, high power budgets, large local data storage and efficient processing enables remote, low-power audio acquisition. A large number of Wireless Acoustic Sensor Networks (WASNs) have been proposed in the last decades, all with their own, application dependent microphone and network topology. These applications range from acoustic source localization [1], to automatic recognition of environmental sound events [2] and objective noise nuisance monitoring [3]. Neglecting power consumption in WASNs restricts the remote monitoring to short events or limits the amount of mounting locations to those with access to the power grid. To overcome the issues of fixed sensor networks, a long device autonomy and low sensor cost are of utmost importance [4]. In WASNs, the focus lies on data driven energy conservation schemes as acoustic sensing and processing consume significantly less than communication operations [5].

A promising resolution to this problem is Compressed Sensing (CS). CS enables improved data compression of linear, non-adaptive measurements, with a number of measurements much lower than the number of samples by the classic theorem of Shannon-Nyquist. In the last decade, intensive research permitted a wide variety of applications with well-known examples such as the single-pixel camera [6] and the improved acquisition time of magnetic resonance imaging [7]. The applicability of CS to audio signals can be found in [8], [9], [10]. [11], [12] show the universality and lack of complexity on the sensor

side in a multi-sensor system, both for non-sparse and sparse audio signals. In this paper, we proceed on this previous research and implement several CS techniques on energy-efficient RISC microprocessors. The scientific contribution of this study is twofold. First, it constitutes a comparison on speed, processor intensity and accuracy of CS reconstruction algorithms for acoustic data. Secondly, it researches the energy consumption of four data driven energy conservation schemes at the WASN sensor side.

While the target definition has been described in Section I, the following section presents an introduction to the general CS algorithm and discusses its potential within WASN. Multiple CS algorithms are tested on accuracy, computational time and processor intensity through simulations in Section III. In Section IV, the energy consumption of four data driven energy conservation schemes is measured on a low-power RISC microprocessor. Conclusions and future work are presented in Section V.

II. METHODS

A. The CS Problem

In this section, a brief mathematical introduction is given. We refer to [6] for a more in-depth overview of the CS problem. Fig. 1 visualizes the CS problem. Nyquist rate sampling of the acoustic signal $x(t)$ results in a one dimensional discrete signal consisting of N elements: $x(n)$, $n = 1, 2, \dots, N$. Any signal in \mathbb{R}^N can be represented in terms of a basis of $N \times 1$ vectors: ψ_i , $i = 1, \dots, N$. Transformation to a certain domain is done using an $N \times N$ transformation matrix $\Psi = [\psi_1 \ \psi_2 \ \dots \ \psi_N]$:

$$\mathbf{x} = \Psi \mathbf{s} \quad (1)$$

with \mathbf{s} an $N \times 1$ vector that in the ψ -space has the same representation of the signal \mathbf{x} .

Currently, a full N -sample signal \mathbf{x} is still required, the complete set of transform coefficients s_i needs to be computed and the K largest coefficients needs to be located and encoded. Compressed sensing addresses this sample-then-compress framework by directly acquiring a compressed signal representation. The $M \times N$ measurement matrix Φ reduces the amount of samples to $M \ll N$. Substituting $\mathbf{x} = \Psi \mathbf{s}$ in Eq. 1 gives:

$$\mathbf{y} = \Phi \mathbf{x} = \Phi \Psi \mathbf{s} = \Theta \mathbf{s} \quad (2)$$

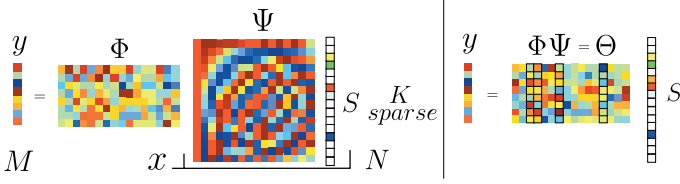


Fig. 1: The CS problem visualized with measured signal \mathbf{y} of length M , measurement matrix Φ , transformation matrix Ψ , K -sparse signal \mathbf{s} and original signal \mathbf{x} of length N (left) and with the reconstruction matrix Θ (right) [6].

where $\Theta = \Phi\Psi$ is an $M \times N$ matrix, called the reconstruction matrix. Three conditions need to be met for reconstruction of \mathbf{x} with acceptable accuracy and less samples than imposed by the Shannon-Nyquist theorem.

The signal needs to be sparse. A signal is K -sparse if it is a combination of only K basis vectors. K of the N coefficients of \mathbf{s} are nonzero. For the problem to be solvable, $M \geq K$ is required.

Φ needs to satisfy the restricted isometry property (RIP) [7].

Incoherence requires the rows of Φ to not be sparsely represented by the columns of Φ and vice versa.

Both the RIP and incoherence requirement can be achieved with high probability by selecting Φ as a random Gaussian matrix [6].

B. CS in WASNs

The WASN topology depicted in Fig. 2 consists of two sides. Low-power, low-cost acoustic sensor nodes are deployed across the area of interest. The captured data is transmitted to a central gateway. Data driven energy conservation schemes perform local processing before energy-expensive data transmission. On the other hand, complex algorithms can increase the processing time, keeping the sensor nodes awake for too long. The straightforward implementation of CS at the sensor side makes it an attractive data compression scheme, finding a balance between the paradoxical resolutions. Fig. 3 shows the CS standard acquisition model for implementation at the sensor side. The reconstruction model is implemented on the gateway side. The potential energy gain is researched by comparing the total energy consumption at the sensor side for four cases:

- 1) **Transfer all data.** This is the worst case scenario in terms of data transmission related energy consumption.
- 2) **CS with true random measurement matrix.** Out of the Nyquist sampled input data, M values are randomly selected, resulting in the measurement data \mathbf{y} of length M . The random matrix Φ is fixed at initialization and known at the sensor and gateway side. For correct reconstruction, both the value and indices of M are transmitted to the gateway side, resulting in a data transmission of $2M$ data elements.

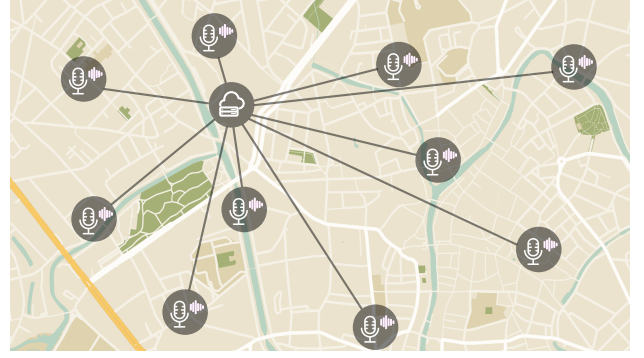


Fig. 2: Wireless Acoustic Sensor Network as a star topology with a central gateway and low-power, low-cost acoustic sensor nodes.

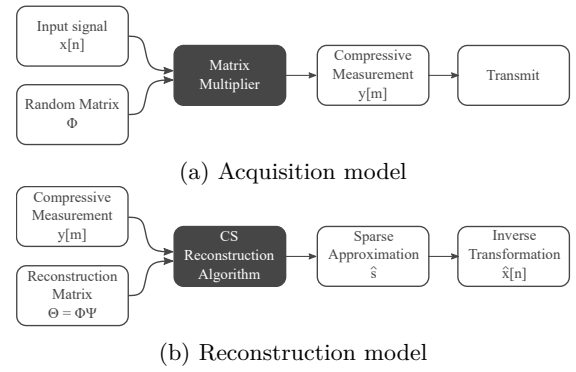


Fig. 3: General CS acquisition and reconstruction model.

- 3) **CS with one-time random measurement matrix.** The M indices are one-time randomly sampled to bypass energy demanding implementations of true random sampling in hardware or software. These indices are shared between the two entities at initialization and used at every sample event. The transmitting data elements are reduced to M .
- 4) **Local reconstruction.** Sending the sparse vector \mathbf{s} and the related indices reduces the data elements to $2K$. In this case, not only the acquisition is performed on the sensor, but reconstruction as well, i.e. all matrices multiplications for reconstruction are performed on every sensor node locally. At the central gateway, only an inverse transformation is performed to retrieve the reconstructed input signal.

Despite the substantial sample reduction to be obtained through compressive measurements, we expect the *Local reconstruction* approach to be less energy-efficient due to the large number of matrix operations that need to be performed on the RISC processor during reconstruction. Still, energy consumption measurements will provide more insights into the applicability of CS in battery-powered WASN networks.

C. Reconstruction Algorithms

From CS-measurements, the sparse estimation of the original input signal can be obtained through CS reconstruction algorithms. The research driving factors in this area are the ability to recover the original signal from a minimal amount of measurements, noise robustness, speed, complexity, performance guarantees, etc. [13]. In [14], six CS reconstruction approaches are classified: the convex optimization, Greedy, thresholding, combinatorial, non-convex optimization and Bayesian approach. This paper does not consider the implementation of the combinatorial approach as it requires noiseless and specific patterns in the measurements. The remaining five approaches can be split up in two groups. All are based on optimization problems except for the Bayesian method, which is based on probabilities. Table I gives an overview of the considered CS algorithms, as well as the corresponding approach and complexity of each algorithm.

Various criteria assess the relevance of the sparse recovery algorithms. For the audio application in this paper, we considered three:

- 1) **Accuracy:** The accuracy of the algorithm is measured by the resemblance of the reconstructed signal with the original signal.
- 2) **Speed:** We consider the computational time it takes to estimate $\hat{\mathbf{s}}$ from the measurements \mathbf{y} using reconstruction matrix \mathbf{A} .
- 3) **Processor Usage:** In combination with the speed criterion, processor usage enables us to compare the complexity of the algorithms. Parallel processing can increase the speed but at a higher processing cost.

TABLE I: Overview of the CS algorithms and the corresponding approach [14]

Algorithm	CS Approach	Complexity
L1Magic	Convex Optimization	$O m^2 n^3$
GPSR_Basic	Convex Optimization	$O m^2 n^3$
CSRec_SP	Greedy (parallel)	$O mn.iter$
MFOCUSS	Non-Convex Optimization	$O m^2 n^3$
MSBL	Bayesian	$O m^2 n$
TwIST	Thresholding	$O mn.iter$
FPC_AS	Convex Optimization	$O m^2 n^3$

III. COMPRESSED SENSING SIMULATION COMPARISON

In order to find the most suitable CS algorithm for implementation on an energy-efficient microcontroller, comparative tests on the aforementioned four parameters are conducted in a MATLAB environment.

A. Test Environment

The similarity of the CS algorithm is determined using cross-correlation between the original and reconstructed signals. In the literature, this is also known as *Performance Guarantees*. To measure the processor intensity during sparse recovery, the *PerformanceCounter Class* [15] from the open source developer platform .NET is applied. It

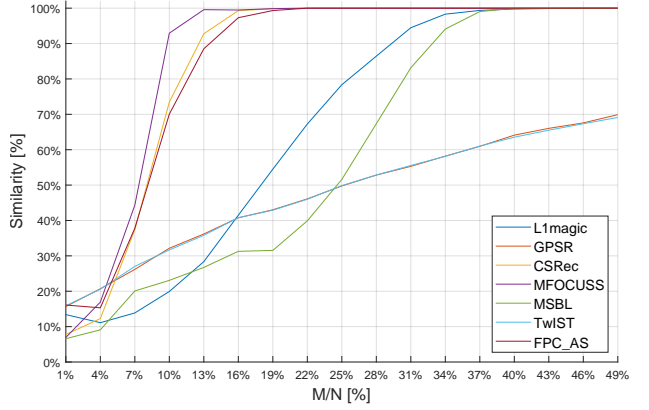


Fig. 4: Mean similarity between the original and reconstructed signal after 100 iterations in function of the used (M) to available (N) sample degree where $N = 256$ and M is variable. The tested signal is composed of 4 sine waves.

monitors the percentage intake of the MATLAB process on the processor¹. The computational time of the sparse representation $\hat{\mathbf{s}}$ from the measurements \mathbf{y} is calculated as the time interval in which the aforementioned processor intensity lies above 10%.

All measurements were conducted on a computer with an Intel(R) Core(TM) i7-4720HQ CPU @ 2.6 GHz, 8GB RAM and NVIDIA GeForce GTX 960M GPU.

B. Results

Fig. 4 shows the mean similarity between the original and reconstructed signal in function of the used sample degree $\frac{M}{N}$ where N is kept constant at 256 samples. The original input signal consists of a superposition of four sine waves with equal amplitude but random frequency in the range of 0 kHz to 20 kHz, sampled at a sample frequency of 44.1 kHz. The advantage of this test signal is that we are certain that it is sparse. In section IV, we use realistic audio signals, but the simple superposition signal is sufficient for this testing environment. The similarity shown is the mean result of a Monte Carlo simulation of 100 iterations at each sample degree $\frac{M}{N}$. The CS algorithms MFOCUSS, FPC_AS and CSRec_SP show the greatest similarity to the original signal after reconstruction, especially for lower $\frac{M}{N}$. The original signal can already be reconstructed with more than 70% similarity when only 10% of the N available samples is used, and nearly completely when the sample degree $\frac{M}{N}$ is 16%.

The mean processor intensity and processing time of various CS reconstruction algorithms are shown in Table II. The mean values are the result of a Monte Carlo simulation of 100 iterations. The test signal \mathbf{x} consists of a superposition of 16 sine waves with equal amplitude but random frequency in the range of 0 kHz to 20 kHz. The multiplication of the mean processor intensity and processing time can be interpreted as a measure for the

¹This also includes the overhead of the MATLAB program on top of the algorithm execution.

TABLE II: Comparison of reconstruction algorithms

Algorithm	Acc. [%]	Time [ms]	Proc. Int. [%]
L1magic	60.00	130	33.45
GPSR_Basic	49.95	31	31.75
CSRec_SP	88.62	113	19.31
MFOCUSS	95.48	1761	31.89
MSBL	38.88	45054	28.03
TwIST	50.00	19	36.18
FPC_AS	90.25	491	40.20

required energy consumption of the CS algorithm. A CS algorithm might take up a high amount of processor time but could require only a fraction of computation time. TwIST exhibits the smallest multiplication result, followed by GPSR_Basic and CSRec_SP with respectively 1.6 and 3.4 times the multiplication result relative to TwIST.

In conclusion, the CS_Rec algorithm shows both a good similarity to the original after reconstruction at low sample degree $\frac{M}{N}$ as well as a low processor intensity in function of the computation time. Hence, the CS_Rec algorithm shows the best performance properties for implementation on the energy-efficient microcontroller.

IV. EMBEDDED IMPLEMENTATION

The energy consumption of the four data driven energy conservation schemes presented in Section II-B is investigated at the WASN sensor side through calculations and practical measurements. A Vesper VM1010 MEMS microphone and non-inverting amplifier circuit are connected to the analog-to-digital converter of a Pearl Gecko microcontroller. This microcontroller is equipped with a 32-bit ARM Cortex M4 microprocessor and features an on-board floating-point processor and true random number generator (TRNG). The ADC sample rate is set to 44.1 kHz and a 1s audio signal is used in each of the following scenarios. Note that the implementation is considered for a single sensor node. Increased energy consumption due to for example packet loss are not considered in this paper. The energy measurements of the four data driven energy conservation are carried out as follows:

- 1) **Transfer all data:** the ADC fills a buffer of 44100 samples through Direct Memory Access (DMA). The entire sample buffer is then transmitted over RF.
- 2) **CS with true random measurement matrix:** after the buffer is filled by the ADC, a fourth of the 44100 available samples is randomly selected. The on-board TRNG is used to generate the random indices. The selected samples are then placed in a new data buffer and transmitted over RF together with their corresponding indices. A CS algorithm can be executed at the gateway side to reconstruct the original signal.
- 3) **CS with one-time random measurement matrix:** at initialization, the random indices are generated only once and shared with the gateway side. After sampling, the same indices are used recurrently to select one fourth of the 44100 available ADC

TABLE III: Energy consumption of the four data driven energy conservation schemes for each level of the WASN operation.

Energy consumption (mJ)				
	Sensing	Computing	RF	Total
All	9.81	0	65.54	75.35
Random	12.69	0	24.52	37.21
One-time random	10.71	0	16.35	27.06
Local	10.82	2031	18.39	2060.21

samples. Again, the extracted samples are placed in a new data buffer and transmitted over RF. The corresponding indices do not have to be transferred since they remain constant at all times and are known at the gateway side. Hence, for this scenario, the random index generation process is not included in the energy measurement. A CS algorithm can be executed at the gateway side to reconstruct \mathbf{x} .

- 4) **Local reconstruction:** CS reconstruction is performed locally on the Pearl Gecko microcontroller. However, the entire ADC buffer cannot be processed at once since RAM memory is limited to 256 kB. Consequently, the buffer is divided into 256 frames of $N = 160$ samples. From each frame, $M = 40$ samples are randomly selected based on a one-time random measurement matrix, which is random for each frame. Next, CS_Rec reconstruction is performed on each frame using the M random samples. The resulting $K = 10$ most significant coefficients per frame and corresponding indices are saved in a new data buffer and ultimately sent over RF. For the energy measurements, only the first 25 frames are estimated with CS_Rec. The energy consumption corresponding to the reconstruction of all frames is obtained through extrapolation.

Power measurements are performed through the Pearl Gecko's energy profiler available in Simplicity Studio. The results are summarized in Table III and are provided for each level of the WASN operation, i.e. sensing, computing and RF transmission. The energy values for RF transmission are calculated based on the technical datasheet of a TI CC1310 ultra-low power wireless MCU with sub-GHz RF transceiver [16].

In the first three scenarios, the differences in total energy consumption are mainly caused by RF transmission. The CS scenario with one-time random measurement matrix shows the lowest energy consumption. Since only one fourth of the samples need to be transferred and the corresponding indices are already known at both sides of the communication, a reduction of 65 % with respect to transfer-all-data scenario can be stated. In contrast to the one-time measurement matrix scenario, random sample indices are calculated in the random measurement case. From comparison between the sensing energy consumption follows that this random indices calculation only entails a small increase in the total energy consumption. Conse-

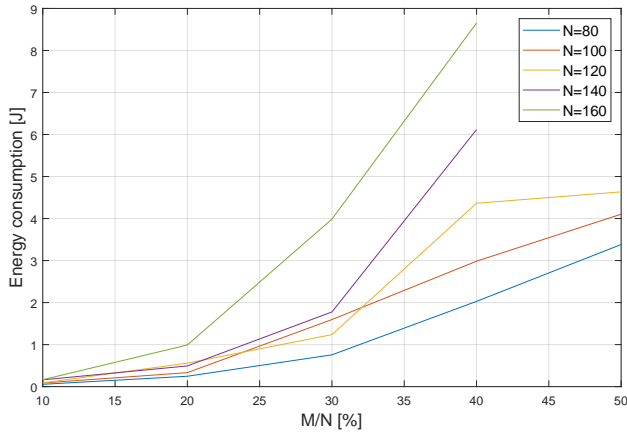


Fig. 5: Measured energy consumption of the CS_Rec computation on the Pearl Gecko microcontroller for several sample degrees $\frac{M}{N}$ and different frame lengths N . CS_Rec is applied to a 1 s male voice audio signal.

quently, 80% of the total energy increase (10 mJ) follows from additional RF transmission of the indices.

When CS_Rec reconstruction is performed locally, the total energy consumption is found to be two orders of magnitude higher than all other cases. Although the CS_Rec algorithm greatly reduces the elements to $2K$ per frame, RF transmission still takes up about the same energy budget as in the cases with random and one-time random measurement matrices. This can be explained by the fact that each significant component in K is represented by a complex single floating-point number, which takes up 8 bytes in memory while a single ADC sample is saved as an unsigned 2-byte number. This completely neutralizes the energy gain by reducing the $M = 40$ random samples to the $K = 10$ most significant components after reconstruction. From Table III it follows that the computation of CS_rec is responsible for the huge increase in total energy consumption. However, this only shows the case for one specific set of N , M and K .

A more in-depth study into the energy consumption of the CS_Rec computation on the Pearl Gecko microcontroller is shown in Fig. 5. The same 1 s male voice audio signal is split into frames of different sample amount N . For each case of frame length N , the energy consumption is measured at fixed sample degrees $\frac{M}{N} = 10, 20, 30, 40, 50$ %, where M is again the number of randomly selected samples from N . The number of significant components K taken after estimation is fixed at one fourth of M , and is rounded up when this fraction does not result in an integer. The energy consumption of the CS_Rec computation is measured for the first 25 frames and is extrapolated to a total of $44100/N$ frames.

The results in Fig. 5 show that the measured energy consumption remains similar for sample degrees $\frac{M}{N}$ more or less up to 30% irrespective of frame length N , except for $N = 160$. For higher sample degrees $\frac{M}{N}$, the energy consumption increases significantly for larger frame lengths

N . In this case, a small frame length N helps to keep the energy consumption as low as possible. However, the lower N , the more frames that need to be reconstructed and concatenated to approximate \mathbf{x} . Hence, more spectral leakage and thus noise will be introduced in the reconstructed signal. Overall, the energy consumption of the CS_Rec computation remains below 1 J for sample degrees $\frac{M}{N} = 20$ % irrespective of N . However, this still requires a significantly larger energy budget compared to the other three data driven energy conservation schemes.

V. CONCLUSIONS

In this research we compared different CS reconstruction algorithms for RISC implementation. We show that the CSRec reconstruction algorithm meets the quality requirements for embedded implementation, namely a high accuracy and low processing time. Practical measurements show the possibility of implementing this algorithm on a 32-bit ARM Cortex M4 microprocessor. But even for small acoustic data sets, the energy consumption of this method is 30 times higher than conventional methods due to the high local processing time and necessary power.

A second comparative study shows that the most suitable data driven energy conservation method with CS implementation on the local WASN sensor node is the one-time random sampling method. It is shown that this method is three times more energy efficient than the conventional transmit-all-data method as a result of the smaller transmit data size. Due to the limited memory on the microprocessor, the experimental results reported here are only applicable for short audio signals (< 1 s). For actual application in existing WASN, a more detailed investigation should reveal the possibilities of this method on longer audio snippets. To the full potential of local CS, a more extended research should be performed on both the local reconstruction optimization to decrease the spectral leakage and on newer, lesser known CS algorithms. In addition, this work only considered the data acquisition and transmission for a single sensor-gateway pair. Future work will exploit the spatial dimension of WSNs and focus on signal correlations between multiple sensor nodes.

REFERENCES

- [1] B. Thoen, "Indoor localization in energy constrained wireless acoustic sensor networks," Ph.D. dissertation, KU Leuven, Gebroeders De Smetstraat 1, 9000 Gent, 12 2019.
- [2] A. J. Eronen, V. T. Peltonen, J. T. Tuomi, A. P. Klapuri, S. Fagerlund, T. Sorsa, G. Lorho, and J. Huopaniemi, "Audio-based context recognition," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 14, no. 1, pp. 321–329, 2006.
- [3] J. Segura Garcia, S. Felici-Castell, J. Perez-Solano, M. Cobos, and J. M. Navarro, "Low-cost alternatives for urban noise nuisance monitoring using wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 836–844, 09 2014.
- [4] C. Buyle, B. Thoen, B. Cox, M. Alleman, S. Wielandt, and L. De Strycker, "Ultra-low-power smart sensing platform for urban sound event monitoring," *SITB2019*, vol. 30, pp. 28–33, 2019.

- [5] C. Alippi, G. Anastasi, M. Di Francesco, and M. Roveri, "Energy management in wireless sensor networks with energy-hungry sensors," *IEEE Instrumentation and Measurement Magazine*, vol. 12, no. 2, pp. 16–23, Apr. 2009.
- [6] R. G. Baraniuk, "Compressive sensing [lecture notes]," *IEEE Signal Processing Magazine*, vol. 24, no. 4, pp. 118–121, 2007.
- [7] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.
- [8] M. Fakhr, "Robust watermarking using compressed sensing framework with application to mp3 audio," *The International Journal of Multimedia and Its Applications*, vol. 4, 12 2012.
- [9] M. G. Christensen, J. Østergaard, and S. H. Jensen, "On compressed sensing and its application to speech and audio signals," in *Asilomar Conf. on Signals, Systems and Computers*, vol. 43, 2009, pp. 356–360.
- [10] S. Yu, R. Wang, W. Wan, L. Du, and X. Yu, "Compressed sensing in audio signals and its reconstruction algorithm," in *2012 International Conference on Audio, Language and Image Proces.*, 2012, pp. 947–952.
- [11] A. Griffin and P. Tsakalides, "Compressed sensing of audio signals using multiple sensors," in *European Signal Processing Conference*, vol. 16, 2008, pp. 1–5.
- [12] R. Rana, C. T. Chou, S. Kanhere, N. Bulusu, and W. Hu, "Ear-phone: An end-to-end participatory urban noise mapping system," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 01 2010, pp. 105–116.
- [13] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. Birkhäuser Basel, 2013.
- [14] M. Rani, S. B. Dhok, and R. B. Deshmukh, "A systematic review of compressive sensing: Concepts, implementations and applications," *IEEE Access*, vol. 6, pp. 4875–4894, 2018.
- [15] "Performance counter class (system.diagnostics)," <https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.performancecounter?view=dotnet-plat-ext-5.0>, accessed: 2020-11-09.
- [16] *SimpleLink Sub-1 GHz CC1310 wireless MCU LaunchPad development kit*, Texas Instruments, 2018, rev. A.

Convergence of Stochastic PDMM

Sebastian Jordan
Delft University of Technology
Delft, The Netherlands
s.o.jordan@student.tudelft.nl

Richard Heusdens
Netherlands Defence Academy,
Delft University of Technology
Delft, The Netherlands
r.heusdens@{mindef.nl,tudelft.nl}

I. ABSTRACT

In this work, we analyse a stochastic version of the primal-dual method of multipliers (PDMM), which is a promising algorithm in the field of distributed optimisation. So far, its convergence has been proven for synchronous implementations of the algorithm [1], [2]. Simulations have shown that PDMM also converges if it is implemented asynchronously, having the advantage that there is no need for clock synchronisation between the nodes in a distributed network. Furthermore, a broadcast implementation of asynchronous PDMM can be derived, instead of the usual unicast implementation. This broadcast implementation comes with a number of benefits. For example, it is a lot simpler to implement and requires less transmissions per iteration. Broadcast PDMM also lends itself to an efficient privacy preservation method that was introduced in [3].

In this paper, we analyse the convergence properties of different implementations of PDMM. In order to perform a rigorous analysis of a number of empirical findings, first a general stochastic version of PDMM is introduced. This general definition encompasses both asynchronous updating and transmission losses. Next, a formal proof is derived for the convergence of stochastic PDMM. This proof follows similar steps to the ones taken in [4] and builds upon a previous unfinished proof from [5]. The convergence proof makes use of the fact that the sequence of auxiliary errors of PDMM forms a non-negative supermartingale. By using Markov's inequality and Borel Cantelli's lemma, stochastic PDMM can be shown to converge almost surely to a bounded random variable that is supported by the set of fixed points of the standard PDMM operator. These points correspond to primal optimal points of the optimisation problem in question. The only assumption required for convergence is the fact that all edge variables must have a non-zero probability of updating.

In the case of unicast PDMM, asynchronous PDMM and PDMM with transmission losses can both be seen as specific instances of stochastic PDMM and thus also converge almost surely. Broadcast PDMM, however, requires each auxiliary variable to be stored at two nodes. In the case of transmission losses, a mismatch occurs between the two values stored for the same variable. This mismatch causes the algorithm to reach a fixed point that does not correspond to a primal optimal solution. As long as the two versions of the same variable are never mismatched, broadcast PDMM is equivalent to unicast

PDMM. This why asynchronous broadcast PDMM does converge. With unicast PDMM, each auxiliary variable is only needed at one node, which makes unicast PDMM inherently robust against transmission loss and thus favourable when compared to broadcast PDMM. In Fig. 1 simulation results are given to show the difference in convergence behaviour between unicast and broadcast PDMM in the presence of transmission losses.

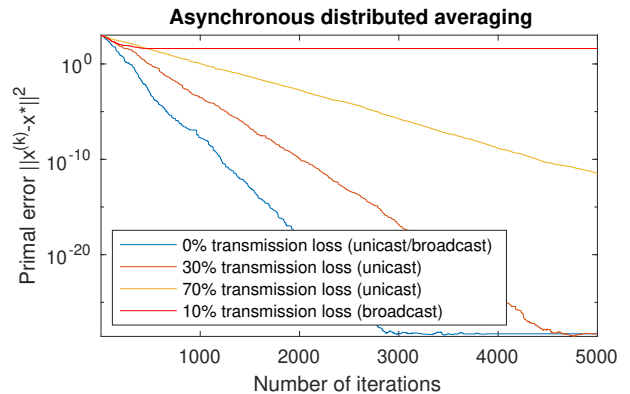


Fig. 1. Experimental convergence results for distributed averaging in the presence of transmission losses. Simulations are performed for a random geometric network with 30 nodes and asynchronous PDMM is used as optimisation algorithm.

REFERENCES

- [1] T. W. Sherson, R. Heusdens, and W. B. Kleijn, "Derivation and Analysis of the Primal-Dual Method of Multipliers Based on Monotone Operator Theory," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 2, pp. 334–347, Jun. 2019.
- [2] G. Zhang and R. Heusdens, "Distributed Optimization Using the Primal-Dual Method of Multipliers," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 173–187, Mar. 2018.
- [3] Q. Li, R. Heusdens, and M. G. Christensen, "Privacy-Preserving Distributed Optimization via Subspace Perturbation: A General Framework," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5983–5996, 2020.
- [4] P. Bianchi, W. Hachem, and F. Iutzeler, "A Coordinate Descent Primal-Dual Algorithm and Application to Distributed Asynchronous Optimization," *IEEE Transactions on Automatic Control*, vol. 61, no. 10, pp. 2947–2957, Oct. 2016.
- [5] T. Sherson, R. Heusdens, and W. B. Kleijn, "Derivation and Analysis of the Primal-Dual Method of Multipliers Based on Monotone Operator Theory," *arXiv:1706.02654 [math]*, Nov. 2017, arXiv: 1706.02654.

Spatial Diversity Effects for Multi-node Ultrasonic Indoor Positioning

Daan Delabie, Liesbet Van der Perre, Lieven De Strycker

*KU Leuven, WaveCore, Department of Electrical Engineering (ESAT), Ghent Technology Campus
Ghent, Belgium
daan.delabie@kuleuven.be*

Abstract

Highly accurate and reliable indoor 3D positioning of low power or even energy-neutral devices is becoming increasingly important in new Internet-of-Things (IoT) related applications for the future digital society. Acoustic or ultrasonic based positioning systems are an interesting candidate since these signals exhibit a relatively low propagation speed (343 m/s) allowing centimeter accuracy to be achieved based on Time of Flight (ToF) measurements without high-speed and hence power hungry electronics [1]. Current Indoor Positioning Systems (IPSs) have good accuracy characteristics, but show a large variance and many outliers while there is not enough reliability across the entire 3D space [2]. By advancing scattered arrays to increase the spatial diversity, reverberation can be overcome to reliably and accurately locate many devices and moving objects [3]. Within this paper, the influence of the number, selection and position of Micro-Electro-Mechanical-System (MEMS) microphone based anchor nodes is investigated in a setup where a movable speaker, serving as mobile node, emits an ultrasonic chirp signal. Pulse compression between the original and received chirp combined with a peak prominence algorithm provides ToF, and therefore ranging information to support indoor localisation [4]. The distributed effect on the accuracy and reliability is tested via an Image Source Model (ISM) shoebox simulation and could be expanded to a real-life measurement in an acoustically challenging testbed called Techtile [5]. A Data Acquisition (DAQ) system is available in the testbed, ensuring that synchronisation for, in this case Time Difference of Arrival (TDoA) measurements, is inherently present. Besides using traditional multilateration methods such as simple intersections, Chueng or Gauss-Newton, physics inspired deep learning models [6], [7] could be an option to take advantage of the difficult acoustic properties of the testbed.

REFERENCES

- [1] C. Medina *et al.*, “Ultrasound Indoor Positioning System Based On a Low-power Wireless Sensor Network Providing Sub-centimeter Accuracy,” *Sensors*, vol. 13, no. 3, pp. 3501–3526, 2013.
- [2] F. Zafari, A. Gkelias, and K. K. Leung, “A Survey of Indoor Localization Systems and Technologies,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.
- [3] S. Wielandt *et al.*, “Indoor Multipath Assisted Angle of Arrival Localization,” *Sensors*, vol. 17, no. 11, p. 2522, Nov. 2017, ISSN: 1424-8220.
- [4] B. Cox, L. van der perre, S. Wielandt, G. Ottoy, and L. De Strycker, “High precision hybrid RF and ultrasonic chirp-based ranging for low-power IoT nodes,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, p. 187, Sep. 2020.
- [5] D. Delabie, B. Cox, L. D. Strycker, and L. V. der Perre, *Techtile: a Flexible Testbed for Distributed Acoustic Indoor Positioning and Sensing*, 2022. arXiv: 2204.06352.
- [6] A. Nessa, B. Adhikari, F. Hussain, and X. Fernando, “A Survey of Machine Learning for Indoor Positioning,” *IEEE Access*, vol. 8, pp. 214 945–214 965, Jan. 2020.
- [7] P. Roy and C. Chandreyee, “A Survey of Machine Learning Techniques for Indoor Localization and Navigation Systems,” English, *Journal of Intelligent Robotic Systems*, vol. 101, no. 3, Mar. 2021.

Aircraft Trajectory Prediction using ADS-B Data

Xuzhou Yang
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
Email: x.yang-20@student.tudelft.nl

Junzi Sun
Faculty of Aerospace Engineering
Delft University of Technology
Delft, The Netherlands
Email: j.sun-1@tudelft.nl

Raj Thilak Rajan
Faculty of EEMCS
Delft University of Technology
Delft, The Netherlands
Email: r.t.rajan@tudelft.nl

Abstract—Automatic Dependent Surveillance - Broadcast (ADS-B) is a surveillance technology that is used extensively in Air Traffic Control (ATC) applications. Aircraft equipped with ADS-B transponders actively broadcast navigation information such as position, altitude, and velocity, and thus ATC is able to track aircraft continuously, even in regions not covered by traditional radars. However, raw ADS-B messages are typically contaminated with noise, which is typically mitigated using model-based tracking methods to predict the trajectories. In this work, we propose and evaluate the performance of several filtering strategies for trajectory prediction on an existing open source *TrajAir* aircraft data set and our own data set i.e., collected by Delft university of technology (TUD). In our evaluation, we observe the standard Kalman filter cannot accurately track the aircraft trajectory, especially for sharply maneuvering targets. A fading-memory filter tracks maneuvering targets but introduces delay in estimates, and requires a trade-off between responsiveness and smoothness by target-specific parameter tuning. The Kalman filter with augmented process noise also involves similar trade-off and parameter tuning. Finally, the particle filter performs the best during target maneuvers but admits more noise during steady-state and increases computational cost. In this paper, we present various filtering techniques, and study the performance of these algorithms on the *TrajAir* and *TUD* aircraft data sets.

Index Terms—ADS-B, Kalman filter, Particle filter.

I. INTRODUCTION

Automatic Dependent Surveillance - Broadcast (ADS-B) is an surveillance technology that is used extensively in Air Traffic Control (ATC) applications. Aircraft broadcast ADS-B messages periodically with on-board Mode-S transponders, which include navigational information such as surface/airborne position, airborne velocity, call sign, operational status, etc. ADS-B enables ATC ground stations to track aircraft continuously in regions that are not covered by traditional radars, as its coverage can be greatly extended by ground-based or space-based ADS-B receivers. It is considered to be a key component of the future air transportation system and is mandated both by EUROCONTROL [3] in Europe and FAA [4] in the U.S. since 2020.

Prior to the introduction of ADS-B, ATC applications heavily relied on the primary surveillance radar (PSR) and the secondary surveillance radar (SSR). PSR provides slant distance as well as aircraft's azimuth information with respect

to the radar location, while SSR provides aircraft's altitude and identity. However, inherent limitations of PSR and SSR technology hinder further improvement in accuracy and coverage. ADS-B is thus introduced to enhance situational awareness for ATC controllers and pilots.

In this paper, we evaluate several model-based tracking methods on aircraft ADS-B data set. Section II explains the information provided by the ADS-B messages and data pre-processing techniques used to extract the relevant data. In Section III, we build theoretical foundations of our tracking methods with state space models and a Bayesian framework and introduce the standard Kalman filter under constant velocity dynamics (CV-KF). We further explore advanced filtering algorithms in Section IV, i.e., the Kalman filter with augmented noise (AP-KF), fading-memory Kalman filter (FM-KF), and the particle filter (PF) are introduced. In Section V, these methods are applied to predict aircraft trajectories, and a comparison between different methods and more comments are provided. Finally, in Section VI we summarize the results, with insights on future work.

II. ADS-B DECODING AND PRE-PROCESSING

Nowadays, most of the aircraft are equipped with an ADS-B system. It is thus easy to acquire these ADS-B signals, and thus data, using an appropriate receiver system. Furthermore, an open-source package *pyModeS*¹ [10] provides us comprehensive functionalities to decode these ADS-B messages. In this section, we briefly look at message parsing, and the pre-processing of decoded data and relevant assumptions.

A. Description of data set

In this paper, we work with two realistic ADS-B data sets. The first data set is an open source data set called the *TrajAir* dataset², contributed by the AirLab from the robotics institute at Carnegie Mellon University. The other data set is collected by the faculty of aerospace engineering (AE) at TU Delft [5], which we call the *TUD* data set.

1) *TrajAir* data set: The *TrajAir* data set contains fully decoded ADS-B messages. The data set is collected at the Pittsburgh-Butler Regional Airport. In this data set, we have

This work is partially funded by the European Leadership Joint Undertaking (ECSEL JU), under grant agreement No 876019, the ADACORSA project - "Airborne Data Collection on Resilient System Architectures."

¹<https://github.com/junzis/pyModeS>

²<https://theairlab.org/trajair/>

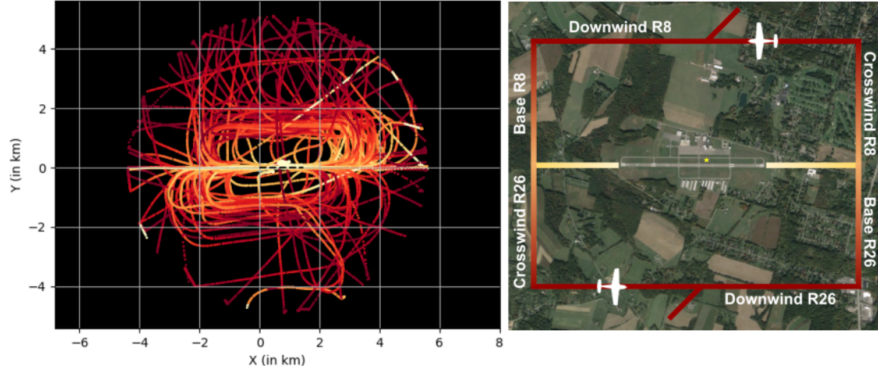


Fig. 1: *TrajAir* dataset: The left figure shows a snippet of processed aircraft trajectories and right figure demonstrates the left traffic pattern and nomenclature for the runways at the airport [2].

the information about an aircraft’s status, including timestamps, geographical coordinates, velocity readings, track angles, altitudes, and vertical rates at every valid time instance. That is to say, the alternate transmitting behaviour of ADS-B is not seen. Trajectories of landing or takeoff of a group of aircraft are visualized in Fig.1. We can clearly see the lobes for traffic patterns around this airport. The right part of this figure shows the “Left Traffic” patterns. These patterns are rectangular-shaped with left-handed turns relative to the direction of landing or takeoff. Lighter color of trajectories for lower altitude [2].

2) *TUD data set*: The *TUD* data set contains demodulated (not decoded) ADS-B signals. The data set records about 15 minutes of air traffic near the region of Delft, covering most part of the southern Holland. Every entry contains timestamp, International Civil Aviation Organization (ICAO) address, receiving power, garbling (True or False), cyclic redundancy check (CRC) sign, and the 112-bit message string. ADS-B broadcasts different types of messages alternately. For position and velocity messages, which are of particular interest in our application, the airborne transmitting frequency is 2Hz. However, the *TUD* data set provides trajectories mostly from commercial jets. To include more additional aircraft trajectories, we use the *TrajAir* data set, which also contains trajectories from light general aviation (GA) aircraft.

B. Decoding

In this section, we summarize the details of time of arrival decoding, airborne position and airborne velocity decoding from [1].

1) *Time of arrival decoding*: ADS-B is not designed to contain any time of transmit information, but both data sets timestamp received signals. So we associate aircraft positions with time of arrival instead. Assumptions are made when we replace time of transmit with the time of arrival. We assume that for a sequence of messages, the time of propagation from source to receiver is very short and approximately the same. That means: 1) the aircraft does not travel a large distance between two consecutive transmissions with reference to the receiver; 2) there is no large difference in propagation time due

to multi-path. In this paper, these two assumptions generally hold.

2) *Airborne position decoding*: A typical airborne position message contains longitude, latitude, and altitude of an aircraft. It is trivial to decode altitude but longitude and latitude are encoded in Compact Position Reporting (CPR) format. We use locally unambiguous position decoding for our own data set. Locally unambiguous position decoding [1] requires a known reference position. It should be close to the decoded position, e.g., within a range of 180 nautical miles (NM). The advantage is that from every piece of encoded messages we can decode a position. Here we choose the faculty of Aerospace Engineering building as the reference point.

3) *Airborne velocity decoding*: The airborne velocity message reports velocity decomposed in East-West, North-South and vertical directions. In the field of civil aviation, it is common to compute the track angle without considering altitude changes. It is trivial to decode the message itself. But it is worth noting that only ground speed can be used in our application. The ground speed of aircraft is the sum of the true airspeed vector and the wind velocity vector.

C. Data pre-processing and formatting

After decoding, we reorganize the data into tables of records. A record or a row in a table contains an aircraft’s two-dimensional positions and velocity, associated with a timestamp. The initial timestamp and positions are set to zeros and other timestamps and positions in this table are calculated with respect to this. A table contains consecutive records for an aircraft. A ready-for-use table of a BOEING 737-4Z9 flying over southern Holland is shown in Table I. The first available position in the data sequence is set as (0,0). Based on the assumptions in section II-B, we assign messages received within, say, one-second interval with the *same* timestamp. Similar pre-processing is applied to the *TrajAir* dataset as well, but with a finer step in time. This pre-processing technique makes sure that for each time instance both the position and velocity data are available.

1) *Two flight scenes*: We chose two typical flight scenes from each data set respectively, which we refer to as *Scene*

TABLE I: A snippet of fully decoded ADS-B data

Time(s)	icao	$P_x(\text{m})$	$P_y(\text{m})$	$V_x(\text{m/s})$	$V_y(\text{m/s})$
0	4CA8AD	0	0	175.8	-143.9
1	4CA8AD	157.6	-129.0	175.8	-143.9
1	4CA8AD	241.1	-197.4	175.8	-143.9
2	4CA8AD	334.2	-273.6	175.8	-143.9
2	4CA8AD	412.9	-338.0	175.8	-143.9
3	4CA8AD	505.3	-413.7	175.8	-143.9
3	4CA8AD	594.7	-486.9	175.8	-143.9
4	4CA8AD	704.0	-576.4	175.8	-143.9
4	4CA8AD	764.6	-626.0	175.8	-143.9
5	4CA8AD	849.8	-695.8	175.8	-143.9

1 and Scene 2 in this paper. We use X_{data} to denote raw trajectories.

- *Scene 1*: This scene contains a trajectory of an jet liner, which flew in linear motion for some time period, and then made a lazy turn. The aircraft maintains cruising speed and altitude in this period. The trajectory of the aircraft is shown in Fig.2a.
- *Scene 2*: It contains the landing trajectory of a GA aircraft. The aircraft made sharper turns and changed its velocity frequently. Compared to that in Scene 1, this trajectory exhibits more abrupt changes in states. This is shown in Fig.2a.

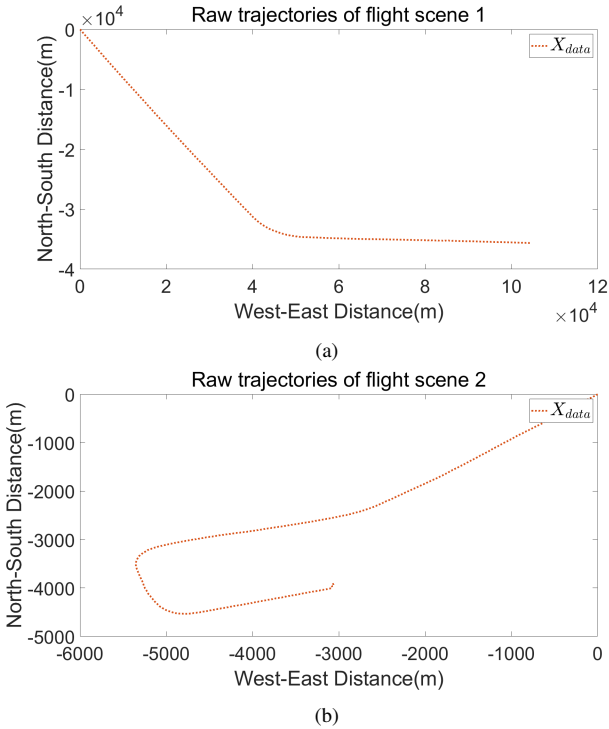


Fig. 2: Two flight scenes. Scene 1 is from the *TUD* data set and Scene 2 is from the *TrajAir* data set.

III. STATE SPACE MODEL AND KALMAN FILTER

Almost all existing tracking methods heavily rely on the models of the aircraft motion. However, in our task, the precise knowledge of aircraft dynamics is not assumed. Furthermore, it is not computationally efficient to use a very sophisticated model. Thus, we rely on simple dynamic models in this application. It is then an important problem that how we can mitigate the model mismatch caused by this oversimplification.

A. Kalman filter

The task of trajectory prediction can be considered as a state estimation problem. It requires the algorithm to retrieve signal of interest from noisy data and construct a reasonable (regarding target dynamics) trajectory from available data. If we consider a linear Gaussian state space model, then the Kalman filter (KF) is an optimal filter. Here, the process and the measurement equations are given respectively by

$$\mathbf{x}_k = \mathbf{F}\mathbf{x}_{k-1} + \mathbf{w}_{k-1} \quad (1)$$

$$\mathbf{z}_k = \mathbf{H}\mathbf{x}_k + \mathbf{v}_k \quad (2)$$

Here, the previous state \mathbf{x}_{k-1} is transformed to the current state \mathbf{x}_k by the process matrix \mathbf{F} and corrupted by process noise \mathbf{w}_{k-1} . The second equation, i.e., the measurement equation describes how the system's output \mathbf{z}_k is related to internal states through measurement matrix \mathbf{H} . In the set up of the Kalman filter, we assume the noise to be white, zero-mean Gaussian, and independent from each other, which can be represented as

$$p(\mathbf{w}) \sim \mathcal{N}(0, \mathbf{Q}) \quad (3)$$

$$p(\mathbf{v}) \sim \mathcal{N}(0, \mathbf{R}) \quad (4)$$

The Kalman filter works in a recursive manner. At each recursive step, it performs prediction and then correction, and computes a factor called Kalman gain. This factor controls the trade-off between prior knowledge and data.

We first define the initial state and posterior covariance matrix, \mathbf{x}_0 and \mathbf{P}_0 . \mathbf{x}_0 is simply set according to the first available ADS-B record in a data sequence. Practically, we fill all diagonal entries of \mathbf{P}_0 with positive values. According to [6], whether the initial values are large or small, the filter always converges.

For the prediction phase:

$$\hat{\mathbf{x}}_k^- = \mathbf{F}\hat{\mathbf{x}}_{k-1} \quad (5)$$

$$\mathbf{P}_k^- = \mathbf{F}\mathbf{P}_{k-1}\mathbf{F}^T + \mathbf{Q} \quad (6)$$

and the correction phase, we have

$$\mathbf{K}_k = \mathbf{P}_k^- \mathbf{H}^T (\mathbf{H} \mathbf{P}_k^- \mathbf{H}^T + \mathbf{R})^{-1} \quad (7)$$

$$\hat{\mathbf{x}}_k = \hat{\mathbf{x}}_k^- + \mathbf{K}_k (\mathbf{z}_k - \mathbf{H}\hat{\mathbf{x}}_k^-) \quad (8)$$

$$\mathbf{P}_k = (\mathbf{I} - \mathbf{K}_k \mathbf{H}) \mathbf{P}_k^- \quad (9)$$

Here we use $\hat{\mathbf{x}}_k^-$ to denote the predicted state at the k -th step while $\hat{\mathbf{x}}_k$ denotes the corrected state estimate at the k -th step. Similar notations are used for \mathbf{P}_k^- and \mathbf{P}_k . The matrix \mathbf{K}_k is the Kalman gain computed at the k -th step.

B. Constant-velocity dynamic model

To ensure the smooth functioning of the Kalman filter, we need to choose proper dynamic models. Commercial airliners usually maintain designated speed, heading, and altitude during en route flying. The movement can be considered as uniform linear motion. Therefore, a constant velocity (CV) model is sufficient in most cases. We consider the CV model in a two-dimensional space, with x and y representing two-dimensional positions and \dot{x} , \dot{y} two-dimensional velocities. The state vector is then defined as $\mathbf{x}_k = [x_k, y_k, \dot{x}_k, \dot{y}_k]^T$. Given recursive time step δt , the process matrix \mathbf{F} is given by

$$\mathbf{F} = \begin{bmatrix} 1 & 0 & \delta t & 0 \\ 0 & 1 & 0 & \delta t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (10)$$

Note that in this task we define a set of states whose measurements can be directly extracted from ADS-B data (i.e., positions and velocities), which is equivalent to set \mathbf{H} as an identity matrix.

C. Constant-velocity Kalman filter (CV-KF)

The constant velocity Kalman filter (CV-KF) is a Kalman filter under the assumption of constant-velocity dynamics. The pseudo code for CV-KF is presented in Algorithm 1.

Algorithm 1 The CV-KF filter

- 1: **Input:** \mathbf{x}_0 , \mathbf{P}_0 , sequence of data $\mathbf{z}_{1,k}$
 - 2: **Output:** Sequence of state estimates $\mathbf{x}_{1,k}$, posterior covariance $\mathbf{P}_{1,k}$ and Kalman gains $\mathbf{K}_{1,k}$
 - 3: Initialize \mathbf{x}_0 and \mathbf{P}_0
 - 4: **For** $t = 1$ to n **do**
 - 5: Project \mathbf{x}_{t-1} to \mathbf{x}_t^-
 - 6: Project \mathbf{P}_{t-1} to \mathbf{P}_t^-
 - 7: Compute \mathbf{K}_t
 - 8: Update \mathbf{x}_t^- to \mathbf{x}_t with \mathbf{K}_t and \mathbf{z}_t
 - 9: Update \mathbf{P}_t^- to \mathbf{P}_t with \mathbf{K}_t
 - 10: **end**
-

The CV-KF is guaranteed to give optimal estimates under the assumption of the linear model with white Gaussian noise. However, real systems do not always fulfill these assumptions, and non-linear dynamics cannot be ignored. Specifically, in our application, when an aircraft is close to the airport, it must follow certain arrival or departure procedures. The procedures may require the aircraft to make a series of turns and pass designated waypoints in order to align with the runway.

We evaluate the performance of CV-KF in the two scenes from the *TrajAir* and *TUD* datasets respectively, which was discussed in Section II-C1.

- *Scene 1:* The results are shown in Fig.3a - 3c, where X_{CV-KF} denotes the filtered trajectory by CV-KF and X_{data} the raw data points. Here, x , y are position coordinates and \dot{x} and \dot{y} velocities. From Fig.3a and Fig.3b we can observe that the filter diverges on position

estimates when the target performs a turn. Fig.3c shows that the filter fails to estimate velocity.

- *Scene 2:* The results are shown in Fig.4a - 4c, where the correction always lags the transition of states. It seems that after the filter enters a steady state, it loses the ability to track changes in the aircraft's states.

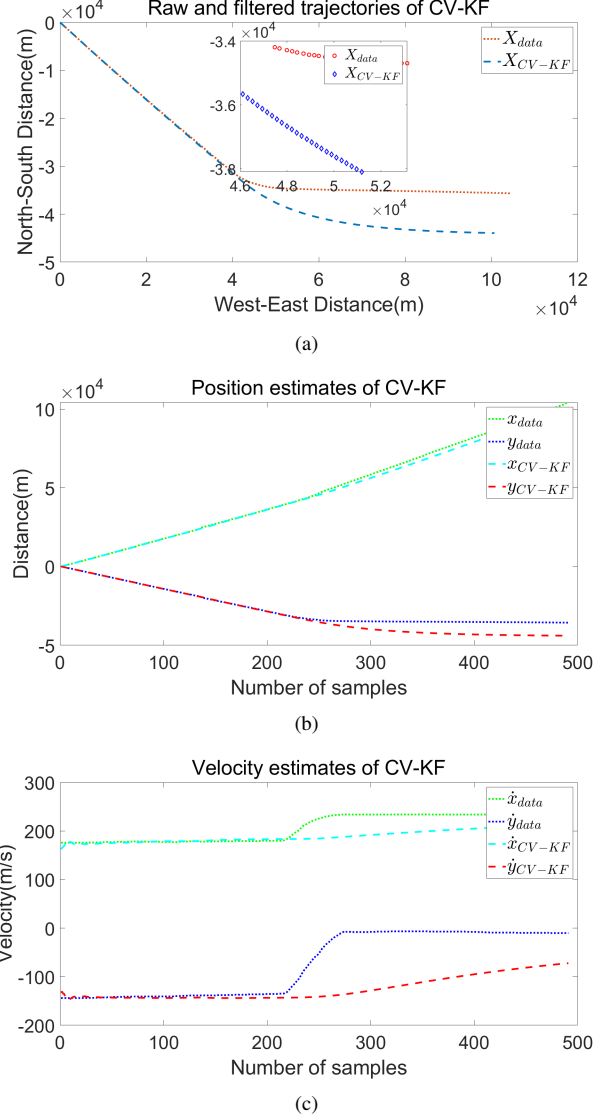


Fig. 3: *Scene 1:* Predicted trajectory, position and velocity estimates using CV-KF

The CV-KF fails mainly due to model mismatch, and thus the assumed oversimplified model fails to capture the real dynamics of maneuvering aircraft. Hence, we have to adapt our algorithm to enable accurate tracking. A good algorithm relies on both the model to capture dynamics and the filter to fuse prior knowledge and data. Traditionally, more advanced dynamical models have been proposed, however there is no silver bullet to this problem. Alternatively, we can retain the simplified CV-model but propose advanced filtering techniques

to enable more accurate tracking.

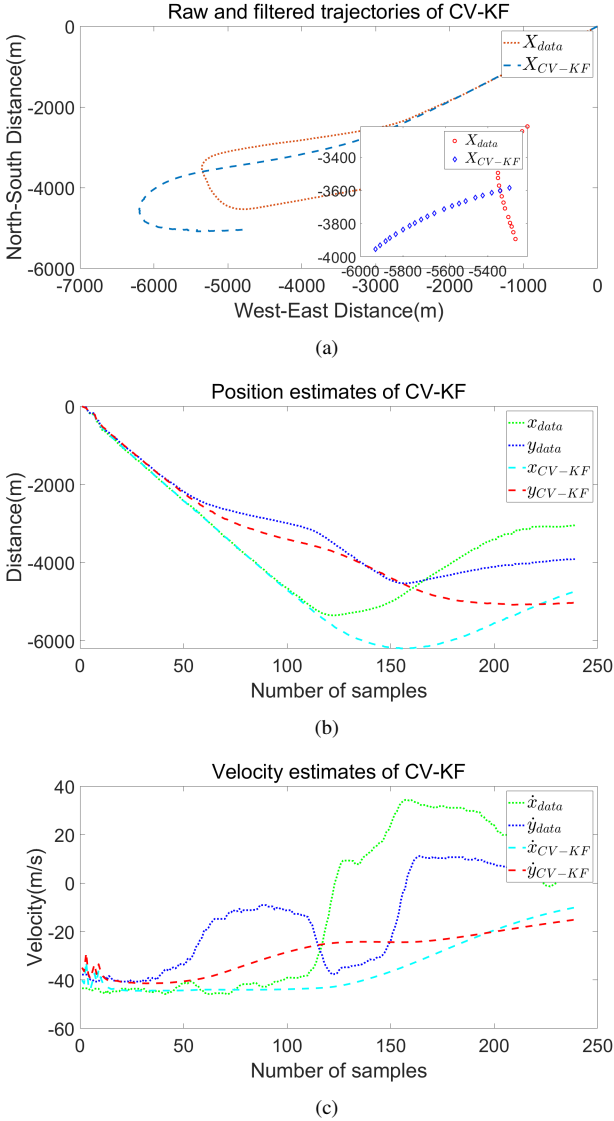


Fig. 4: Scene 2: Predicted trajectory, position and velocity estimates using CV-KF

IV. ADVANCED FILTERING ALGORITHMS

In this section we explore advanced filtering algorithms, to overcome the limitations of the CV-KF discussed in the previous section.

A. Augmented process noise Kalman filter (AP-KF)

We now introduce the Augmented process noise Kalman Filter (AP-KF). Recall that the posterior covariance matrix is computed by

$$\mathbf{P}_k^- = \mathbf{F}\mathbf{P}_{k-1}\mathbf{F}^T + \mathbf{Q} \quad (11)$$

To augmented process noise is equivalent to increase the values in diagonal entries of the \mathbf{Q} matrix. Then for each step \mathbf{P}_k^- will increase, as compared to that of the CV-KF. As mentioned

above, to remove the measurement noise as much as possible, sometimes we set \mathbf{Q} as zero. But AP-KF incorporates \mathbf{Q} to compensate for model mismatch [7]. The Kalman gain is now given by $\mathbf{K}_k = \mathbf{P}_k^- \mathbf{H}^T (\mathbf{H} \mathbf{P}_k^- \mathbf{H}^T + \mathbf{R})^{-1}$, and since \mathbf{H} is an identity matrix, and both \mathbf{P}_k^- and \mathbf{R} are diagonal matrices, the Kalman gain is reduced to

$$\begin{aligned} \mathbf{K}_k &= \mathbf{P}_k^- (\mathbf{P}_k^- + \mathbf{R})^{-1} \\ &= \begin{bmatrix} \frac{p_{k1}}{p_{k1}+r_1} & & & \\ & \frac{p_{k2}}{p_{k2}+r_2} & & \\ & & \frac{p_{k3}}{p_{k3}+r_3} & \\ & & & \frac{p_{k4}}{p_{k4}+r_4} \end{bmatrix} \end{aligned} \quad (12)$$

where p_{ki} and r_i refer to diagonal elements of \mathbf{P}_k^- and \mathbf{R} , respectively. It is then clear that every diagonal entry of \mathbf{K}_k increases as p_{ki} increases or as every diagonal entry of \mathbf{Q} increases. Thus the AP-KF increases the Kalman gain as compared to the CV-KF, giving more weights to the measurements. However, this benefit comes at the cost of admitting more measurement noise. The extreme case is that the process noise covariance is large enough such that the filter discards the prediction and simply follows the measurement, which is not desired, and hence this method requires the tuning of \mathbf{Q} .

B. Fading memory Kalman filter (FM-KF)

The fading memory Kalman filter (FM-KF) is an alternative method to augment the posterior covariance matrix. For older prediction and measurement, we aim to increase the covariance matrices by multiplying a factor greater than one, and let the factor shrink (but always greater than one) for newer predictions and measurements. Thus, the covariance matrices at are revised to be

$$\tilde{\mathbf{Q}}_k = \alpha^{K-2k+2} \mathbf{Q}_k, k \leq K \quad (13)$$

$$\tilde{\mathbf{R}}_k = \alpha^{K-2k} \mathbf{R}_k, k \leq K \quad (14)$$

where K denotes the total number of time steps in the filtering process.

After some mathematical manipulation, the final effect on posterior covariance matrix is almost identical to that of augmenting process noise [6]. The revised posterior covariance matrix is given by

$$\tilde{\mathbf{P}}_k^- = \alpha^2 \mathbf{F} \tilde{\mathbf{P}}_{k-1} \mathbf{F}^T + \mathbf{Q}_{k-1} \quad (15)$$

The implementation of a FM-KF relies on the hyper parameter α . A larger α indicates that the "memory" is shorter and the filter is more able to track changes of target's states. In our application, a larger α gives the filter more flexibility to handle maneuvers. However, in practise we have to tune α for every given target, which is a limitation.

C. Particle filter (PF)

In Section III-C, we discussed the model mismatch i.e., discrepancy between the assumed linear model and the actual nonlinear model. Moreover, precise knowledge of the sensor noise model is not assumed. We do not know the statistics of

the measurement noise, nor do we know if it is appropriate to assume the noise to be Gaussian. Furthermore, we observe that the process noise is not straightforward to model due to external factors e.g., atmospheric disturbances. Therefore, we need a filtering method that does not depend on the restrictive assumptions of Gaussian linear state space models, for example the particle Filter (PF) [12].

The particle filter is an instance of sequential importance sampling (SIS), where we are interested in a general state space model of the form

$$\mathbf{x}_k = f_k(\mathbf{x}_{k-1}, \mathbf{w}_k) \quad (16)$$

$$\mathbf{z}_k = h_k(\mathbf{x}_k, \mathbf{v}_k) \quad (17)$$

where for the k th time instance, $f_k(\cdot)$ denotes the process model, $h_k(\cdot)$ denotes the measurement model, \mathbf{w}_k indicates the process noise, and \mathbf{v}_k indicates the measurement noise. Note that a Gaussian linear model is not assumed here. Under the assumption that the Markov property holds, we have

$$p(\mathbf{x}_k | \mathbf{x}_{1,k-1}, \mathbf{z}_{1,k-1}) = p(\mathbf{x}_k | \mathbf{x}_{k-1}) \quad (18)$$

$$p(\mathbf{z}_k | \mathbf{x}_{1,k}, \mathbf{z}_{1,k-1}) = p(\mathbf{z}_k | \mathbf{x}_k) \quad (19)$$

We start with the sequential estimation of $p(\mathbf{x}_{1,k} | \mathbf{z}_{1,k})$ and the estimation of the marginal $p(\mathbf{x}_k | \mathbf{z}_{1,k})$ will be a by-product. Using (18) and (19), we can write

$$\begin{aligned} p(\mathbf{x}_{1,k} | \mathbf{z}_{1,k}) &= p(\mathbf{z}_k | \mathbf{x}_k) p(\mathbf{x}_k | \mathbf{x}_{k-1}) p(\mathbf{x}_{1,k-1} | \mathbf{z}_{1,k-1}) \\ &= \frac{p(\mathbf{x}_{1,k}, \mathbf{z}_{1,k})}{\int p(\mathbf{x}_{1,k}, \mathbf{z}_{1,k}) d\mathbf{x}_{1,k}} = \frac{p(\mathbf{x}_{1,k}, \mathbf{z}_{1,k})}{Z_k} \end{aligned} \quad (20)$$

where Z_k is the normalizing constant at the k th instant. The posterior distribution is proportional to the joint distribution in (20), and thus we approximate $p(\mathbf{x}_{1,k}, \mathbf{z}_{1,k})$ via a set of generated particles. We define the weights of particles as

$$\omega_k(\mathbf{x}_{1,k}) = \frac{p(\mathbf{x}_{1,k}, \mathbf{z}_{1,k})}{q_k(\mathbf{x}_{1,k})} \quad (21)$$

where $q_k(\cdot)$ is a proposal distribution. According to sequential importance sampling [12], the recursive relation between the current and past weights are given by

$$\omega_k(\mathbf{x}_{1,k}) = \omega_{k-1}(\mathbf{x}_{1,k-1}) \frac{p(\mathbf{z}_k | \mathbf{x}_k) p(\mathbf{x}_k | \mathbf{x}_{k-1})}{q_k(\mathbf{x}_k | \mathbf{x}_{k-1}, \mathbf{z}_{1,k})} \quad (22)$$

where we exploit (20), and we choose a proposal distribution such that

$$q_k(\mathbf{x}_k | \mathbf{x}_{1,k-1}, \mathbf{z}_{1,k}) = q(\mathbf{x}_k | \mathbf{x}_{k-1}, \mathbf{z}_k). \quad (23)$$

Finally, the estimation is obtained by

$$\hat{p}(\mathbf{x}_{1,k} | \mathbf{z}_{1,k}) = \sum_{i=1}^N W_k^{(i)} \delta(\mathbf{x}_{1,k} - \mathbf{x}_{1,k}^{(i)}) \quad (24)$$

$$\hat{p}(\mathbf{x}_k | \mathbf{z}_{1,k}) = \sum_{i=1}^N W_k^{(i)} \delta(\mathbf{x}_k - \mathbf{x}_k^{(i)}) \quad (25)$$

where N is the number of particles and $W_k^{(i)}$ is the normalized weight for the i -th particle at time k .

To combat the problem of degeneracy in practical use, resampling may be used. However, resampling can also limit parallel processing and cause sample impoverishment. Hence, it is only performed when the following metric

$$N_{eff} \approx \frac{1}{\sum_{i=1}^N (W_k^{(i)})^2} \quad (26)$$

is smaller than a preselected value N_T , which is typically $N_T = \frac{N}{2}$. We now present the pseudo code of the particle filter with SIS and resampling techniques.

Algorithm 2 The SIS particle filter

```

1: Input:  $N$  streams of particles from prior pdf  $p$  of  $\mathbf{x}_0$ 
2: Output:  $N$  particles conformed to  $p(\mathbf{x}_t | \mathbf{z}_{1,t})$ 
3:
4: For  $i = 1$  to  $N$  do
5:   Draw  $\mathbf{x}_0^{(i)} \sim p(\mathbf{x})$ ; initialize  $N$  streams.
6:   Set  $W_0^{(i)} = \frac{1}{N}$ ; All initial weights are equal.
7: end
8: For  $k = 1$  to  $n$  do
9:   For  $i = 1$  to  $N$  do
10:    Draw  $\mathbf{x}_k^{(i)} \sim q(\mathbf{x} | \mathbf{x}_{k-1}^{(i)}, \mathbf{z}_k)$ 
11:     $\omega_k^{(i)} = \omega_{k-1}^{(i)} \frac{p(\mathbf{z}_k | \mathbf{x}_k^{(i)}) p(\mathbf{x}_k^{(i)} | \mathbf{x}_{k-1}^{(i)})}{q(\mathbf{x}_k^{(i)} | \mathbf{x}_{k-1}^{(i)}, \mathbf{z}_k)}$ 
12:   end
13:   For  $i = 1$  to  $N$  do
14:    Compute normalized weights  $W_k^{(i)}$ 
15:   end
16:   Compute  $N_{eff}$ .
17:   If  $N_{eff} \leq N_T$ ;  $N_T$  preselected
18:     Resample  $\{\mathbf{x}_k^{(i)}, W_k^{(i)}\}_{i=1}^N$  to get  $\{\bar{\mathbf{x}}_k^{(i)}, \frac{1}{N}\}_{i=1}^N$ 
19:     Set  $\mathbf{x}_k^{(i)} = \bar{\mathbf{x}}_k^{(i)}$ ,  $\omega_k^{(i)} = \frac{1}{N}$ 
20:   end
21: end

```

V. SIMULATION AND ANALYSIS

In this section we present the trajectory prediction results of the advanced filtering algorithms discussed in Section IV, i.e., augmented noise Kalman filter (AP-KF), the fading-memory filter (FM-KF), and the particle filter (PF). Table II lists some notations we use in this section.

TABLE II: Notations for different filters

Filter	Trajectory	Position coordinates	Velocities
AP-KF	X_{AP-KF}	$x_{AP-KF} \ y_{AP-KF}$	$\dot{x}_{AP-KF} \ \dot{y}_{AP-KF}$
FM-KF	X_{FM-KF}	$x_{FM-KF} \ y_{FM-KF}$	$\dot{x}_{FM-KF} \ \dot{y}_{FM-KF}$
PF	X_{PF}	$x_{PF} \ y_{PF}$	$\dot{x}_{PF} \ \dot{y}_{PF}$

A. AP-KF

As discussed in Section IV-A, we incorporate the \mathbf{Q} matrix with its diagonal entries filled with positive values σ^2 . In the experiments, we set the noise power σ to 10. Results of Scene 1 and Scene 2 are shown in Fig.5a - 5c and Fig.6a - 6c respectively. For both the scenes, the AP-KF predicts

the positions, velocities and generates smooth trajectories, reasonably well. On the outset, it seems that the raw and predicted trajectories are identical, however a closer look reveals the filter do not completely follow the measurements. We observe that the aircraft's velocities are much harder to track than positions. Comparing the velocity estimates in both scenes, we find that augmenting process noise is a reasonably good technique to track abrupt changes of states but may not give as satisfying results when the target is in steady state. In Fig.5c we observe that the estimates give many small spikes while the aircraft seems to maintain a constant velocity according the measurements. If we set a smaller noise power by decreasing the stand deviation values of the noise distribution, the magnitudes of these spikes will be smaller but it impairs the filter's tracking capability as well. There is a trade-off between smoothness and agility. Making covariance of process noise larger gives the filter more flexibility to handle maneuvers at the cost of being more vulnerable to disturbances.

B. FM-KF

A similar trade-off exists for the fading memory Kalman filters since the two methods, as explained, are fundamentally identical. More interestingly, FM-KF has a tunable parameter α , which is set between 1 and 1.5 practically. A larger α forces the filter to have a "shorter memory". For Scene 1, α is set to 1.05, and we observe in Fig.7a - 7c that while the filter gives good position estimates, the velocity estimates are notably lagging from the velocity values. In the case of Scene 2, we explore two values of α i.e., $\alpha = 1.2$ and $\alpha = 1.5$. The results of Scene 2 are presented in Fig.8a and Fig.8c, where we observe for a larger α , we have less lag and less smoothness in the prediction. Hence, for the FM-KF the parameter α controls the trade-off. A small α makes the filter to rely more on past measurements, which makes the filter more stable and generates smoother results. At the same time, the filter will be less responsive. A large α , however, forces the filter to quickly adapt to the changes of target's states and admit more noise.

C. PF

The last set of results are produced for the particle filter, which is shown in Fig.9a - 9c and Fig.10a - 10c, for Scene 1 and Scene 2 respectively. An important parameter to tune is the number of particles initialized (N). Unlike the Kalman filters, PF relies on Monte Carlo simulation to sample from probability distributions of our interest. It starts from any arbitrary initial distribution and gradually adjusts the distribution to be more and more similar to real posterior distribution. So with more initialized particles the filter can obtain more samples for adjustment and gives a more precise approximation. See for example, the Fig.10c, where not surprisingly, the prediction with 20000 particles is smoother than that with only 5000 particles. Moreover, due to the extreme flexibility of PF, both trajectories have no evident lag or deviation, which indicates that PF effectively handles the model mismatch problem. PF is

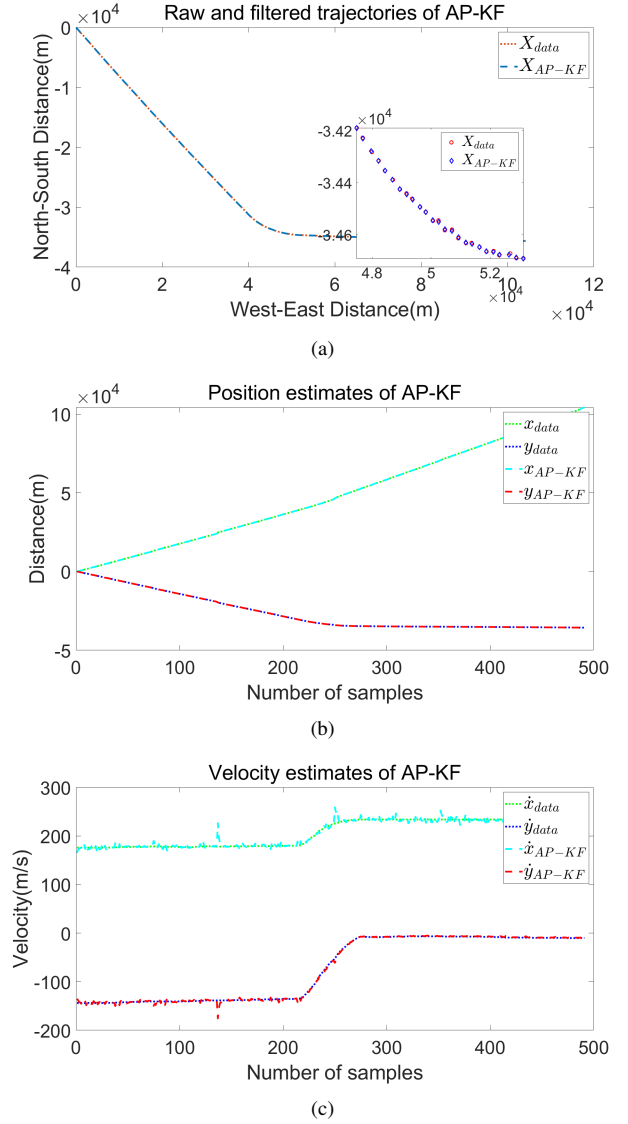
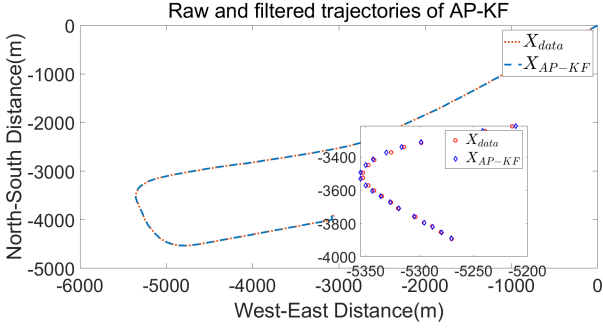


Fig. 5: Scene 1: Predicted trajectory, position and velocity estimates using AP-KF

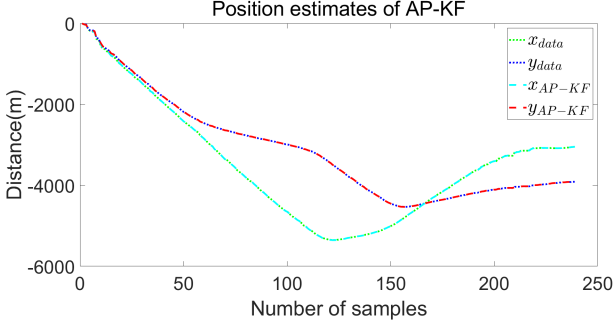
also more robust, with better responsiveness and smoothness, particularly in contrast to FM-KF.

VI. CONCLUSION AND FUTURE WORK

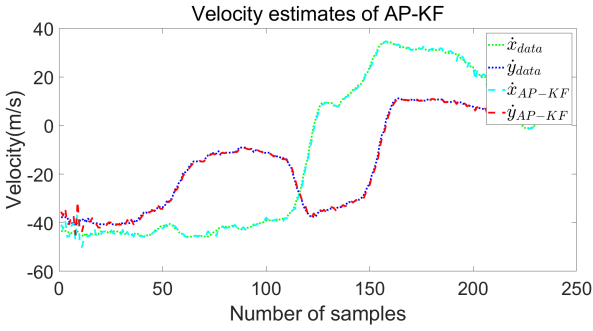
In this paper, we presented relevant knowledge of working with ADS-B system and evaluated several target tracking methods on realistic ADS-B data sets. These methods are based on models of simplified flight dynamics. We discussed the CV-KF algorithm and showed through experiment results that it does not meet our requirements, due to simplified Gaussian linear state space model assumption. To overcome the limitation of CV-KF, we propose three improved methods, namely the AP-KF, FM-KF, and PF. Simulation results show that all three methods offer improvements as compared to the CV-KF on trajectory, position and velocity estimation in the two flight scenes. In particular PF outperforms the other



(a)

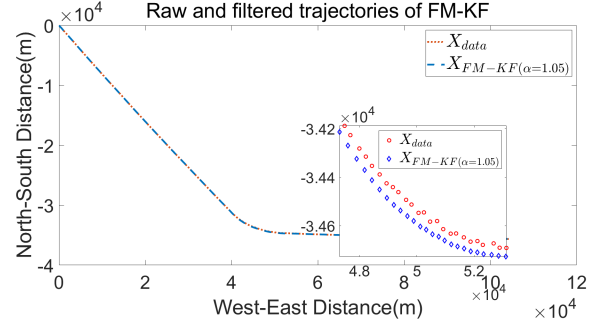


(b)

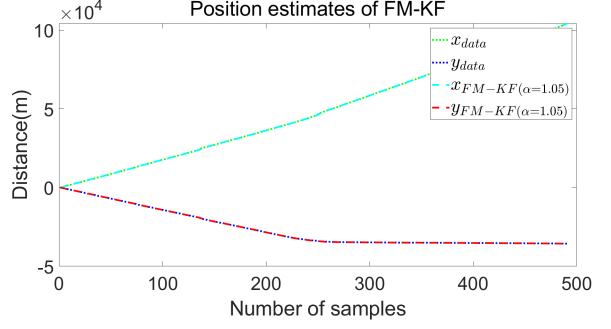


(c)

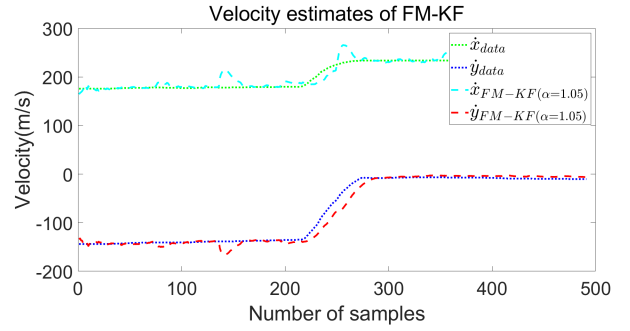
Fig. 6: *Scene 2*: Predicted trajectory, position and velocity estimates using AP-KF



(a)



(b)



(c)

Fig. 7: *Scene 1*: Predicted trajectory, position and velocity estimates using FM-KF

solutions, since it overcomes the underlying assumption of Gaussian linear state space models, of the Kalman filters.

The accuracy of PF for the prediction comes with the cost of large memory and computational load, and hence other non-linear filtering methods and non-parametric models could be explored. In general, the use of only one dynamic model creates a bottleneck for the tracking performance, hence a multiple model approach or data-driven approaches could yield more optimal results [11]. Furthermore, in this paper we explored only a limited part of the data set i.e., 2 scenes, and that from 2 flights, which is a limitation. Additional experiments which use a large number of flights from both the *TrajAir* and *TUD* data sets must be evaluated to investigate the performance of the proposed solutions.

REFERENCES

- [1] J. Sun, *The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals*, 2nd ed. TU Delft OPEN Publishing, 2021.
- [2] J. Patrikar, B. Moon, J. Oh, and S. Scherer, "Predicting Like A Pilot: Dataset and Method to Predict Socially-Aware Aircraft Trajectories in Non-Towered Terminal Airspace," arXiv:2109.15158 [cs.RO], Sep. 2021.
- [3] Regulation (EU) 2020/587 by European Union Aviation Safety Agency. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020R0587>.
- [4] Code of Federal Regulations by Federal Aviation Administration. Retrieved from <https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-91/subpart-C/section-91.225>.
- [5] W. Huygen, "ADS-B Signal Integrity and Security Verification Using a Coherent Software Defined Radio: Mitigation of the threat of maliciously injected signals in ADS-B networks," M.S. thesis, faculty of aerospace engineering, TU Delft, Delft, 2021. Available: <http://resolver.tudelft.nl/uuid:1129afb3-304f-4c63-afa3-ca9f2bd73f86>.
- [6] D. Simon, *Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006.

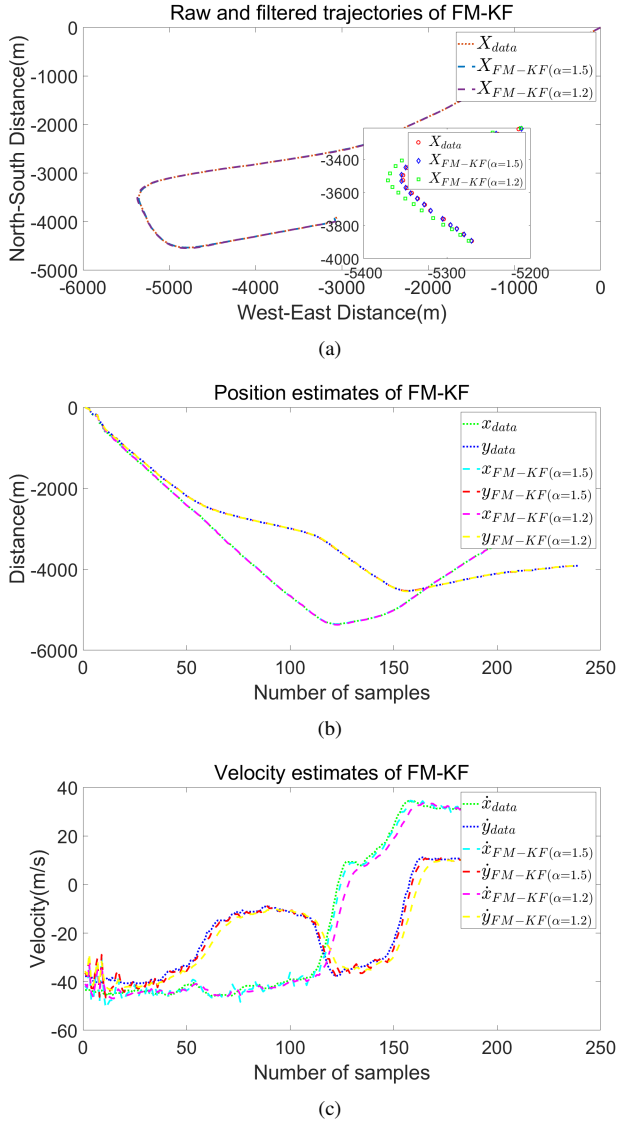


Fig. 8: Scene 2: Predicted trajectory, position and velocity estimates using FM-KF

- [7] P. Zarchan and H. Musoff, *Fundamentals of Kalman Filtering: A Practical Approach*, VA, Reston: American Institute of Aeronautics and Astronautics, pp. 616-617, 2005.
- [8] B. Ristic, M. S. Arulampalam, N. Gordon, *Beyond the Kalman Filter, Particle Filters For Tracking Applications*, Artech House, 2004.
- [9] A. F. M. Smith and A. E. Gelfand, "Bayesian statistics without tears: A sampling-resampling perspective", *Amer. Statist.*, vol. 46, no. 2, pp. 84-87, 1992.
- [10] J. Sun, H. Vũ, J. Ellerbroek and J. M. Hoekstra, "pyModeS: Decoding Mode-S Surveillance Data for Open Air Transportation Research," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 7, pp. 2777-2786, July 2020, doi: 10.1109/TITS.2019.2914770.
- [11] X. Rong Li and V. P. Jilkov, "Survey of maneuvering target tracking. Part V. Multiple-model methods," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 41, no. 4, pp. 1255-1321, Oct. 2005, doi: 10.1109/TAES.2005.1561886.
- [12] S. Theodoridis, *Machine Learning: A Bayesian and Optimization Perspective*. San Diego, CA, USA: Academic, 2015.

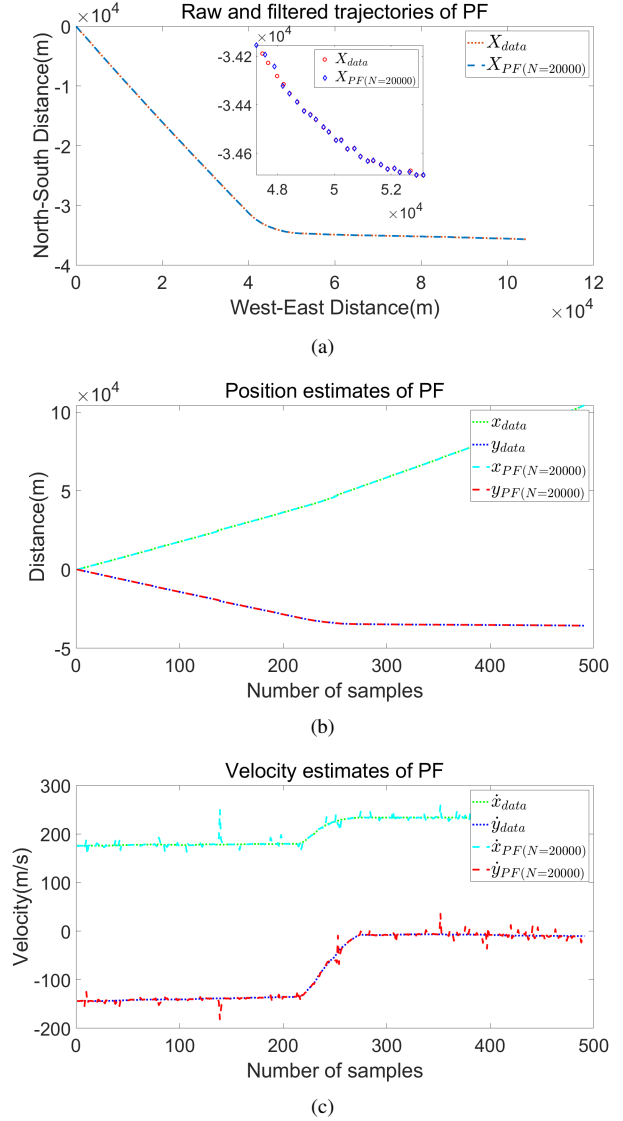
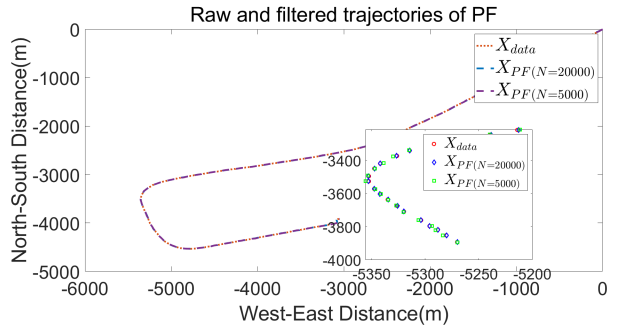
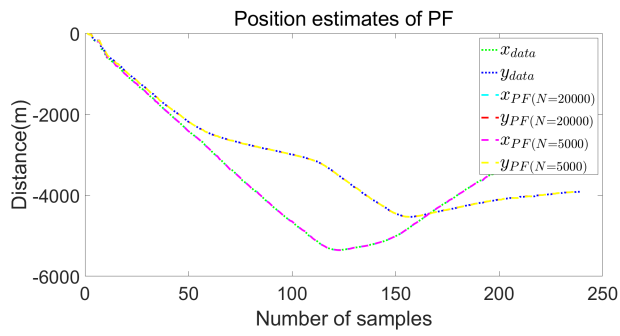


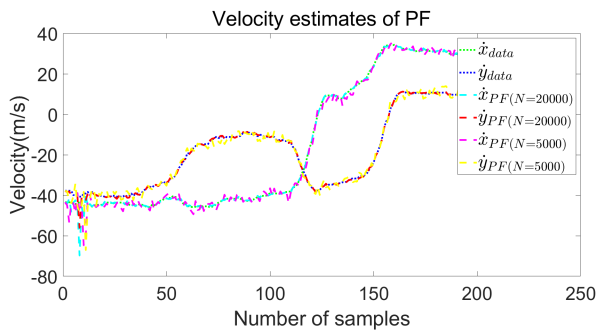
Fig. 9: Scene 1: Predicted trajectory, position and velocity estimates using PF



(a)



(b)



(c)

Fig. 10: *Scene 2*: Predicted trajectory, position and velocity estimates using PF

Temporal synchronization of radar and lidar streams

David Aledo

*Circuits and Systems Group
Delft University of Technology
Delft, The Netherlands
d.aledoortega-1@tudelft.nl*

Tanmay Manjunath

*Circuits and Systems Group
Delft University of Technology
Delft, The Netherlands*

Raj Thilak Rajan

*Circuits and Systems Group
Delft University of Technology
Delft, The Netherlands*

Darek Maksimiuk

*Innatera Nanosystems
Rijswijk, The Netherlands*

Rene van Leuken

*Circuits and Systems Group
Delft University of Technology
Delft, The Netherlands*

Abstract—In multi-sensor systems, several sensors produce data streams, commonly, at different frequencies. If they are let running wild without synchronization, after a period of time, they are likely to be disordered, presenting as simultaneous measures that have been recorded at different times. That can be disastrous in many data fusion applications. This paper is about their temporal synchronization and ordering, so they can be coherently fused. Some sensors do not have timestamps from which order the streams, and even if they have, they may be not trustable for different reasons. First, we define mathematically the problem of multi-sensor data stream synchronization. Then, we handle the problem of estimating the actual time of sensor measurement using mean or median filters. Next, we address the issue of reconstructing incoming sensor data streams according to the estimated sensor measurement times while maintaining minimal latency and synchronization error by employing an adaptive stream buffering technique utilized in distributed multimedia systems. In order to test our methods, we have recorded an easy-to-use dataset with a radar and a lidar sensors without timestamps. We define a synchronization event that is easily identifiable by a human annotator in both sensor streams. From this dataset, a suitable filter for timestamp estimation is selected, and an analysis of the effects of the stream synchronization algorithm's parameters on buffering latency and synchronization error is presented. Finally, the solution is efficiently implemented on a FPGA.

Index Terms—multi-sensor, synchronization,

I. INTRODUCTION

For precise fusion of different sensors, measurements need to be synchronized both temporally and spatially. This paper aims to design a solution of the temporal synchronization problem for multi-sensor data fusion applications.

Consider a system with multiple data streams provided by different sensors. Probably, some of them have different measurement frequencies. Even if they have the same data rates, there may be drifts between their particular sensor timelines. If they are let running wild without any synchronization, after

a period of time, they are likely to be disordered, presenting as simultaneous measures that have been recorded at different times. That can be disastrous in many data fusion applications.

Particularly, this work has been motivated by the scenarios presented in two European projects: PRYSTINE and ADACORSA. The PRYSTINE project addresses challenges in automotive applications, while ADACORSA aims to enable beyond-visual line of sight (BVLOS) for drone navigation. In both these projects, the environment perception of the agent (e.g., automotive or drone) is crucial and is achieved by sensor fusion of on-board sensors e.g., cameras, radars and lidars. In both scenarios, the temporal synchronization must to be realized in real-time, with minimum latency, and low resources (specially power). While data fusion involving cameras has been more extensively studied, including its synchronization, radar and lidar data synchronization and fusion can be more challenging. The main reason is that camera images are more easily understandable by the human annotators, allowing for easier test and calibration mechanisms like chessboards. Our consider system includes a radar sensor and a lidar sensor, which provides two data streams without timestamps. The streams are collected in a centralized processing system. The module that collects the data streams withing the processing system is the acquisition system, which can add a timestamp on the data upon its arrival. The goal is to introduce a synchronization module, just after the acquisition system, that can correctly order the data streams, with a minim latency and resource utilization, before the main data fusion or processing.

Since some sensors do not have timestamps from which order the streams, and even if they have, they may be not trustable for different reasons, first we need to estimate the measurements timestamps. Therefore, the original problem is divided into two: measure timestamp estimation, and real-time synchronization of timestamped streams.

To better illustrate the problem we are trying to solve, Fig. 1 shows the synchronization problem for the two streams coming from the radar and lidar sensors, and the same two streams correctly synchronized by our solution.

The paper is structured as following: first, a related work section highlighting the available solutions in the state of the

This work was supported by the PRYSTINE Project, funded by Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL JU) in collaboration with the European Union's H2020 Framework Programme and National Authorities, under grant agreement no. 783190. This work is partially funded by the European Leadership Joint Undertaking (ECSEL JU), under grant agreement No 876019, the ADACORSA project - "Airborne Data Collection on Resilient System Architectures."

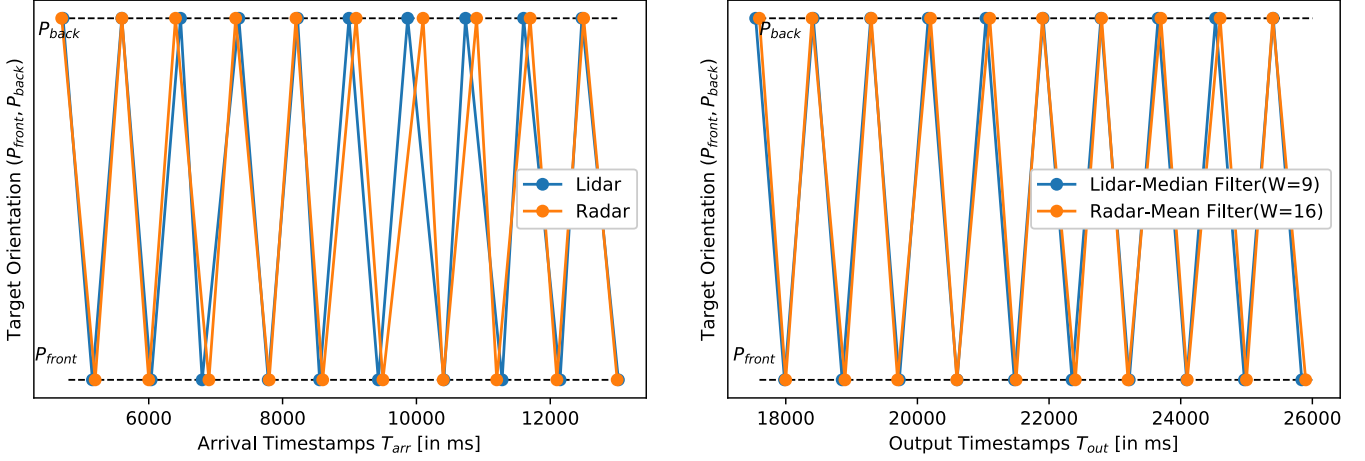


Fig. 1. Synchronization events at given timestamps before (left) and after (right) synchronization.

art for both the timestamp estimation problem and the synchronization problem. Then, in section III, we formulate these problems mathematically, and present the solution algorithm. Section IV describes the dataset collected for the experimental results presented in the following section or results. Finally, in VI, the hardware implementation is described, and in VII the conclusions.

II. RELATED WORK

To address the issue of timestamping sensor measurements in free-running sensor network systems, earlier, in simpler multi-sensor systems, the timestamp on arrival at the acquisition system was used as the true time of measurement for fusion applications [1]. This approach completely overlooks the possibility that the sensor data may be subjected to delays and jitters during transmission and acquisition, causing asynchrony between the measurements. In [2], a software timestamping approach which aims to improve the timestamps quality by reducing delays and jitters during acquisition, is proposed. However, the the sensor data is still timestamped after its arrival at the acquisition system and the data is still subjected to transmission delays and jitters. Hence, these solutions are not suitable for time critical applications where timing misalignment cannot be ignored.

A popular approach is to employ hardware based timestamping for sensor measurements. In [3], a device is used to attach a timestamp to each sensor data frame, before it is transmitted to the acquisition system through the communication link. It has an embedded GPS receiver to get precise UTC (Universal Time Coordinate) times for timestamping. However, this approach cannot be applied to all sensors as it may require the sensors to be programmable and to also have special interfaces. Similar GPS receiver based hardware devices have been used for the synchronization of externally triggered sensors, where the device precisely triggers the sensors at the right instances [4], [5].

For free running asynchronous sensors systems without external synchronization support, the only timestamping that can

be done, is at the acquisition system. Approaches presented in [6], [7] utilise these arrival times to estimate the true sensor measurement times. All these solutions are software timestamping based on linear Kalman filters to essentially filter out delay jitters from arrival times while preserving the effect of the internal sensor clock drift in the true measurement times. However, the estimation procedures in these solutions are software based and are not designed for real-time applications.

The problem of synchronizing streams of data has been extensively investigated in the area of distributed multimedia systems. A classical example of this scenario is the *lip-sync* problem [8], [9], where audio and video streams need to be accurately synchronized during play-out.

The problem of multimedia synchronization can be classified based on location, real-time requirement, type of synchronization (within or between streams), purpose of the synchronization protocol and availability of timing and network information. Based on the real-time requirement of the stream play-out, synchronization techniques are classified as live or synthetic. The former deals with synchronizing live data streams in real-time whereas the later deals with stored media frames [10]. Here, only live synchronization solutions are presented, as they are relevant to our problem.

Media synchronization is an end-to-end problem [11], hence, based on the application, it can be addressed either on the source [12], receiver [13], [14] side, or both [10], [15]. On the source side, a common solution is to attach timestamps and sequence numbers to the transmitting frames [13], [14]. Other source-side techniques mainly consists of changing the properties of the media streams. In some cases, the sources can interleave streams into a single stream before transmission as in [16], [17]. This solution succeeds in eliminating the need for inter-stream synchronization, however, intra-stream synchronization still needs to be addressed. In [17], [18], the source changes the transmission rate of the streams depending on the feedback received from the receiver on the network conditions to prevent asynchrony. On the receiver side, buffer-

ing techniques are commonly employed. The buffering time can either be static based on a maximum jitter value or can be made to vary depending on the network delays [19] and the available buffer size [14]. Other receiver-side techniques consist of dropping late arriving frames [10] or older frames during buffer full conditions [19]. The dropped frames are either left empty or interpolated [14].

For intra-stream synchronization, techniques that aim at reducing the effects of jitter are used. This includes receiver buffering techniques [19]–[21] to smooth the effects of delay variabilities. For inter-stream synchronization, normally, master/slave techniques are used, where one stream is set as a master or reference and the rest as slave streams [20], [21]. At a certain point in time, the bottleneck stream, i.e., the stream affected by the most delay is chosen as the master or reference. Then, the play-out rates of slave streams are adapted to maintain the correct temporal relations with the master stream. In [20], dynamically switch master and slave streams during run-time. However, it is necessary to first remove the effects of network jitter by establishing intra-stream synchronization between the frames before applying inter-stream techniques [11].

Moreover, the complexity of the synchronization solutions majorly depend on the nature of the timing of media frames (as in periodic or non-periodic) and network information such as delays and jitters. If the nature of frame generation is non-periodic then timestamps of frame generation from the source side is compared with the arrival timestamps at the receiver to estimate jitter and buffer the frames accordingly [22]. On the other hand, for periodic streams, arrival period at the receiver can be compared with the period of the stream to estimate jitters and also, inter-stream synchronization becomes less complex than the non-periodic case. In certain systems, assumptions can be made on the network delays and jitter based on the network characteristics. If exact bounds on network jitters are known then constant delay buffers at the receiver would suffice to ensure both inter- and intra-stream synchronization. Also, this eliminates the need for timestamps from the source side. However, if the maximum bound on jitters is too high, then the frames need to buffer for a longer time, leading to large buffering latencies. Besides, in most applications, an exact bound on jitters cannot be known. In such cases, a tolerable synchronization error value is set and the frames are buffered for lesser time. This leads to a trade off between the quality and latency of the synchronization algorithm. To overcome it, adaptive control based solutions are proposed in [20], [21]. They consists of a control algorithm which keeps the latency and quality at check by changing the buffering delays during run-time according to the current jitter conditions while maintaining a pre-set minimum latency and synchronization error. Ideally the control algorithm makes sure that the buffering delays are large enough to compensate for the effects of jitter and stay within tolerable synchronization error but not too large, to keep the latency minimum.

TABLE I
SYSTEM EVENTS AND THEIR TIMESTAMPS

Event	Description	Timestamp
e1	Radar measurement	T_{mea}^R
e2	Radar frame transmission starts	T_{tr}^R
e3	Arrival of radar frame at acquisition system	T_{arr}^R
e4	Lidar measurement	T_{mea}^L
e5	Lidar frame transmission starts	T_{tr}^L
e6	Arrival of lidar frame at acquisition system	T_{arr}^L
e7	Radar synchronization output	T_{out}^R
e8	Lidar synchronization output	T_{out}^L

III. MATHEMATICAL FORMULATION OF THE SYNCHRONIZATION PROBLEM

To formulate the problem formally, we first define all the events in the system, which includes the sensors radar and lidar, and the acquisition system that collects the data streams before processing. We introduce a synchronization module just after the acquisition system. For each event, a timestamp is assigned. Events and their corresponding timestamps are listed in Table I. The events ($e1, e2, e3$) and ($e4, e5, e6$) occur in a sequence. We define these sequences of events as: the radar acquisition process ($P^R : e1 \rightarrow e2 \rightarrow e3$), and the lidar acquisition process ($P^L : e4 \rightarrow e5 \rightarrow e6$). These processes occur asynchronously and are independent of each other. There are any relationships between the events of the two processes, since, depending on the sensor sampling rate and the initial start offset between the sensors, the order can change during the run time.

The considered radar and lidar sensors do not have clocks or any other mechanism to record the times of their events. However, at the acquisition system, the arrival times of radar and lidar frames (T_{arr}^R and T_{arr}^L) are assigned by a common clock. A solution to this issue may be to connect external clocks to record the event timestamps. However, this solution is both expensive and unreliable since the triggering of an event cannot be observed accurately from external clocks due to distortions introduced by the interconnecting cables.

From the moment the sensors capture the measurements to the point they arrive at the acquisition system, the sensor data stream is subjected to various delays. These delays are unpredictable and their magnitudes have no definite bounds, leading to vastly varying arrival latencies. In addition, delays are different for each sensor data stream resulting in measures captured at different time being presented as simultaneous to the fusion algorithm. A good understanding of the nature of the delays along with the source of delay variability factors is essential to formulate an efficient synchronization algorithm. Some of the significant delays in the considered system are:

- **Pre-processing delays:** are delays that are incurred on the sensors for modifying/processing the raw sensor measurements. It includes delays due to on-sensor chip pre-processing steps and packetization of sensor measurements into appropriate format transmission. With respect

to the model, these are the delays between events $e1$ and $e2$ in the radar, and between $e4$ and $e5$ events in the lidar.

- **Communication delays:** are the delays experienced by the sensor data during its transfer from the sensor to the acquisition system. Depending on the size of the measurements, a single sensor measurement can be broken down into several packets/frames¹. The delays due to queuing of these frames, the physical transmission of the data, all constitute communication delays. In the model, these are the delays between events $e2$ and $e3$ in radar, and between $e5$ and $e6$ events in the lidar.

We now define the term *measurement latency*, which refers to the overall latency experienced by the k^{th} sensor measurement from its capture at the sensor to its arrival at the acquisition system. *Measurement latency* ($\Delta\tau^R[k]$, $\Delta\tau^L[k]$) is given by:

$$\Delta\tau[k] = T_{arr}[k] - T_{mea}[k]. \quad (1)$$

Measurement latency is essentially an abstraction of all the delays and their associated delay variability that a sensor measurement is subjected to, and hence, can also be modelled as:

$$\Delta\tau[k] = d - \delta_{jitter}[k] \quad (2)$$

where $\delta_{jitter}[k]$ denotes the jitters in delays for the k^{th} sensor measurement and, d represent the expected value (mean) of their respective sensor delays.

With events, timestamps, and delays of the system defined, we now mathematically formulate the problem. On the top level, we aim to maintain the same temporal relationships between the measurements in which they were originally recorded. We define two types of temporal relations in the model:

- **Intra-stream relations:** refers to the temporal relationship between the frames belonging to the same stream. More precisely, the intra-stream relation is the time difference between events of two consecutive sensor measurements captured by the same sensor. The intra-stream temporal relation between the $[k-1]^{th}$ and k^{th} events of the same stream is:

$$\Delta T[k-1, k] = T[k] - T[k-1]. \quad (3)$$

- **Inter-stream relations:** refers to the temporal relationship between corresponding frames belonging to different streams. It is the delay difference between events of two corresponding measurements captured by different sensors. The inter-stream temporal relation between between the k^{th} radar and lidar events is:

$$\Delta T^{R,L}[k] = T^R[k] - T^L[k]. \quad (4)$$

To meet our goal, we need to achieve:

¹For simplicity, we associate each measurement with a single frame.

- 1) **Intra-stream synchronization:** to maintain the intra-stream relationships in which the measurements were originally recorded, the following condition must hold:

$$\Delta T_{out}[k-1, k] = \Delta T_{mea}[k-1, k]. \quad (5)$$

- 2) **Inter-stream synchronization:** analogously,

$$\Delta T_{out}^{R,L}[k] = \Delta T_{mea}^{R,L}[k]. \quad (6)$$

However, due to the jitter component of the delay factors, disturbances are introduced into the temporal relationships of sensor measurements as they arrive at the acquisition system. Thus, we can expect

$$\Delta T_{arr}[k-1, k] \neq \Delta T_{mea}[k-1, k], \quad (7)$$

and

$$\Delta T_{arr}^{R,L}[k] \neq \Delta T_{mea}^{R,L}[k]. \quad (8)$$

Using (1), (2), and (3), we can view $\Delta T_{arr}[k-1, k]$ as a noisy version of $\Delta T_{mea}[k-1, k]$:

$$\Delta T_{arr}[k-1, k] = \Delta T_{mea}[k-1, k] + \delta_{jitter}[k] - \delta_{jitter}[k-1] \quad (9)$$

where δ_{jitter} is assumed to be zero-mean white noise.

With this, a straightforward solution will be to re-construct the sensor data streams at the acquisition system by buffering accordingly to compensate for the effect of jitters on each sensor frame. Unfortunately, in our concerned system, T_{arr}^R and T_{arr}^L are the only timing information available. Therefore, we formulate the solution into the following steps:

- 1) Estimate intra-temporal relations of measurements ($\hat{\Delta T}_{mea}[k-1, k]$) by filtering the observed $\Delta T_{arr}[k-1, k]$.
- 2) Extract estimated timestamps (\hat{T}_{mea}) from temporal relation estimates.
- 3) Buffer and re-construct the data streams. The main objective here is to ensure that the incoming sensor data is streamed out in real-time while maintaining time synchronization.

As we do not have any measure or estimate of the measurement latency, and since for us it is more important the stream ordering rather than knowing the exact time of a measurement, the arrival time of the first sensor measurement at the acquisition system is assigned as estimator of the first $e1$ and $e4$ timestamps

$$\hat{T}_{mea}[0] = T_{arr}[0], \quad (10)$$

although a better estimate can be obtained if d is known or estimated

$$\hat{T}_{mea}[0] = T_{arr}[0] - d. \quad (11)$$

The timestamps extracted from the above method can be inaccurate during the following two scenarios and have to be corrected accordingly:

- 1) When the calculated measurement timestamp is greater than its corresponding arrival timestamp ($\hat{T}_{mea}[k] >$

$T_{arr}[k]$). It would mean that the measurement is captured in the sensor later than its arrival at the acquisition system. Hence, the estimate is reset with (10) or (11) using the current arrival timestamp.

- 2) When a frame is lost. In this case, the timestamp of the next measurement can be wrongly associated to the timestamp of the lost measurement. The observed cycle time after a lost measurement is larger than normal cycle times. Therefore, a threshold is set to detect lost measurements ($\Delta\hat{T}_{mea}[k-1, k] > Th_{lost}$), and $\hat{T}_{mea}[k]$ is reset like in the previous case.

After timestamp estimation, the implemented algorithm is based on solutions presented in [20], [21], [23]. These algorithms ensure intra- and inter-stream synchronization in real-time by employing control-based adaptive buffering techniques. With the estimates and arrival timestamps available, the algorithm accomplishes synchronization by comparing and equalising measurement latency of each sensor. The equalization is carried out by piece-wise adjustment of buffering times while meeting a set of Quality of Service (QoS) factors along with a minimal overall latency. The QoS factors are:

- **Maximum intra-stream phase distortion.** Intra-stream phase distortion (Intra-SPD), $\Delta\phi_{intra}$, is the difference between the measurement latencies of two consecutive frames of the same sensor stream. A maximum allowable threshold on intra-SPD is set for each sensor ($Th \cdot \Delta\phi_{intra}$). If the arrival of an incoming sensor measurement does not fall within it, then, the frame is considered to have arrived too late and thus, discarded. Intra-SPD is calculated as:

$$\Delta\phi_{intra}[k-1, k] = |\Delta\tau[k] - \Delta\tau[k-1]|. \quad (12)$$

Since we do not know $\Delta\tau[k]$, we use its estimator

$$\Delta\hat{\tau}[k] = T_{arr}[k] - \hat{T}_{mea}[k]. \quad (13)$$

- **Maximum inter-stream phase distortion.** Inter-stream phase distortion (inter-SPD) is the difference between the measurement latencies of two adjacent sensor measurements belonging to different sensor data streams. Here, *adjacent sensor measurements* refer to measurements that have been most closely captured by two different sensors. A maximum allowable threshold on inter-SPD ($Th \cdot \Delta\phi_{inter}^{R,L}$) is set. Any frame arriving beyond it, is discarded. Inter-SPD is calculated as:

$$\Delta\phi_{inter}^{R,L}[k] = |\Delta\tau^R[k] - \Delta\tau^L[k]|. \quad (14)$$

Intra-SPD and inter-SPD quantifies the disruption in intra- and inter-stream relationships, respectively.

The synchronization algorithm can be divided into two schemes focusing on intra-stream and inter-stream synchronization. On the top level, intra-stream synchronization is first established by adaptive buffering and then inter-stream synchronization is ensured by maintaining the buffering alignment of different streams.

It occurs in two steps for every data stream independently: 1) *output time decision*, and 2) *adaptive control algorithm for buffering*.

Output Time Decision: in this step, the output time of the each sensor measurement (T_{out}) is decided. A virtual clock-timer is employed on the acquisition system and the sensor measurements are streamed out with respect to the its timeline. The virtual timer can be set-back or advanced, thereby controlling the buffering times. We define three output cases *wait*, *nowait* and *discard* where the sensor measurement is buffered, streamed out immediately and discarded, respectively. The output case is decided by comparing the time of arrival of the sensor measurement at the acquisition system, recorded by the virtual timer, and the estimated time of its capture. The virtual timer is initialised to the arrival time of the first sensor data frame. The virtual timer value at current time is denoted T_{vt} . The conditions for each of the output cases are:

- **Wait** case: if the arrival time of the incoming sensor measurement (recorded by the virtual timer) is lesser than the estimated measurement capture time, means that the current measurement arrived earlier, compared to the previous sensor measurement, and hence, it needs to be buffered. The *wait* case condition for sensor frame k is

$$T_{arr}[k] \equiv T_{vt} < \hat{T}_{mea}[k]. \quad (15)$$

In this case, the frame is buffered until the virtual timer reaches $\hat{T}_{mea}[k]$. Therefore, the buffering time is

$$\Delta\tau_{buffer}[k] = \hat{T}_{mea}[k] - T_{arr}[k]. \quad (16)$$

- **Nowait** case: the incoming sensor measurement is considered to arrive late if its arrival time (recorded by the virtual timer) is larger than the estimated measurement capture time. In this case, if its arrival time falls within the intra-SPD threshold, the frame is streamed immediately. The *nowait* case condition for sensor frame k is

$$\hat{T}_{mea}[k] < T_{arr}[k] \equiv T_{vt} < \hat{T}_{mea}[k] + Th \cdot \Delta\phi_{intra}. \quad (17)$$

- **Discard** case: if the incoming frame is too late that its arrival time falls out of the maximum intra-SPD allowed, it is discarded. The *discard* case condition for sensor frame k is

$$T_{arr}[k] \equiv T_{vt} \geq \hat{T}_{mea}[k] + Th \cdot \Delta\phi_{intra}. \quad (18)$$

An adaptive control algorithm for buffering is employed to keep the synchronization error versus buffering time latency trade-off in check. The control algorithm keeps a count of each of the output cases. At any point in time, the count values of the *wait*, *nowait* and *discard* cases represent the arrival distributions of the sensor measurements. Hence, based on this values and certain pre-set thresholds, the algorithm determines whether the sensor measurements are being under- or over-buffered over the past window of time. Furthermore, the algorithm setbacks or advances the virtual timer depending on under-buffer and over-buffer conditions, accordingly.

- **Under-buffer** case: if the the count of *nowait* or *discard* cases is greater than its threshold (Th_{nowait} and $Th_{discard}$). *Nowait* and *discard* cases introduce synchronization errors because the frames are not streamed out at \hat{T}_{mea} . So, when under-buffering is detected, the virtual timer is set-back to ensure higher buffering times and reduce the synchronization error. The set-back displacement (ΔT_{vt}^-) is

$$\Delta T_{vt}^- = (1 - \#wait/Th_{wait}) max.\Delta T_{vt} \quad (19)$$

where $\#wait$ is the count of *wait* cases, and $max.\Delta T_{vt}$ is the maximum shift allowed. Further, the count values of *nowait* and *discard* are reset to 0.

- **Over-buffer** case: if the count of *wait* cases is greater than its upper threshold and *nowait* and *discard* counts are below a lower threshold (LTh_{nowait} and $LTh_{discard}$). The virtual timer is advanced to reduce the latency of future frames, and $\#wait$ is reset to 0.

$$\Delta T_{vt}^+ = (1 - \#nowait/Th_{nowait}) max.\Delta T_{vt} \quad (20)$$

Intra-stream synchronization is established by equalising measurement latencies, thereby, ensuring that the offset between the virtual arrival time and the measurement capture time of the sensor measurement is corrected. In a similar fashion, inter-stream synchronization is established by further buffering sensor measurements in order to align the virtual timers of the two streams. Firstly, a reference sensor stream is selected. The reference stream is the stream whose measurement frames experience larger delays among the considered sensor streams. It can be easily identified as the stream with the smallest virtual timer value. This is because, considering the larger measurement latency, the control algorithm would have initiated set-back calibrations to the stream. Initially, any arbitrary sensor stream can be set as the reference stream. We denote the virtual timer value of the reference stream T_{vt}^{ref} , and the follower one T_{vt}^{fol} . Overall, the idea is to set-back the virtual timer of the follower stream if the offset between the streams is more than a tolerable bound of inter-SPD. The inter-stream offset condition is

$$T_{vt}^{fol} - T_{vt}^{ref} \leq Th.\Delta\phi_{inter}^{ref,fol} - \max(Th.\Delta\phi_{intra}^{ref}, Th.\Delta\phi_{intra}^{fol}). \quad (21)$$

This condition is checked every time a set-back or advance calibration is performed on the reference stream. If the condition is not satisfied, then the follower stream is set-back by the difference between the two sides of the inequality (21). In addition, any advance displacement of the follower stream is cancelled to match with the slower buffering rate of the reference stream.

IV. EXPERIMENTAL DATASET

To verify the accuracy of the temporal synchronization solution, a moving Meccano contraption, as shown in Fig. 2 was set up to be used as a common target for both the radar and lidar sensors. The device consists of a clear and distinguishable target (the twin plates), which revolves

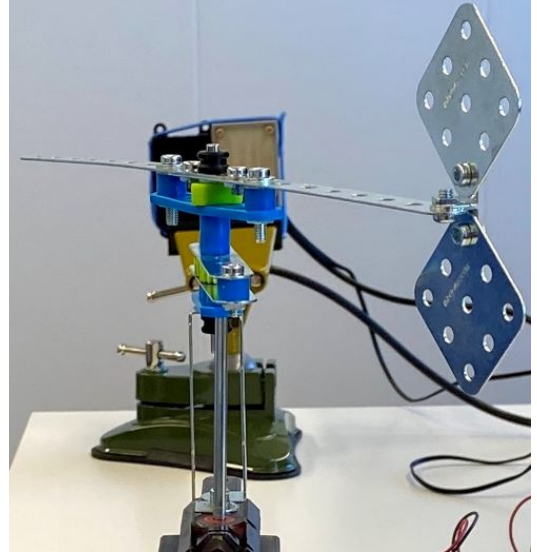


Fig. 2. Rotating device used as a common target of the sensors.

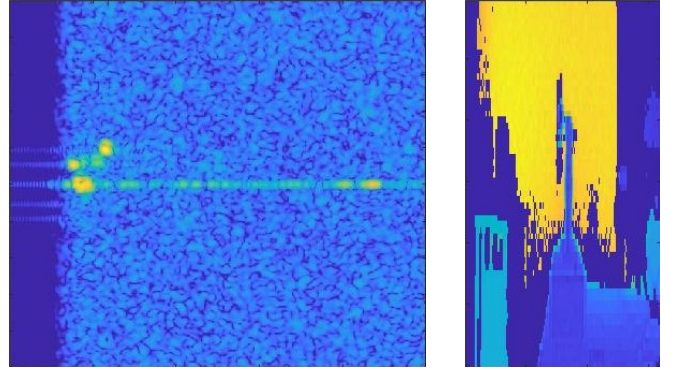


Fig. 3. Example frames of a synchronization event. Left: radar range-Doppler map. Right: lidar depth map.

around a fixed axis at a constant speed. This setup ensures that the position measurements obtained by both sensors are distinguishable for comparison and that the spatial error in the position measurement is negligible. Thus, the differences in the positions of the target observed from the sensors are solely due to the temporal errors.

The radar sensor is a 77GHz radar from RFBeam model MR3003_RD. And the lidar sensor is a solid state lidar from Hypersen model HPS-D160-U. Fig. 3 show the captured radar range-Doppler map and lidar depth map of the rotating device. The position of the revolving plates can be clearly observed from both the range-Doppler map as well as the depth map. To verify the synchronization, the observed positions of the revolving plates by both the sensors are compared at the output of the synchronization system. This setup, though simple, is effective and sufficient enough to evaluate the correctness of the temporal synchronization solution.

For our experiments, the sensor data acquisition and arrival timestamping was performed on a Windows 10 based laptop

TABLE II
MEAN AND VARIANCE OF THE OBSERVED CYCLE TIMES

	Mean (ms)	Variance (ms ²)
$\Delta T_{arr}^R[k-1, k]$	99.998	2.25
$\Delta T_{arr}^L[k-1, k]$	109.315	0.9616

TABLE III
INTER-STREAM RELATIONS FOR DIFFERENT ESTIMATORS

Radar filter	Lidar filter	Average $\Delta T_{out}^{R,L}$ (ms)
none	none	52.709
mean ($W = 16$)	mean ($W = 16$)	43.342
mean ($W = 16$)	mean ($W = 50$)	44.711
mean ($W = 16$)	median ($W = 9$)	27.390
mean ($W = 16$)	median ($W = 59$)	28.742
median ($W = 9$)	mean ($W = 16$)	47.042
median ($W = 9$)	mean ($W = 50$)	47.685
median ($W = 9$)	median ($W = 9$)	37.997
median ($W = 9$)	median ($W = 59$)	37.892

with a 1Gb network interface. The radar data stream comes from an Ethernet port and, the arrival timestamps for the measurements are generated after the measurement is read from the TCP/IP socket. Similarly, the lidar data stream comes from a serial port and, the arrival timestamps are generated after reading each data measurement from the serial port. The time resolution of the timestamps is 1ns and stored as a 64bit unsigned integers.

V. RESULTS

A population size of 5000 frames is used for calculation of the statistical measures. The mean and the variance values of the observed intra-stream relations are summarized in Table II. Fig. 4 shows the observed intra-stream relations at arrival for the radar and lidar sensors, and the estimators at measure time obtained by different filters. The radar shows a repeating pattern of alternating between two Gaussian distributions with variances of 0.00045ms² and 0.00046ms² centered at 100.59ms and 99.40ms, respectively. The median filter is not very effective in removing this high frequency details. However, on the lidar, that shows a lot of outliers, the median filter is more robust.

Fig. 5 shows the corrected inter-stream relation between synchronization events with different combinations of filters, and Table III their average. We need them to be preferably smaller than approximately half the average cycle time of the sensors ($\Delta T[k-1, k]$) to prevent wrong association with another sensor measurement.

The choice of appropriate $Th \cdot \Delta \phi_{intra}^R$, $Th \cdot \Delta \phi_{intra}^L$, and $Th \cdot \Delta \phi_{inter}^{R,L}$ parameters is based on the Intra-SPD and Inter-SPD. They are set to 0.8ms, 1ms and 2ms, respectively, as shown in Fig. 6 and 7.

The effect of window size (of the adaptive control buffering algorithm) on the total number of setback and advance calibrations of the virtual timer is shown in Fig. 8. The ratio of the output events (wait:nowait:discard) was kept constant as (7:2:1). Next, we observed that the window size did not have

TABLE IV
OUTPUT CASES COUNTS FOR DIFFERENT THRESHOLD RATIOS

Th ratio	wait	nowait	discard
1:7:2	739	4239	21
2:6:2	1807	3188	4
3:5:2	2196	2800	3
4:4:2	2424	2572	3
5:4:1	2098	2897	4
6:3:1	2647	2348	4
7:2:1	3548	1148	3
8:1:1	4296	700	3

significant impact on the number of *wait*, *nowait* and *discard* output cases (Fig. 9). No noticeable trend in buffering latency or synchronization error was observed, however, we cannot expect robust results from smaller window sizes as they may fluctuate the buffering process over small changes in the arrival delay.

To analyse the effect of *wait*, *nowait* and *discard* thresholds, results of buffering latency and synchronization error (inter-SPD on *nowait* cases) with varying buffer control configurations are shown in Fig. 10 and 11. The maximum calibrating factor $max.\Delta T_{vt}$ is set to the average delay variation observed in the stream (average intra-SPD), which is 0.6ms and 0.3ms for radar and lidar streams, respectively. This ensures a smooth offsetting of timer reference. Keeping the window size to 100, the total number of each output case for different threshold ratios are presented in Table IV. There is a direct correlation between the corresponding thresholds and the observed number of events. However, it is to be noted that the set threshold do not hard guarantee the same ratio of events at output. We can observe that with a relatively higher Th_{wait} , buffering latency increases and synchronization error decreases. This is expected because the buffer control algorithm will frequently hit the under-buffer condition due to lower Th_{nowait} and $Th_{discard}$ and hence, increases buffering latency by setting back the virtual timer. Overall, the increase in buffering time also ensures lower synchronisation errors. Conversely, we observe that with lower Th_{wait} , synchronisation error increases and buffering latency decreases due to setting of over-buffering condition leading to advance calibration of virtual timer.

VI. HARDWARE IMPLEMENTATION

The design consists of a buffer, virtual timer, filter, and control block per sensor stream; and a common inter-stream control. The buffers store incoming sensor data and eventually streamed them out as AXI4 streams, according to the decision of control block (based on the estimators provided by the filter). First, the arrival time is recorded by the virtual timer block. Next, the measure timestamp is estimated by the filter. The estimated measurement timestamp is available 2 clock cycle after the arrival of the sensor measurement. The control block also checks the over-buffer and under-buffer cases and sends appropriate setback or advance commands to the virtual timer.

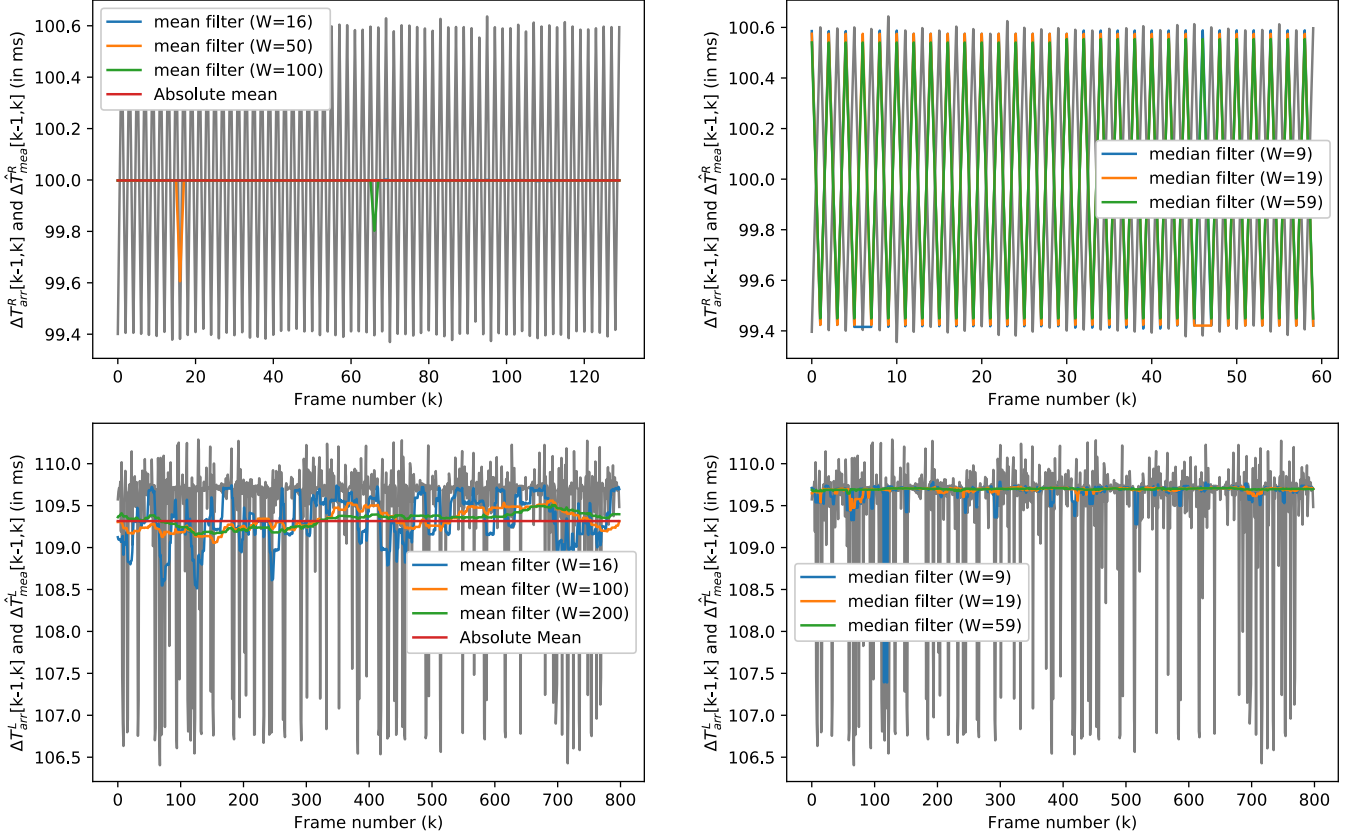


Fig. 4. Observed intra-stream relations at arrival (grey) and estimators obtained by different filters (see legends) for radar (top) and lidar (bottom).

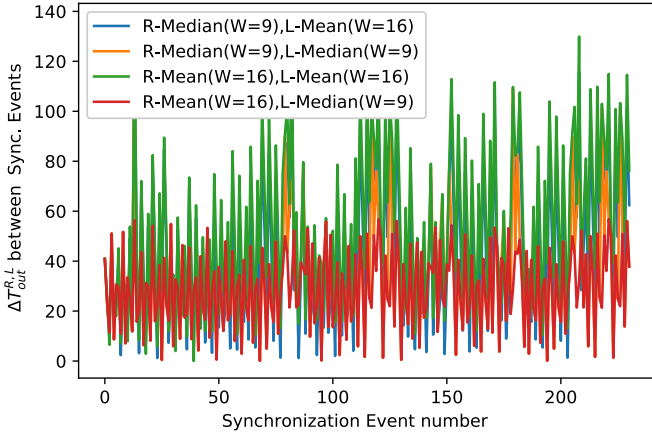


Fig. 5. Inter-stream relation (in ms) between synchronization events with different combinations of filters.

The common inter-stream control block takes care of communications between the streams and ensures inter-stream synchronization. The timestamps are recorded as 64-bit unsigned integers (which is standard for sensor measurement timestamps). A precision of 30ns is used so that drift due to sensor clock, if present, can be taken into account. The design is fully parameterized.

TABLE V
RESOURCE UTILIZATION OF SYNCHRONIZATION BLOCK COMPONENTS

Component	LUT	FF	DSP
Timer	233	136	0
Control	238	92	1
Inter-stream	295	133	0
Full design ^a	2105	1639	2

^aExcluding buffers.

TABLE VI
RESOURCE UTILIZATION OF FILTERS

Filter	Window	LUT	FF	DSP
Mean	16	378	569	0
	20	296	642	1
	32	438	858	0
	50	567	1183	1
	100	1019	2084	1
	128	1401	2588	0
Median	9	462	443	0
	19	1072	624	0
	59	2240	1345	0

Resource utilization of some components of the implemented solution are presented in Table V obtained in Vivado 2018.3 for a Zynq ZC702 evaluation kit. Table VI shows the resource utilization of different filters.

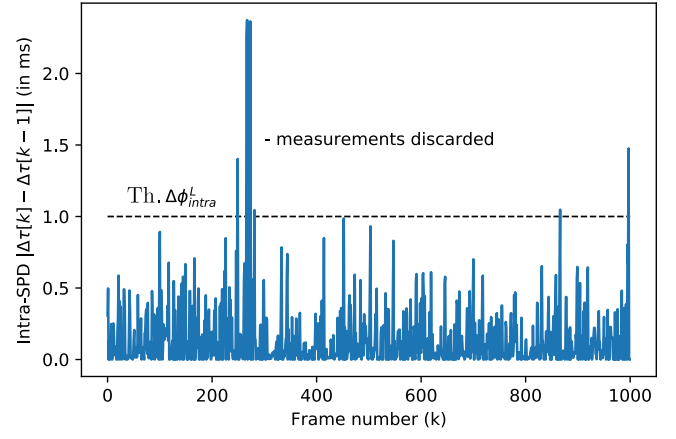
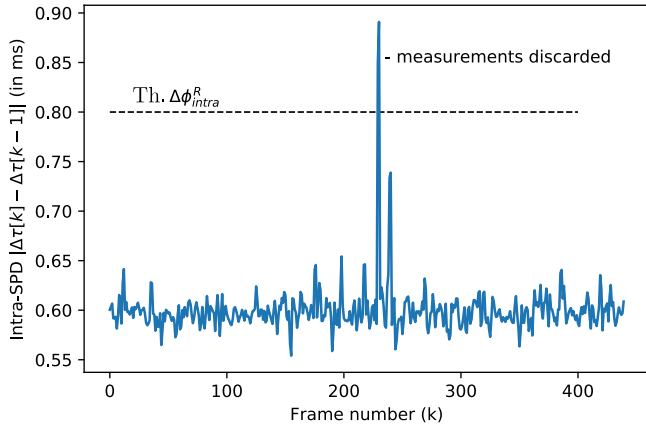


Fig. 6. Intra-SPD and its threshold for radar (left) and lidar (right).

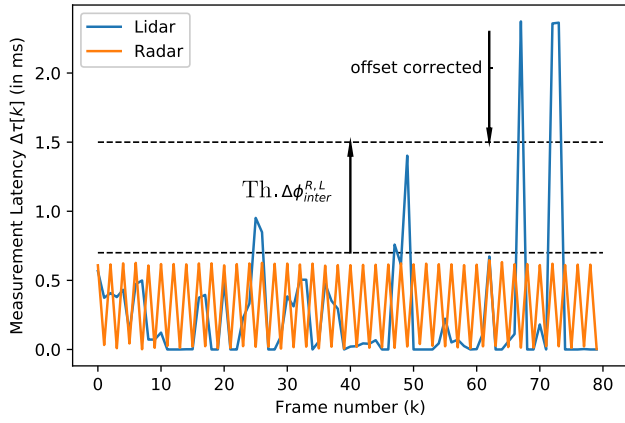


Fig. 7. Measurement latency of adjacent radar and lidar measurements and the maximum inter-SPD threshold.

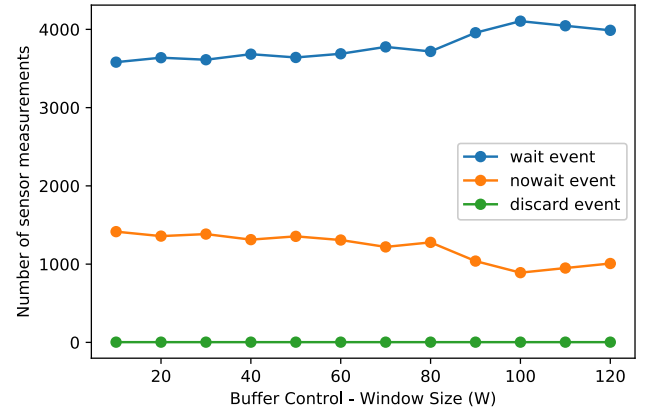


Fig. 9. Effect of window size on the buffering output cases.

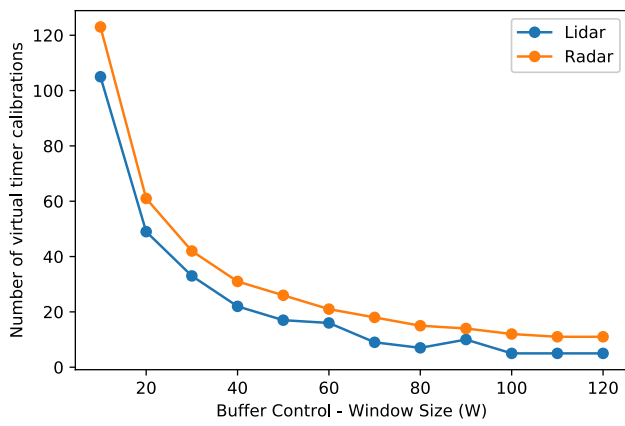


Fig. 8. Effect of window size on the number virtual timer calibrations.

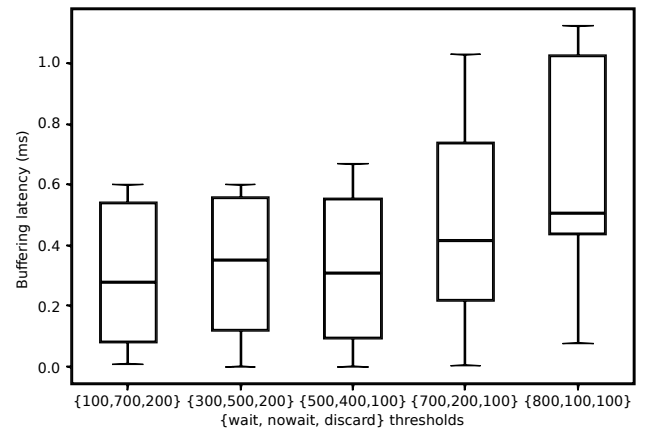


Fig. 10. Box plot of buffering latency for different output cases thresholds.

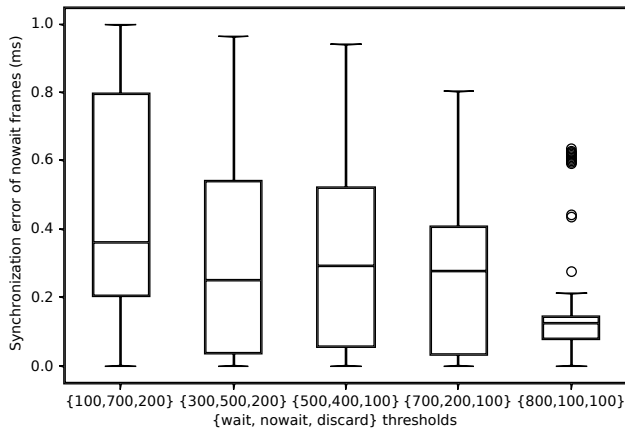


Fig. 11. Box plot of synchronization error caused by streaming-out immediately for different output cases thresholds.

VII. CONCLUSIONS

A temporal synchronization of sensor streams is proposed, which is flexible and can be tuned to the right level of latency versus synchronization error trade-off, according to the needs of the application. For the particular application that triggered this research, composed of 2 streams (radar and lidar), the most optimal output case thresholds are (500, 400, 100) with average buffering latency of 0.32ms and synchronization error of 0.316ms. With a mean filter with window size of 16 for the radar stream, and a median filter with window size of 9 for the lidar stream.

We have recorded an easy-to-use dataset with a radar and a lidar sensors without timestamps. The synchronization event is easily identifiable by a human in both sensor streams. This dataset is perfectly suited for other data fusion application tests. Thus, it is currently on the process of being published.

Finally, an efficient hardware implementation of the synchronization block have been developed, which has a low resource utilization.

It is to be noticed that the acquisition of sensor measurements was done on a machine with Windows10 OS, which does not guarantee real-time requirements and can introduce uncertain delays. Hence, the observed cycle times used in our analysis are not representative of the cycle times observed when sensor acquisition is done directly on hardware or on a real-time operating system.

REFERENCES

- [1] C. Kwok, D. Fox, and M. Meil, "Real-time particle filters," *Proceedings of the IEEE*, vol. 92, no. 3, pp. 469–484, 2004.
- [2] V. Di Lecce, A. Amato, and M. Calabrese, "Gps-aided lightweight architecture to support multi-sensor data synchronization," in *IEEE Instrumentation and Measurement Technology Conference*, 2008, pp. 149–154.
- [3] M. Kais, D. Millescamp, D. Bétaille, B. Lusetti, and A. Chapelon, "A multi-sensor acquisition architecture and real-time reference for sensor and fusion methods benchmarking," in *IEEE Intelligent Vehicles Symposium*, 2006, pp. 418–423.
- [4] D. T. Knight, "Achieving modularity with tightly-coupled gps/ins," in *IEEE PLANS 92 Position Location and Navigation Symposium Record*, 1992, pp. 426–432.
- [5] B. Li, "A cost effective synchronization system for multisensor integration," in *Proceedings of the 17th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS)*, 2004, pp. 1627–1635.
- [6] A. Westenberger, T. Huck, M. Fritzsche, T. Schwarz, and K. Dietmayer, "Temporal synchronization in multi-sensor fusion for future driver assistance systems," in *IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 2011, pp. 93–98.
- [7] J.-O. Nilsson and P. Händel, "Time synchronization and temporal ordering of asynchronous sensor measurements of a multi-sensor navigation system," in *IEEE/ION Position, Location and Navigation Symposium*, 2010, pp. 897–902.
- [8] M. Chen, "A low-latency lip-synchronized videoconferencing system," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '03, 2003, p. 465–471.
- [9] I. Kouvelas, V. Hardman, and A. Watson, "Lip synchronisation for use over the internet: analysis and implementation," in *Proceedings of GLOBECOM'96 IEEE Global Telecommunications Conference*, vol. 2, 1996, pp. 893–898.
- [10] F. Boronat, J. Lloret, and M. García, "Multimedia group and inter-stream synchronization techniques: A comparative study," *Information Systems*, vol. 34, no. 1, pp. 108–131, 2009.
- [11] M. Montagud, P. Cesar, F. Boronat, and J. Jansen, *MediaSync: Handbook on multimedia synchronization*. Springer, 2018.
- [12] S. Baqai, M. Farrukh Khan, M. Woo, S. Shinkai, A. A. Khokhar, and A. Ghafoor, "Quality-based evaluation of multimedia synchronization protocols for distributed multimedia information systems," *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 7, pp. 1388–1403, 1996.
- [13] T. D. C. Little and A. Ghafoor, "Interval-based conceptual models for time-dependent multimedia data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 5, no. 4, pp. 551–563, 1993.
- [14] D. P. Anderson and G. Homsy, "A continuous media i/o server and its synchronization mechanism," *Computer*, vol. 24, no. 10, pp. 51–57, 1991.
- [15] K. Ravindran and V. Bansal, "Delay compensation protocols for synchronization of multimedia data streams," *IEEE Transactions on Knowledge and Data Engineering*, vol. 5, no. 4, pp. 574–589, 1993.
- [16] S. Tasaka and Y. Ishibashi, "Media synchronization in heterogeneous networks: stored media case," *IEICE Transactions on Communications*, vol. 81, no. 8, pp. 1624–1636, 1998.
- [17] —, "A performance comparison of single-stream and multi-stream approaches to live media synchronization," *IEICE Transactions on Communications*, vol. 81, no. 11, pp. 1988–1997, 1998.
- [18] Y. Ishibashi, T. Kanbara, and S. Tasaka, "Inter-stream synchronization between haptic media and voice in collaborative virtual environments," in *Proceedings of the 12th Annual ACM International Conference on Multimedia*, ser. MULTIMEDIA '04. Association for Computing Machinery, 2004, pp. 604–611.
- [19] K. Rothermel and T. Helbig, "An adaptive stream synchronization protocol," in *Network and Operating Systems Support for Digital Audio and Video*. Springer, 1995, pp. 176–189.
- [20] Y. Xie, C. Liu, M. J. Lee, and T. N. Saadawi, "Adaptive multimedia synchronization in a teleconference system," *Multimedia Systems*, vol. 7, no. 4, pp. 326–337, 1999.
- [21] Y. Ishibashi and S. Tasaka, "A synchronization mechanism for continuous media in multimedia communications," in *Proceedings of INFOCOM'95*, vol. 3, 1995, pp. 1010–1019.
- [22] J. Escobar, C. Partridge, and D. Deutsch, "Flow synchronization protocol," *IEEE/ACM Transactions on Networking*, vol. 2, no. 2, pp. 111–121, 1994.
- [23] H. Liu and M. El Zarki, "A synchronization control scheme for real-time streaming multimedia applications," in *Packet Video*, vol. 2003, 2003.

Distributed Detect-and-Avoid with Non-Stationary Obstacles

Ellen Riemens, Raj Thilak Rajan

Circuits and Systems (CAS) Group, Delft University of Technology, The Netherlands

{e.h.j.riemens, r.t.rajan}@tudelft.nl

Abstract—Detect-and-avoid is a crucial challenge in the autonomous navigation of single or multiple agent systems. For safe and reliable autonomous navigation in unknown and dynamic environments, obstacles should be sensed using onboard sensors and the trajectory should be adjusted accordingly. Additional challenge is introduced in the case of multi-agent systems, where the adjusted trajectory could introduce collisions between agents, for example in satellite swarms in Low Earth Orbits (LEO). The increasing amount of occupancy of the low orbit and the presence of space debris gives high risk of damaging satellites due to collisions. With communication between nearby satellites, cooperative methods enable the avoidance of collisions with dynamic obstacles while simultaneously finding an optimal trajectory of the cooperative agents. Drone swarms equipped in industrial settings encounter the challenge of navigating through a dynamic environments in a similar way. The dynamic obstacles are now other autonomous systems as well as humans, performing tasks simultaneously.

In this work, we propose a detect-and-avoid method for multi-agent system, where a distinction is made between cooperative agents and non-cooperative agents, i.e., non-stationary obstacles. A factor graph approach is used to simultaneously estimate the state of both agent categories, followed by an optimal control method in order to adjust the trajectory of the cooperative agents, such that the non-cooperative agents are avoided. This method is fully distributed employing an ADMM approach for consensus on the control strategy.

In our poster, we would show through preliminary results that inclusion of the non-stationary behaviour of objects by distinguishing non-cooperative agents and cooperative agents, decreases the risk of collision. Anticipating the trajectory of the non-cooperative agents within the sensing region leads to an improved trajectory in terms of average direction changes compared to methods assuming stationary obstacles. Reaching consensus between cooperative agents on the control strategy has a similar effect on the average direction changes compared to non-cooperative methods.

Image Search Engine by Deep Neural Networks

Yuan Yuan Yao^{1*}, Qi Zhang^{1*}, Yanan Hu^{1*}, Cristian Meo¹, Yanbo Wang¹, Andrea Nanetti², Justin Dauwels^{1*}

Abstract—We typically search for images by keywords, e.g., when looking for images of apples, we would enter the word “apple” as query. However, there are limitations. For example, if users input keywords in a specific language, then they may miss results labeled in other languages. Moreover, users may have an image of the object they want to obtain more information about, e.g., a landmark, but they may not know the name of it. In such scenario, word-based search is not adequate, while image-based search would be ideally suited. These needs drive us to develop a purely content-based image search engine, meaning that users can search images with an image as query. Motivated by this use case with numerous applications, in this paper we propose and validate an image query based search engine. The image processing pipeline contains the following modules (Fig. 1): feature extraction, approximate nearest-neighbour search and re-ranking.



Fig. 1. Proposed pipeline. First, features are extracted from the query image. Similarly, such features are also extracted from all images in the database. These features are extracted only once, and are then stored for processing the image-based queries. The feature extractor comprises a CNN, followed by an aggregation layer, a whitening layer and an L2 normalization layer, which can be trained end-to-end with various loss functions. The extracted features are then forwarded to an approximate nearest-neighbour search module to produce the initial ranking results, which are next refined by a re-ranking module, generating the final results.

Feature extraction is the cornerstone of an image retrieval system. In this paper, ResNet101 is selected as the backbone of the extractor. In order to obtain more discriminative and compact representations of the target image, GeM Pooling [1] is employed as aggregation methods. After processing by the GeM pooling layer, the feature maps are reduced to one global descriptor. Besides the extraction procedure design, the optimisation of the loss function also needs to be considered. Most work in image retrieval considers pairwise (e.g., contrastive) or tuplewise (e.g., triplet-based, n-tuple-based) loss functions. Both methods train the model by learning the corresponding distances between the positive and negative and the target. However, these methods show limitations in the cluster distribution when processing hard positive images. In this paper, we applied the second-order similarity loss [2] combined with above loss functions to optimize clusters and explore better model learning mechanisms.

Once we obtain the feature vectors, the image retrieval problem becomes a nearest neighbour search problem: finding the relevant images is then finding the database vectors that are close to the query vector. A trivial way is linear scan, which has linear search complexity and may lead to unacceptable

time costs when the database is very large. Therefore, approximate nearest-neighbour (ANN) search methods are proposed to achieve sub-linear complexity, which mainly fall into two categories: compression-based and graph/tree-based. Compression-based methods aim to encode the vector into a much more compact representation, and graph/tree-based methods enable us to calculate and compare distances between only a small portion of the database vectors and the query vector. However, these two types of approaches are usually not discussed and compared together. Also, the possibility of combining them together has not been fully studied. In this paper, we apply methods in both categories, e.g., product quantization [3] and hierarchical navigable small world [4], and explore how to get the best of both worlds.

After the ANN search, the engine outputs the preliminary results of top-K images. However, these results are not robust when there are illumination and viewpoint changes in images. Therefore, we need to implement reranking. The reranking can be divided into two types: global and local feature based reranking. The global feature represents an image with a single feature vector. The global feature based reranking uses the global features from the previous feature extraction to obtain more representative features and implements reranking. By contrast, the local feature represents an image with a multidimensional feature matrix. The local feature based reranking extracts local features of images, calculates the geometric similarity and implements reranking. The global feature based reranking is faster, while the local feature based reranking can provide pixel-to-pixel similarity analysis. However, previous researchers spend little attention to reranking. Therefore, we propose and apply accurate and efficient global and local feature based reranking (Diffusion and SIFT) [5], [6] at a small speed cost.

The most important contribution of this paper is to provide a fine-grained instance-level search engine that can be applied in real-world applications. The system is highly modular and therefore flexible, allowing for easier adaptation to requirements, striking a balance between speed and accuracy. Extensive tests on various datasets have shown that our pipeline achieves state-of-the-art results across the public benchmarks with acceptable time costs.

REFERENCES

- [1] Radenović, Filip and Tolias, Giorgos and Chum, Ondřej, “Fine-tuning CNN image retrieval with no human annotation,” *IEEE transactions on pattern analysis and machine intelligence*, vol. 41, 2018, pp.1655–1668.
- [2] Ng, Tony and Balntas, Vassileios and Tian, Yurun and Mikolajczyk, Krystian, “SOLAR: second-order loss and attention for image retrieval,” *European Conference on Computer Vision*, 2020, pp.253–270.
- [3] Jegou, Herve and Douze, Matthijs and Schmid, Cordelia, “Product quantization for nearest neighbor search,” *IEEE transactions on pattern analysis and machine intelligence*, vol. 33, 2010, pp.117–128.
- [4] Malkov, Yu A and Yashunin, Dmitry A, “Efficient and robust approximate nearest neighbor search using hierarchical navigable small world graphs,” *IEEE transactions on pattern analysis and machine intelligence*, vol. 42, 2018, pp.824–836.
- [5] F. Yang, R. Hinami, Y. Matsui, S. Ly, and S. Satoh, “Efficient image retrieval via decoupling diffusion into online and offline processing,” 2018.
- [6] D. Lowe, “Object recognition from local scale-invariant features,” in *Proceedings of the Seventh IEEE International Conference on Computer Vision*, vol. 2, pp. 1150–1157 vol.2, 1999.




*These authors contributed equally to the work

¹Department of Microelectronics, Delft University of Technology

²School of Art, Design and Media, Nanyang Technological University

*Email: J.H.G.Dauwels@tudelft.nl

Dramco Uno: A Low-Entry IoT Learning Platform for STE(A)M-Oriented Education

Guus Leenders , Geoffrey Ottoy , Gilles Callebaut 
KU Leuven, ESAT-DRAMCO, Ghent Technology Campus
Ghent, Belgium
name.surname@kuleuven.be

The rise of "Industry 4.0" relies heavily on automation and data exchange: core parts of the Internet of Things (IoT) revolution. This results in an increased demand for engineers skilled in IoT development. Research shows that Science Technology Engineering Arts and Mathematics (STEAM) students have limited experience in designing or implementing IoT solutions [1]. To facilitate the need for more IoT related education in STEAM oriented classrooms, we introduce a low-entry learning platform for IoT applications: the Dramco Uno.

The Dramco Uno platform comprises an open-source Arduino compatible microcontroller platform with additional Long Range Wide Area Network (LoRaWAN) communication and three generic sensors. In addition to the hardware platform, we have developed clear and easy-to-follow learning materials for enabling low-entry cloud connections¹.

Since the arrival of the Arduino Uno, fast prototyping platforms have gained traction in educational settings, maker communities and research environments [2]. Supported by a vibrant community, a plethora of libraries have been developed for a large array of possible extensions. We capitalize on this trend by making the Dramco Uno platform fully Arduino compatible: using the Microchip ATMEGA328P microcontroller with additional on-board serial programming circuitry.

The Dramco Uno board extends the standard Arduino Uno by including a LoRaWAN modem for wireless communication (*SX1276-based LoRa transceiver*) and several generic sensors: temperature (*Texas Instruments LMT85*), light (*Vishay BPW34*) and 3-axis motion (*STMicroelectronics LIS2HH12*). When selecting components, careful consideration has been given to low-cost and low-power components with straightforward, low-entry interfaces. This results in a compromise between energy consumption and cost efficiency throughout the Dramco Uno design. The Arduino power circuitry has been redesigned to allow for low-power deep sleep operation. In deep-sleep, all peripherals are powered down to achieve a power consumption of only 25.85 μ W, prolonging battery life dramatically as opposed to the Arduino Uno boards.

To support low-effort application development, we provide a comprehensive library for controlling power circuitry and

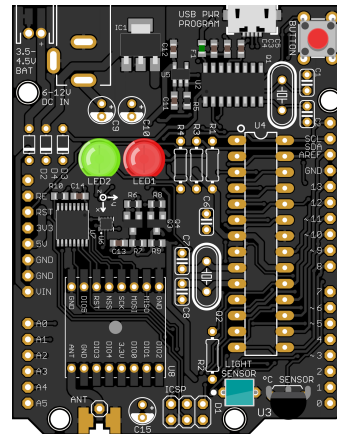


Fig. 1: Render of the Dramco Uno hardware.

interfacing with all peripherals. This library includes the LoRaWAN Medium Access Control (MAC) interface.

The Dramco Uno is being used in various stages of the electronics/ICT engineering course at KU Leuven, Ghent. Firstly, as introduction to electronics, students get to solder all through hole components on their own Dramco Uno board. Secondly, various programming and IoT sessions introduce students to low-entry programming and IoT application development.

REFERENCES

- [1] J. He, D. C.-T. Lo, Y. Xie, and J. Lartigue, "Integrating Internet of Things (IoT) into STEM undergraduate education: Case study of a modern technology infused courseware for embedded system course," in *2016 IEEE frontiers in education conference (FIE)*. IEEE, 2016, pp. 1–9.
- [2] B. Thoen, G. Callebaut, G. Leenders, and S. Wielandt, "A deployable LPWAN platform for low-cost and energy-constrained IoT applications," *Sensors*, vol. 19, no. 3, p. 585, 2019.

¹Open-source hardware, firmware and learning materials are available at dramco.be/uno

Surface Electrocardiogram Reconstruction Using Intra-operative Electrograms

Hanie Moghaddasi

Circuits and Systems

Delft University of Technology
Delft, The Netherlands

H.moghaddasi@tudelft.nl

Borbála Hunyadi

Circuits and Systems

Delft University of Technology
Delft, The Netherlands

B.Hunyadi@tudelft.nl

Alle-Jan van der Veen

Circuits and Systems

Delft University of Technology
Delft, The Netherlands

A.J.vanderVeen@tudelft.nl

Natasja M.S. de Groot

Department of Cardiology

Erasmus Medical Center
Rotterdam, The Netherlands

N.m.s.degroot@erasmusmc.nl

Richard C. Hendriks

Circuits and Systems

Delft University of Technology
Delft, The Netherlands

R.C.Hendriks@tudelft.nl

ABSTRACT

Atrial Fibrillation (AF) is the most sustained arrhythmia in the heart. On the surface electrocardiogram (ECG), AF is characterised by the irregular RR intervals and by fibrillatory waves or the absence of a P wave. Since AF is a progressive disease, timely and correct detection is crucial for AF treatment. Detailed insight into the areas of arrhythmia-related electropathology can be obtained by analyzing high-resolution (inter-electrode distance 2mm) electrograms (EGMs). However, these measurements are rather invasive. By integration of high-resolution epicardial mapping data and surface ECG data, we hope to learn how different stages of AF represent themselves on the ECG. Eventually this can help to guide to identify areas of electropathology as target sites of ablation therapy on the less invasive ECG. A first step in this direction is to learn how to reconstruct the ECG based on EGM measurements. In practice, however, EGMs are only measured at few atrial locations, not covering the complete atria. An important question therefore is: How can we reconstruct ECG based on the observations from a limited part of the heart? To answer this question, we propose two methods. In the first method, we increase the number of observations from a part of the right atrium (RA) to the whole RA by synchronizing EGMs that are measured at different moments in time based on the local activation time (LAT). In the second method, under the assumption that atrial EGMs measured at different spatial areas are linearly related, the conductivity matrix is estimated for the whole atrium which enables us to reconstruct the ECGs from the limited observations. The second method brings twofold benefits. First, the conductivity matrix can be used as a novel diagnostic tool to detect AF as well as areas of electropathology. Second, it provides a practical solution to reconstruct epicardial potentials from ECGs, non-

invasively. The results show that method one increases the reconstruction accuracy. Furthermore, the conductivity matrix reveals the structural differences between sinus rhythm (SR) and AF episodes which could be the first step to interpret the underlying electropathology of AF.

This research was funded in part by the Medical Delta Cardiac Arrhythmia Lab (CAL), the Netherlands.

Feasibility of CSMA/NDA protocol for wireless systems using On-Off Keying

Mehmet Fatih AYTEN
*Faculty of Engineering
Vrije Universiteit Brussel
Brussels, Belgium
mehmet.fatih.ayten@vub.be*

François QUITIN
*Brussels School of Engineering
Université Libre de Bruxelles
Brussels, Belgium
fquitin@ulb.be*

Abstract—This paper presents a wireless implementation of the Carrier Sense Multiple Access/Non Destructive Arbitration (CSMA/NDA) protocol using software-defined radios (SDR). The CSMA/NDA is a broadcast medium allocation protocol that is used in cabled industrial Control Area Networks (CANs), and offers real-time performance of broadcast buses as it allows to preempt collisions on the medium through an arbitration process. CSMA/NDA relies on two properties of the physical medium: 1) the ability to realize full-duplex transceivers and 2) a physical implementation of dominant and recessive bits, both of which are hard to achieve with wireless systems. So far, CSMA/NDA has been limited to cabled network that rely on differential voltage transmissions. In this paper we demonstrate that it is possible to implement the CSMA/NDA protocol using On-Off Keying (OOK) modulation with a wireless system. We provide a proof-of-concept implementation of the CSMA/NDA protocol on a SDR testbed.

Index Terms—Wireless systems, CSMA/NDA, Controller Area Network (CAN), software defined radios

I. INTRODUCTION

In order to avoid packet collisions in multi-emitter broadcast wireless networks, different collision avoidance protocols are used in wireless standards. The most well-known is Collision Sense Multiple Access with Collision Avoidance (CSMA/CA), which allows emitters to detect collision when no acknowledgement (ACK) frame is received from the receiver. However, in heavily-loaded wireless networks, CSMA/CA comes with a distinct waste of bandwidth usage, as collisions are only detected when no ACK frame is received. The probabilistic nature of CSMA/CA in most implementations also makes it unsuitable for industrial real-time networks with hard latency constraints.

One common real-time protocol for cabled broadcast bus networks is the Control Area Network (CAN) protocol. The CAN protocol has been adopted by many industries, and more particularly by the automotive industry. The CAN protocol offers many advantages like fast transmission speed, reliability and robustness; therefore, it is commonly used in real-time applications [1]. The CAN protocol relies on the Carrier Sense Multiple Access/Non Destructive Arbitration (CSMA/NDA) protocol, which offers significant advantages over CSMA/CA in terms of latency and channel usage. However, design and setup of traditional CAN buses can be demanding because of physical wires. Wireless implementation of CAN buses introduces new challenges such as data reliability, latency, power,

and cost. There has been some research on this area to reduce these complications [2]. One of the main reasons that make CAN implementations difficult for wireless transceivers is the impossibility of realizing a full-duplex transceiver. Indeed, the CSMA/NDA protocol requires a bit-by-bit comparison between the transmitted signal and the signal read on the communication bus. A second problem of the CSMA/NDA protocol is that it relies on a dominant and recessive bit mechanisms, which is implemented using differential transmissions in cabled network, but which is harder to realize in wireless systems.

In this paper, we propose an adaptation of the CSMA/NDA protocol for wireless transceivers, and demonstrate it's feasibility on a software-defined radio (SDR) testbed. To overcome the complexity of realizing a full-duplex transceiver, we propose to use On-Off Keying (OOK) during the arbitration phase of the CSMA/NDA protocol, which allows to detect channel usage, even without the use of a full-duplex transceiver.

II. CSMA/NDA PROTOCOL

A. CSMA/NDA protocol in CAN buses

Carrier Sense Multiple Access/Non Destructive Arbitration (CSMA/NDA) is a protocol that is used in Layer 2 (Data Link Layer) of Control Area Networks (CANs). The CSMA part is similar to other CSMA protocols: if the channel is being used, a node that wants to transmit will wait for the channel to become available. If more than one node wants to transmit once the channel becomes available, a collision will occur.

The NDA protocol relies on the concept of dominant and recessive bits. If one node transmits a dominant bit and another node transmit a recessive bit, the nodes will all see a dominant bit on the channel. In the NDA protocol, each nodes that wants to transmit starts by sending an arbitration field (which is similar to the node ID). Each node will then do a bit-by-bit comparison of it's transmitted bits, and the bits the node measures on the channel. If the node is sending a recessive bit, but is seeing a dominant bit on the channel, it will detect a concurrency and stop it's transmission immediately. At the end of the arbitration field (12 bits in the case of a CAN bus), only one node should still be transmitting. An illustration of the CSMA/NDA protocol with three nodes is shown in Figure 1.

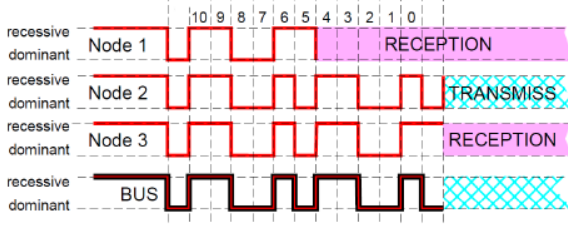


Fig. 1. Example of the CSMA/NDP protocol with three nodes on the bus. At the end of the arbitration field, nodes 1 and 3 stopped their transmission, and only node 2 is still transmitting.

In a CAN bus, the dominant bits are created by imposing a differential voltage on the bus through two pair of CMOS transistors, while recessive bits are set to a zero-differential voltage through a pair of resistive dividers. In this paper, we propose to use OOK to set dominant and recessive bits. The additive properties of the wireless channel will make the On-bit (dominant bit) visible to all nodes that transmit an Off-bit (recessive bit).

B. CSMA/NDP protocol in wireless networks

Wireless transceivers have trouble implementing CSMA/NDP because:

- a full-duplex transceiver is required to perform a bit-by-bit comparison, which is difficult for wireless systems, as the transmitted signals tends to blind the receiver in the same time-frequency band;
- a dominant and recessive bit system needs to be implemented, which is non-trivial for wireless transceivers.

Both of these problems are solved by using On-Off Keying (OOK) modulation for the arbitration field, which implicitly solves both problems. OOK modulation relies on sending a pilot tone to indicate a high bit (on-signal), and to transmit nothing for a low bit (off-signal). When one transmitters transmits a high bit (on-signal) and another transmitter sends a low bit (off-signal), the signal on the wireless channel will be the high bit (on-signal) due to the superposition properties of wireless channels. Therefore, OOK modulation inherently implements a dominant and recessive bit transmission system. The OOK modulation also solves the full-duplex transceiver problem: when the transceiver is sending a low bit (off-signal), it's receiver is no longer blinded by it's transmitted signal, allowing for a bit-by-bit comparison of the transmitted and received signal. When transmitting a high-bit, the transceiver's receiver is blinded by it's own on-signal, but this does not matter for the implementation of the CSMA/NDP protocol.

III. EXPERIMENTAL SETUP AND RESULTS

A. Experimental Setup

The devices used in our experiments are two USRP X310 SDRs [5] in order to implement communications and protocol implementation, one OctoClock CDA-2990 Clock Distribution Device [5] in order to maintain synchronization between

SDRs, one Gigabit ethernet switch in order to make connections between the PC and the SDRs. Wireless communication between SDRs has been maintained using VERT2450 Vertical Antennas [5]. Experiments have been conducted in real-time on the host PC using the GNU Radio framework [4]. In each USRP X310 SDR, one transceiver node has been created by using two antennas. All relevant parameters of the setup and simulation are given in Table I. Since all decisions are made in real-time on the host laptop, the achievable latencies are high and the resulting data rate is quite low. We want to emphasize that this limit is not a fundamental limit of our CSMA/NDP implementation, and could be solved by moving to a full FPGA implementation, allowing for much higher data rates. Figure 2 shows the experimental setup and Figure 3 shows the block diagram of CSMA/NDP implementation on one Tx node used for experiments.

TABLE I
EXPERIMENTAL SETUP PARAMETERS

Parameter	Value
Sampling Rate	196 kHz
Center Frequency	2.45 GHz
Bandwidth	196 kHz
Data Rate	1 kbps
Arbitration Field Length	4 bits



Fig. 2. Experimental setup

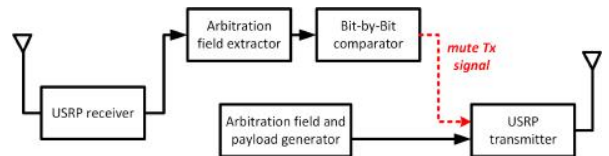


Fig. 3. Block Diagram of CSMA/NDP implementation on one transceiver node

The CSMA/NDP protocol has been tested using randomly generated bits whose first 4 bits are assigned as the arbitration field and the rest are random bits (representing the payload). In the arbitration field, the dominant bit has been decided as '1' and the recessive bit has been decided as '0'. In order to determine the data rate, generated bits have been first interpolated; then, they have been transmitted with carrier sinusoid of 2 kHz.

After receiving bits from the Rx node, Tx nodes compare the sent and received bits, if sent and received bits are equal, the related Tx node continues transmitting; otherwise, it becomes silent, i.e., it starts transmitting '0's. For this comparison, we have used a custom block in GNU Radio. According to result of the comparison, this block sends a command to the message port of the USRP transmitter block. In order to make the USRP transmitter block silent, its gain is set to 0 dB. As a result, the contribution from the silent transmitter never disappears but it is low enough to distinguish between recessive and dominant nodes. We have used the Threshold block in the GNU Radio block diagram in order to decide on bits according to received waveforms. The value of a threshold is specific for each receiver and the threshold is determined by activation of two different transmitters one by one and exploiting the received waveform.

B. Results

During experiments, four different arbitration fields are utilized: [1 1 1 1] (1st highest priority), [1 1 1 0] (2nd highest priority), [1 1 0 0] (3rd highest priority) and [1 0 0 0] (4th highest priority). All possible two combinations of arbitration fields scenarios have been tested and two of these tests will be illustrated and explained.

In the first test, a bit stream whose arbitration field is [1 1 0 0] has been sent from the Tx1. From Tx2, a bit stream whose arbitration field is [1 1 1 0] has been sent. Therefore, we expect Tx2 to continue transmitting; whereas, Tx1 to become silent by setting its gain to 0 dB. In order to validate both waveform addition and decide on the threshold, first, two transmitters have been activated one by one. Then, both transmitters have been activated simultaneously in order to validate CSMA/NDA. Meanwhile, received waveforms on Rx1 and Rx2 have been saved. Figure 4 shows received waveforms on Rx1 when different Tx nodes are activated, likewise Figure 5 illustrates received waveforms on Rx2.

As it can be seen from Fig. 4 and Fig. 5, between 0.1786 ms and 4.1786 ms, the Tx nodes send their arbitration fields. The received waveform is a still sum (bit-wise OR) of the transmitted waveforms. Therefore, after thresholding, both transceivers detect the first four bits to be [1 1 1 0]. After arbitration field decision, both transceivers start the operation of comparison. During the comparison of sent and received bits (between 4.1786 ms and 84.1786 ms), the transmission continues; therefore, the effect of the custom block appears after a while. During the comparison, waveforms coming from transmitters are added; therefore, observed waveform is bit-wise OR result of random bits. The elapsed time until the recessive Tx1 node becomes silent is 84 ms. This is mainly due to the full-software implementation, and this elapsed time could become close to 0 on a full FPGA implementation. Since the data rate is 1 kbps, after the 84th bit, the CSMA/NDA has been successfully activated. Therefore, starting from 84.1786 ms (corresponds to 85th bit), the received bit stream is the one from Tx2 which is the dominant transmitter. As an example for validation of silence of Tx1, between 84.1786 ms and 85.1786

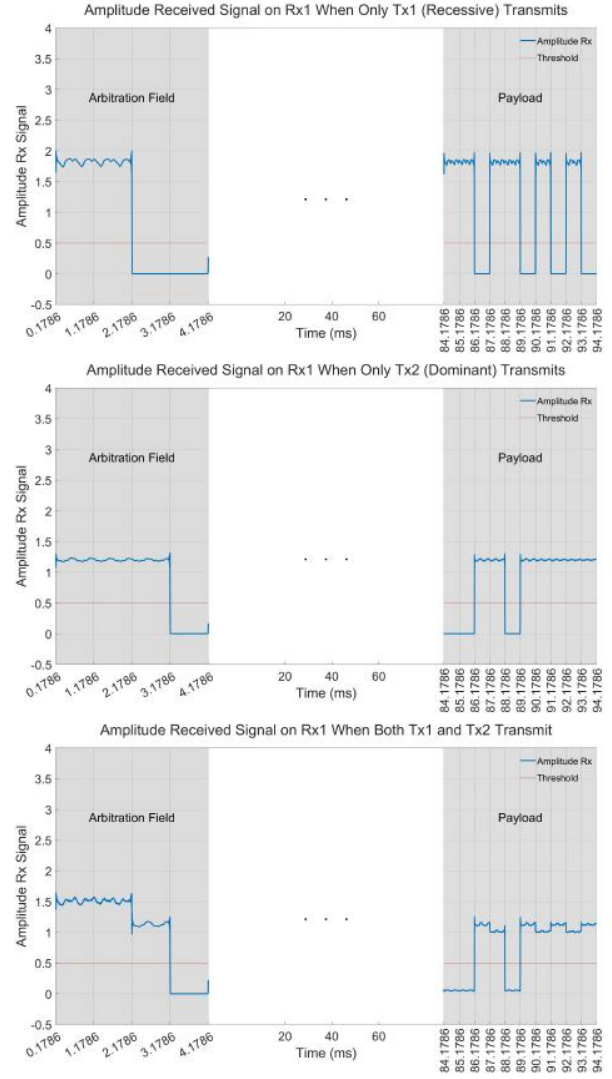


Fig. 4. Test 1: Received waveforms on Rx1 when different Tx nodes are activated

ms, Tx1 transmits 1 but since Tx1 has already become silent, we received 0 at the Rx.

In the second test, a bit stream with arbitration field is [1 0 0 0] has been sent from the Tx1; while, from Tx2, a bit stream with arbitration field is [1 1 1 1] has been sent. We have expected Tx2 to continue transmitting; whereas, Tx1 to become silent by setting its gain to 0 dB since it is of a lower priority. The similar procedures in the first test have been followed and waveforms have been received. Figure 6 shows received waveforms on Rx1 when different Tx nodes are activated, likewise Figure 7 illustrates received waveforms on Rx2.

From Fig. 6 and Fig. 7, one can conclude that since [1 1 1 1] is the highest priority arbitration field and [1 0 0 0] is the 4th, starting from 85th bit, the received bit stream is the exactly one from Tx2.

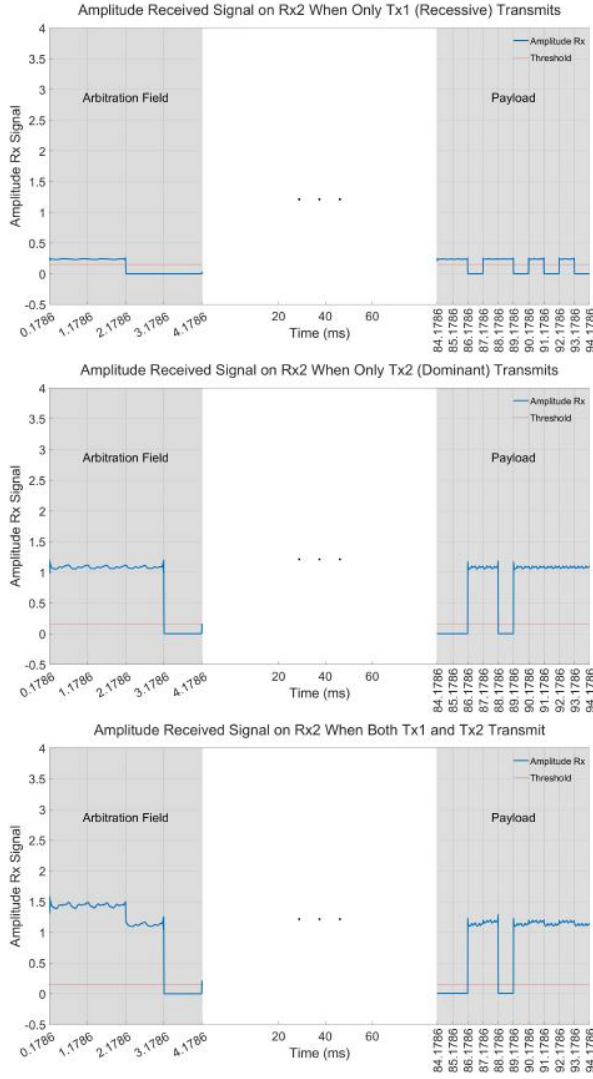


Fig. 5. Test 1: Received waveforms on Rx2 when different Tx nodes are activated

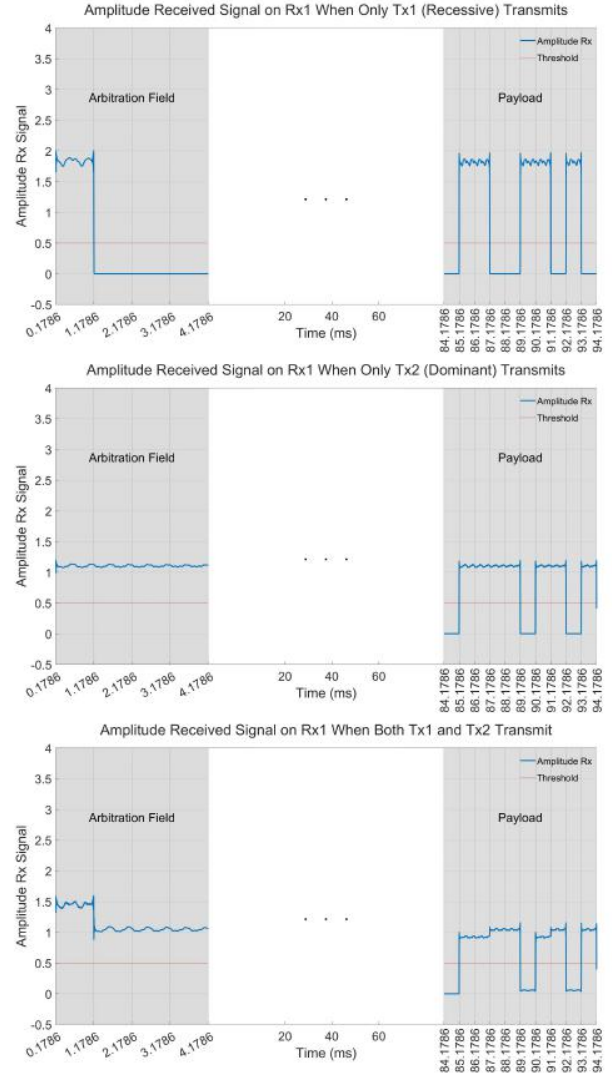


Fig. 6. Test 2: Received waveforms on Rx1 when different Tx nodes are activated

IV. CONCLUSION

This work introduces a way of implementing CSMA/NDA using On-Off Keying modulation on wireless transceivers. Our SDR implementation shows that with OOK, waveforms can be successfully summed at the any transceiver node; therefore it possible to control the bit stream to be sent by interpreting the received arbitration field information. This implementation has been tested using two transceivers. Detailed bit-by-bit presentation of CSMA/NDA protocol with our SDR testbed has been explained with two different arbitration field scenarios. The delay performance of the system has also been investigated. When the testbed is fully moved to FPGA implementation, performance of the protocol would be better.

REFERENCES

- [1] H. Chen and J. Tian, "Research on the Controller Area Network," 2009 International Conference on Networking and Digital Society, 2009, pp. 251-254, doi: 10.1109/ICNDS.2009.142.
- [2] M. Laifenfeld and T. Philosof, "Wireless controller area network for in-vehicle communication," 2014 IEEE 28th Convention of Electrical & Electronics Engineers in Israel (IEEEI), 2014, pp. 1-5, doi: 10.1109/IEEEI.2014.7005751.
- [3] Z. Tong, M. S. Arifanto and C. F. Liao, "Wireless transmission using universal software radio peripheral," 2009 International Conference on Space Science and Communication, 2009, pp. 19-23, doi: 10.1109/ICONS.2009.5352678.
- [4] GNU radio, <https://www.gnuradio.org/>, 2022.
- [5] USRP products, <http://www.ettus.com>, 2022.

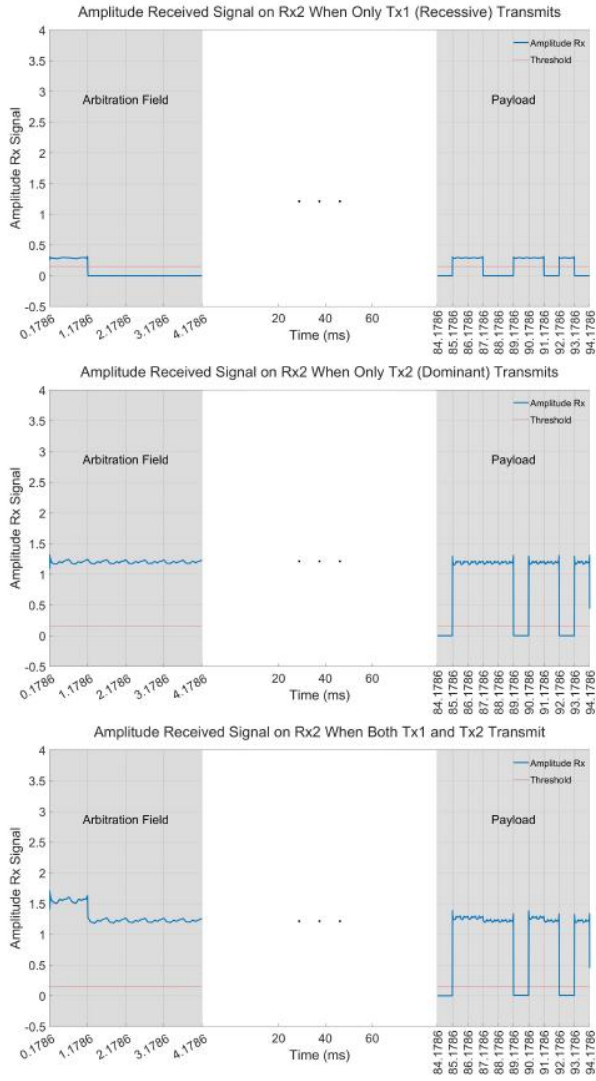


Fig. 7. Test 2: Received waveforms on Rx2 when different Tx nodes are activated

Papers not appearing in the proceedings

The following papers wished not to appear in the proceedings (usually for copyright reasons):

Joint Estimation of Parameters in a Cardiac Tissue Model Using Confirmatory Factor Analysis

Miao Sun, Natasja M.S. de Groot, Richard C. Hendriks

Estimation of Atrial Fibre Direction Based on Activation Maps

Johannes W. de Vries, Richard C. Hendriks and Miao Sun

Finite Impulse Response Filters for Simplicial Complexes

Maosheng Yang, Elvin Isufi, Michael T. Schaub, Geert Leus

Wi-Fi-based passive radars for crowd monitoring

Martin Willame, Jérôme Louveaux, François Horlin

Adaptive Map Matching Based on Dynamic Word Embeddings for Indoor Positioning

Xinyue Lan, Lijia Zhang, Zhuoling Xiao, Bo Yan

Dynamic Bi-Colored Graph Partitioning

Yanbin He, Mario Coutino, Elvin Isufi, Geert Leus

Characterisation and Cancellation of Interference with Multiple Phase-coded FMCW Dual-Function RADAR Communication Systems

François De Saint Moulin, Claude Oestges, Luc Vandendorpe

Single-Pulse Estimation of Target Velocity on Planar Arrays

Costas A. Kokke, Mario Coutiño, Richard Heusdens, Geert Leus, Laura Anitori

Learning Time-Varying Graphs from Online Data

Alberto Natali, Elvin Isufi, Mario Coutino, Geert Leus

Sensor-to-cell height estimation for conductivity estimation in cardiac cells

Cees H. Kos, Miao Sun, Richard C. Hendriks

Node Attachment and Filtering on Expanding Graphs

Bishwadeep Das, Elvin Isufi