Tampere University

KAREL PÄRLIN

Multifunction Radios and Interference Suppression for Enhanced Reliability and Security of Wireless Systems

Tampere University Dissertations 859

Tampere University Dissertations 859

KAREL PÄRLIN

Multifunction Radios and Interference Suppression for Enhanced Reliability and Security of Wireless Systems

ACADEMIC DISSERTATION
To be presented, with the permission of
the Faculty of Information Technology and Communication Sciences
of Tampere University,
for public discussion in the Auditorium TB109
of the Tietotalo building, Korkeakoulunkatu 1, Tampere,
on 10th of November 2023, at 12 o'clock.

ACADEMIC DISSERTATION
Tampere University
Faculty of Information Technology and Communication Sciences
Finland

Responsible supervisor and Custos	Associate Professor Taneli Riihonen Tampere University Finland	
Supervisors	Dr.-Ing. Marc Adrat Fraunhofer FKIE Germany	Dr. Ir. Vincent Le Nir Royal Military Academy Belgium
Pre-examiners	Adjunct Assistant Professor Marc Lichtman University of Maryland USA	Professor Aydin Sezgin Ruhr University Bochum Germany
Opponent	Professor Jyri Hämäläinen Aalto University Finland	

Cover design: Roihu Inc.

ISBN 978-952-03-3048-4 (print)
ISBN 978-952-03-3049-1 (pdf)
ISSN 2489-9860 (print)
ISSN 2490-0028 (pdf)
http://urn.fi/URN:ISBN:978-952-03-3049-1

Carbon dioxide emissions from printing Tampere University dissertations have been compensated.

PunaMusta Oy – Yliopistopaino
Joensuu 2023

PREFACE

The work presented in this thesis was carried out during 2018-2021 in Rantelon, Estonia, and during 2021-2023 in Tampere University, Finland, while over time receiving financial support from the Estonian Ministry of Defence, the Research Council of Finland through the projects Multifunctional Radios in Radio-Frequency Systems' Convergence and Radio Shield Against Malign Wireless Communication, the Finnish Scientific Advisory Board for Defence, the Finnish Support Foundation for National Defence, and the Nokia Foundation. Despite the work having been split in this manner, the support from and collaboration with those involved has spanned beyond the time spent in either site, for which I am deeply grateful.

Specifically, I wish to express my gratitude to my supervisors Prof. Taneli Riihonen, Dr.-Ing. Marc Adrat, and Dr. Ir. Vincent Le Nir. They have directly contributed to this work with countless ideas and improvements, but they have also indirectly contributed to its progression by setting examples of the highest standard in all that surrounds the work. I also wish to express my gratitude to the Rantelon collective, especially to Prof. Emeritus Andres Taklaja, Priit Kinks, and Gaspar Karm. They provided the initial platform for this work to develop while continuing to encourage it throughout, and I am privileged to have received their support.

I am also very grateful to Prof. Aydin Sezgin and Dr. Marc Lichtman with whom unfortunately I did not have any contact directly but who acted as pre-examiners for this thesis and helped improve it through their discerning feedback. Additionally, I wish to thank Prof. Jyri Hämäläinen for agreeing to take on the role of the opponent in the public examination of this thesis.

I have been fortunate that this work has been propelled forward by many others, including Matias Turunen and Jaakko Marin with whom I had the pleasure of working together on several publications; Kalev Märtens, Dr. Toomas Ruuben, Timo Truumaa, and Dr. Mari-Anne Meister who helped with access to some of the devices and locations used for measurements presented in this work but also in bringing this

work closer to potential end-users and collaborators; the IST-175 research task group that helped shape many of the ideas presented in this work; the many anonymous reviewers who have contributed to the improvement of this work through peer-review processes as well as the editors who have overseen that; and last, but not least, my parents, Lea and Kalle, who provided me with the very foundation on which the efforts in this work build. I appreciate it all.

Tampere, August 2023
Karel Pärlin

ABSTRACT

Wireless connectivity, with its relative ease of over-the-air information sharing, is a key technological enabler that facilitates many of the essential applications, such as satellite navigation, cellular communication, and media broadcasting, that are nowadays taken for granted. However, that relative ease of over-the-air communications has significant drawbacks too. On one hand, the broadcast nature of wireless communications means that one receiver can receive the superposition of multiple transmitted signals. But on the other hand, it means that multiple receivers can receive the same transmitted signal. The former leads to congestion and concerns about reliability because of the limited nature of the electromagnetic spectrum and the vulnerability to interference. The latter means that wirelessly transmitted information is inherently insecure.

This thesis aims to provide insights and means for improving physical layer reliability and security of wireless communications by, in a sense, combining the two aspects above through simultaneous and same frequency transmit and receive operation. This is so as to ultimately increase the safety of environments where wireless devices function or where malicious wirelessly operated devices (e.g., remote-controlled drones) potentially raise safety concerns. Specifically, two closely related research directions are pursued. Firstly, taking advantage of in-band full-duplex (IBFD) radio technology to benefit the reliability and security of wireless communications in the form of multifunction IBFD radios. Secondly, extending the self-interference cancellation (SIC) capabilities of IBFD radios to multiradio platforms to take advantage of these same concepts on a wider scale.

Within the first research direction, a theoretical analysis framework is developed and then used to comprehensively study the benefits and drawbacks of simultaneously combining signals detection and jamming on the same frequency within a single platform. Also, a practical prototype capable of such operation is implemented and its performance analyzed based on actual measurements. The theoretical and

experimental analysis altogether give a concrete understanding of the quantitative benefits of simultaneous same-frequency operations over carrying out the operations in an alternating manner. Simultaneously detecting and jamming signals specifically is shown to somewhat increase the effective range of a smart jammer compared to intermittent detection and jamming, increasing its reliability.

Within the second research direction, two interference mitigation methods are proposed that extend the SIC capabilities from single platform IBFD radios to those not physically connected. Such separation brings additional challenges in modeling the interference compared to the SIC problem, which the proposed methods address. These methods then allow multiple radios to intentionally generate and use interference for controlling access to the electromagnetic spectrum. Practical measurement results demonstrate that this effectively allows the use of cooperative jamming to prevent unauthorized nodes from processing any signals of interest, while authorized nodes can use interference mitigation to still access the same signals. This in turn provides security at the physical layer of wireless communications.

CONTENTS

List of Figures

ABBREVIATIONS

ADC	analog-to-digital converter
AGC	automatic gain control
AWGN	additive white Gaussian noise
BER	bit error rate
BFSK	binary frequency-shift keying
CNN	convolutional neural network
CR	cognitive radio
DAC	digital-to-analog converter
DSSS	direct-sequence spread spectrum
EMSE	excess mean-square error
EW	electronic warfare
FD	full-duplex
FHSS	frequency-hopping spread spectrum
FO-LMS	frequency offsets least mean squares
GNSS	global navigation satellite system
GPS	Global Positioning System
HD	half-duplex
IBFD	in-band full-duplex
ISM	industrial, scientific, and medical
JSR	jammer-to-signal ratio
KI	known interference

KIC	known-interference cancellation
LMS	least mean squares
LNA	low-noise amplifier
LPI	low probability of intercept
MSE	mean squared error
PA	power amplifier
RF	radio-frequency
ROC	receiver operating characteristic
SF-STAR	same-frequency simultaneous transmit and receive
SI	self-interference
SIC	self-interference cancellation
SINR	signal-to-interference-plus-noise ratio
SNR	signal-to-noise ratio
SoI	signal of interest

ORIGINAL PUBLICATIONS

P1 K. Pärlin and T. Riihonen. Digitally Assisted Analog Mitigation of Narrowband Periodic Interference. *Proc. Int. Symposium on Wireless Communication Systems*. Aug. 2019, 682–686. DOI: 10.1109/ISWCS.2019.8877336.

P2 K. Pärlin and T. Riihonen. Analog Mitigation of Frequency-Modulated Interference for Improved GNSS Reception. *Proc. Int. Conference on Localization and GNSS*. June 2020. DOI: 10.1109/ICL-GNSS49876.2020.9115518.

P3 K. Pärlin, T. Riihonen, G. Karm and M. Turunen. Jamming and Classification of Drones Using Full-Duplex Radios and Deep Learning. *Proc. Int. Symposium on Personal, Indoor and Mobile Radio Communications*. Sept. 2020. DOI: 10.1109/PIMRC48278.2020.9217351.

P4 K. Pärlin, T. Riihonen, V. Le Nir, M. Bowyer, T. Ranström, E. Axell, B. Asp, R. Ulman, M. Tschauner and M. Adrat. Full-Duplex Tactical Information and Electronic Warfare Systems. *IEEE Communications Magazine* 59.8 (Aug. 2021), 73–79. DOI: 10.1109/MCOM.001.2001139.

P5 K. Pärlin, T. Riihonen, V. Le Nir and M. Adrat. Estimating and Tracking Wireless Channels under Carrier and Sampling Frequency Offsets. *IEEE Transactions on Signal Processing* 71 (Mar. 2023), 1053–1066. DOI: 10.1109/TSP.2023.3259140.

P6 K. Pärlin, T. Riihonen, V. Le Nir and M. Adrat. Physical-Layer Reliability of Drones and Their Counter-Measures: Full vs. Half Duplex. *IEEE Transactions on Wireless Communications* (2023). In press. DOI: 10.1109/TWC.2023.3290257.

P7 K. Pärlin, T. Riihonen, M. Turunen, V. Le Nir and M. Adrat. Known-Interference Cancellation in Cooperative Jamming: Experimental Evalua-

tion and Benchmark Algorithm Performance. *IEEE Wireless Communications Letters* (2023). In press. DOI: 10.1109/LWC.2023.3284006.

Author's contribution

The work in this thesis was carried out by the author under the supervision of Prof. Taneli Riihonen, Dr.-Ing. Marc Adrat, and Dr. Ir. Vincent Le Nir who, together with all other coauthors, played key roles in the work's progress. This compilation thesis consists of a summary that is based on the attached peer-reviewed journal papers **[P5, P6, P7]**, a magazine article **[P4]**, and conference papers **[P1, P2, P3]**. The author of this thesis was the leading author in all of the attached publications **[P1-P7]**. That is, the author developed the algorithms as well as the theoretical frameworks therein, performed simulations and numerical analyzes, prepared the measurement setups, carried out and analyzed the measurements, and led the writing of the manuscripts. Other authors provided invaluable guidance throughout these steps as well as assisted in presenting the works by proof-reading the manuscripts and providing the feedback to improve them.

In addition to the attached publications, there are several additional works on the same topic, specifically **[1, 2, 3, 4, 5, 6, 7, 8, 9]**, that the author has contributed to during the thesis work. Furthermore, **[P5]** is accompanied by an open-source implementation for use within the GNU Radio framework[1] and **[P7]** is associated with a comprehensive dataset that is published in **[10]**.

[1] An implementation of the algorithm is open-sourced at `https://github.com/karel/gr-adapt`

1 INTRODUCTION

1.1 Motivation

Wireless connectivity is a key technological enabler that facilitates many of the practical applications, such as satellite navigation, cellular communication, and media broadcasting, that are nowadays taken for granted. And, the reliance on wireless connections is steadily increasing as more and more applications, e.g., sensor and drone networks, take advantage of the relative ease of sharing information over the air. All of the mentioned examples would be difficult to imagine, or at least implement, with wired connections. However, that relative ease of over-the-air communications has its drawbacks.

On one hand, the broadcast nature of wireless communications means that multiple receivers can receive the same transmitted signal, but on the other hand, it means that one receiver can receive the superposition of multiple transmitted signals. The former results in considerable concern for the security of wirelessly transmitted information because of the susceptibility to eavesdropping, while the latter causes concern about robustness and congestion because of the vulnerability to interference and the limited nature of the electromagnetic spectrum. The increasing reliance on wireless connectivity is only amplifying those concerns.

Since many of the applications that rely on wireless connectivity involve cyber-physical systems that interact with the physical world around them, these concerns not only affect the security and reliability of information, but also the physical safety of the systems' surroundings **[2, 6]**. In order to ensure safety in the environments where wireless systems operate or where wirelessly operated devices could be used with malicious intent, it is therefore vital to have the insight on how significant is the impact of security and reliability on safety, but also to have the means to alleviate the security, reliability, and safety concerns.

1.2 Objective and Main Contributions

The main objective of this thesis is to provide the insight and means for improving the safety of environments where wireless devices function or where malicious wirelessly operated devices can potentially raise safety concerns (as illustrated in Fig. 1.1). Or, in other words, to gain dominance in the electromagnetic spectrum and translate that to improved safety in the physical domain, e.g., when countering remotely-controlled drones. To that end, two closely related research directions are targeted: taking advantage of in-band full-duplex (IBFD) radio technology to benefit security and reliability of wireless communications in the form of multifunction IBFD radios; and extending the self-interference cancellation (SIC) capabilities of IBFD radios to multi-radio platforms on a wider scale.

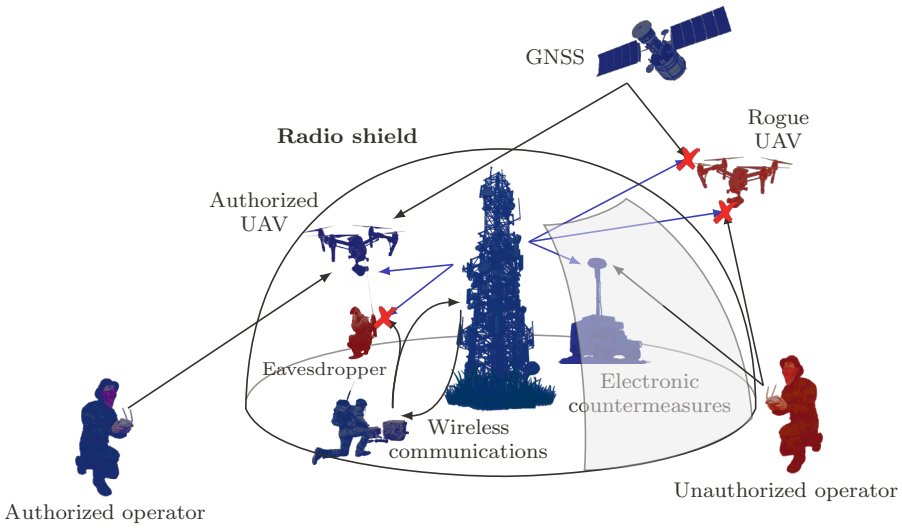


Figure 1.1 Idealized concept for protection from cyber-physical threats — a radio shield.

Typical wireless nodes are incapable of simultaneously transmitting and receiving on the same frequency because of the inevitable self-interference (SI) that any such attempt results in [11]. Still, seemingly full-duplex (FD) two-way communication is achievable by separating the transmission and reception in either time or frequency. However, these approaches take twice the resources that true FD operation would. Motivated by the promise of doubling the spectral efficiency of wireless communications, recent research has led to sufficient SI cancellation capabilities, making true

FD radio technology, or IBFD radio technology, a viable solution [12]. Various benefits have also been envisioned for multi-radio systems that could suppress interference across nodes instead of within a single node, but doing so is a more complex challenge that has yet to receive the same level of attention as SIC [13].

As such, the specific objectives within the two research directions are as follows. Firstly, finding out the extent that advances in SIC and the feasibility of IBFD operation mode can be used for combining radio functions other than information transmission and reception on a single platform in the form of multifunction radios and what is the resulting impact on the reliability and security of these systems. Secondly, developing interference cancellation methods that allow to extend the IBFD radio concept from a single radio to multiple radios, so that interference across radios can be canceled. And also, studying the impact that such capability can have in practice on the security of wireless communication systems.

The main contributions of this thesis are:

- A theoretical framework for studying the impact of half-duplex (HD) and FD operation modes in counter-drone scenarios along with a detailed comparison highlighting the benefits of either mode [**P6**] and an overview of the impact that IBFD operation can have on tactical information and electronic warfare systems [**P4**].
- A deep learning-based method for detecting and classifying signals, along with measurements-based analysis of its performance when simultaneously interfering and detecting drone remote control signals in IBFD mode [**P3**].
- A digitally assisted analog interference mitigation scheme for suppressing periodic interference in co-existing interferer and receiver scenarios where powerful interference needs to be handled in the analog domain so as to avoid quantization noise from masking any weak signals of interest [**P1**]. A study of the scheme's performance for improving global navigation satellite system (GNSS) reception [**P2**].
- An adaptive frequency offsets least mean squares (FO-LMS) filter capable of simultaneously and explicitly estimating and tracking a wireless channel as well as carrier and sampling frequency offsets[1] [**P5**] and an extensive study of its performance in the context of cooperative jamming [**P7**].

[1] An implementation of the algorithm is open-sourced at `https://github.com/karel/gr-adapt`

- An extension of the well-known energy conservation relation method to facilitate analyzing the steady-state performance of adaptive filters with self-induced nonstationarity, such as the proposed FO-LMS [**P5**].

Altogether, these contributions provide a much improved understanding on when and how IBFD radio technology can be used for enhancing the reliability and security of wireless systems, but also when it is better to rely on conventional HD technology. The contributions presented herein with regards to IBFD technology rely on the significant advances in SIC made over the recent years and assume that SI is suppressible to a great extent. However, suppressing interference across multiple radios is considerably more challenging and not nearly as well studied as dealing with SI. As such, in order to provide practical means for extending the reliability and security benefits of IBFD radios to multi-radio setups, this work provides novel methods for radio interference suppression across nodes. Furthermore, the work demonstrates the effectiveness of these methods in enhancing the security of practical wireless communication systems.

1.3 Structure of the Thesis

The remainder of this thesis is aligned with the structure in Fig. 1.2 and is organized as follows. Firstly, Chapter 2 reviews the fundamental methods used for improving and degrading the resilience of wireless communications. Then, Chapter 2 gives an overview of IBFD radio technology, including the SI problem, its cancellation techniques, and the general ideas behind multifunctional IBFD radios. Chapter 2 also gives an overview of the potential benefits of interference cancellation across multiple platforms and discusses the challenges therein. Chapter 3 presents proof-of-concept measurements that demonstrate the viability of applying IBFD radio technology for combining simultaneous signals intelligence and neutralization tasks and studies the practicality of several such relevant combinations. Chapter 4 proposes methods for suppressing periodic or known interference and demonstrates the performance of those methods in cooperative jamming scenarios. Finally, Chapter 5 presents the summary and conclusions of this thesis.

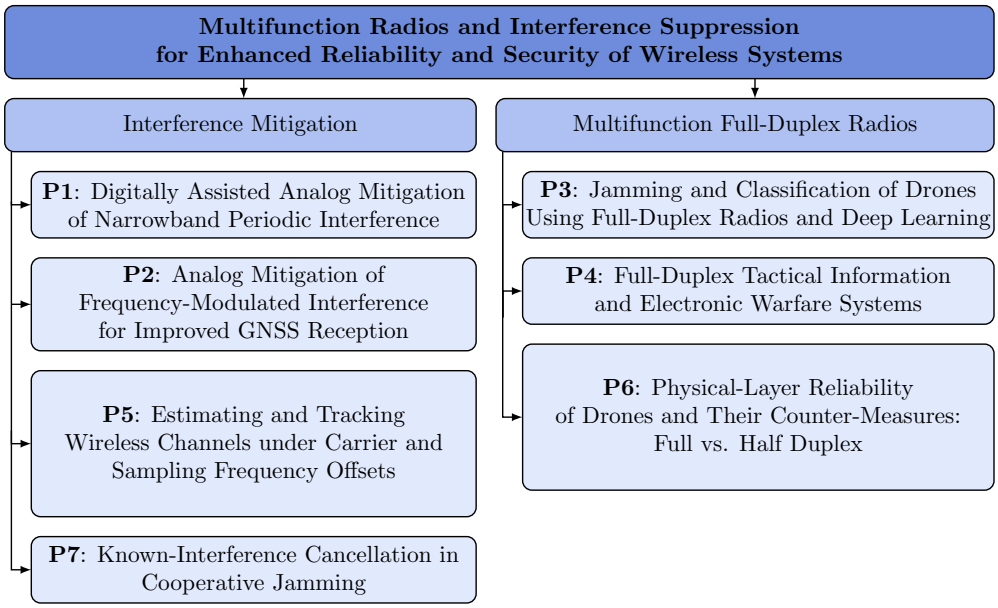


Figure 1.2 Structure of the research presented in this doctoral thesis.

2 BACKGROUND

This chapter provides fundamental background information on the security and reliability of wireless communications, reviews the same-frequency simultaneous transmit and receive (SF-STAR) technology that facilitates single platform radios to operate in IBFD mode, and finally discusses the challenges and appeal of extending the SF-STAR concept to multi platform radios.

2.1 Wireless Communications and Electronic Countermeasures

The wireless medium is inherently accessible to anyone and this is what facilitates communication between mobile devices that cannot rely on wired infrastructure. However, this accessibility is also what makes these same wireless communications vulnerable. In contrast to wired communications, where attackers cannot carry out hostile actions towards the communications without being physically connected to the network, wireless communications are susceptible to electronic countermeasures that require nothing other than the attacker being in the vicinity of the other wireless nodes. These countermeasures include, e.g., eavesdropping and jamming. Improving the resilience of wireless communications against countermeasures has been, and continues to be, an important research goal. At the same time, it is also of interest to improve the countermeasures themselves so that wireless devices (e.g., drones) cannot be freely used for malicious purposes. Herein this contest for control of the electromagnetic spectrum is considered by relying on the three-node system model illustrated in Fig. 2.1. The system model includes a transmitter-receiver pair and an adversary that is capable of intercepting or jamming the wireless communications between the pair.

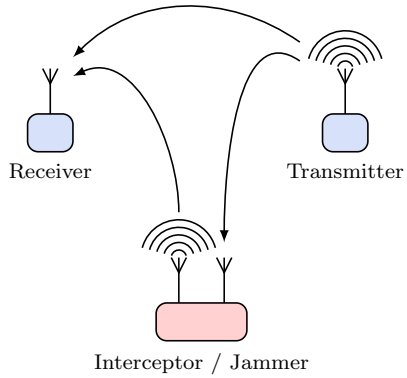


Figure 2.1 Three-node system model for wireless communications and electronic countermeasures.

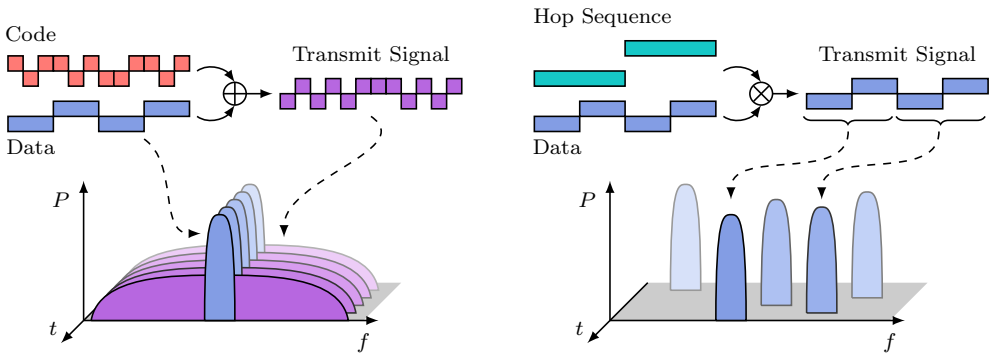
2.1.1 Anti-Jam & Anti-Intercept Techniques

Regardless of whether the adversary intends to intercept or jam the wireless communication between the transmitted and receiver, the communicating nodes are motivated to prevent the adversary from succeeding. Ensuring the escape from interception or jamming in wireless communications is regretfully impossible. Under the right circumstances all wireless systems can be eavesdropped or jammed [14]. That is, with sufficient signal-to-noise ratio (SNR) at the interceptor or jammer-to-signal ratio (JSR) at the receiver these attacks will succeed. Still, anti-jam and anti-intercept techniques have been developed to deter such attacks.

The prevalent methods for protecting wireless communications against eavesdropping and jamming are various spread spectrum techniques which, in one way or another, try to hide the communication signal from the adversary, consequently making the signal a more difficult target. Essentially, as the name suggests, spread spectrum systems take advantage of the transmitted signal occupying a significantly wider bandwidth than the information signal requires. This bandwidth expansion accounts for the favorable properties of spread spectrum systems and is typically referred to as the processing gain, which is defined as

$$G_{\mathrm{P}} = \frac{W}{B}, \tag{2.1}$$

where W is the bandwidth of the spread spectrum signal and B is that of the information signal.



(a) DSSS **(b)** FHSS

Figure 2.2 Comparison of the signal power, P, distribution over time, t, and frequency, f, for spread spectrum techniques.

The most practical and dominant spread spectrum techniques are direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) techniques (illustrated in Fig. 2.2). Direct-sequence spreading entails combining a high-rate spreading code with relatively low-rate data, which results in a transmitted signal with wider bandwidth than that of the data. Compared to a plain data signal, the direct-sequence spread spectrum signal will occupy a wider bandwidth but at a lower power spectral density, keeping the total power unchanged. As such, the spread spectrum signal becomes less indistinguishable from the noise floor and more challenging to detect. Ideally, a direct sequence signal with binary phase shift keying can be expressed as

$$x(t) = u(t)p(t)\cos(2\pi f_c t), \tag{2.2}$$

where $u(t)$ is the data signal, $p(t)$ is the spreading code, and f_c is the carrier frequency. Direct sequencing requires that both the transmitter and receiver know and use the same spreading code $p(t)$. Removing the spreading code in the receiver results in contraction of the bandwidth back to the data bandwidth and, against certain types of interference, this contraction can be taken advantage of through filtering to remove a portion of the interference [15].

Frequency hopping entails systematically changing the carrier frequency of the transmitted signal. In contrast to direct sequencing, which spreads the instantaneous bandwidth of the transmitted signal, frequency hopping moves the instantaneously narrowband signal around within a wide bandwidth. Like direct sequencing, fre-

quency hopping tries to avoid being intercepted or jammed by making its position and existence in the electromagnetic spectrum less obvious to an electronic countermeasure system. When avoiding these countermeasures fails, it is hopefully only momentary due to the systematic changing of the carrier frequency. A frequency-hopped signal with binary frequency shift keying can be represented by

$$x(t) = \cos(2\pi(f_c(t) + u(t)f_\Delta)t), \tag{2.3}$$

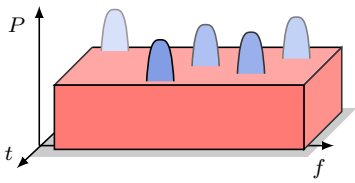
where the carrier frequency $f_c(t)$ is time-varying and f_Δ is the frequency deviation. The main requirement for frequency hopping is that both the transmitter and receiver agree on how the carrier frequency changes in time and that the receiver is actually able to adjust its carrier frequency in unison with the transmitter.

Both direct sequencing and frequency hopping rely on the transmitter-receiver pair having a preshared secret (i.e., spreading code or frequency hopping sequence) and the benefits of spectrum spreading rely on the adversary not knowing that secret. This added complexity of agreeing on and managing a shared secret across multiple devices, in addition to having the hardware capable of utilizing that secret, is the cost of improved security and resilience over plain wireless communications. However, it is remarkable that for the effectiveness of spread spectrum communications, no underlying theoretical limit exists. That might not be immediately clear because, e.g., it could be assumed that increasing the bandwidth of a direct-sequence spread spectrum signal needs the receiver filter to pass more noise than necessary to the subsequent signal processing stages. However, when applying a matched filter to the superposition of a signal, which it is matched to, and additive white Gaussian noise (AWGN) noise, then the output of that filter has a SNR that depends only on the energy-to-noise density ratio [15]. Therefore, the spread spectrum signal's bandwidth is inconsequential and without inherent theoretical limitations. Although, practical radio-frequency (RF) front-ends are typically limited in frequency, which also limits the frequency rage in which the signals can be spread.

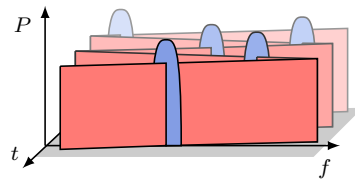
2.1.2 Jamming

As it is practically impossible to prevent wireless communications from being intercepted or jammed under all circumstances, it is in the attacker's interest to succeed with minimal effort or equivalently with maximal effective range. That is, from the

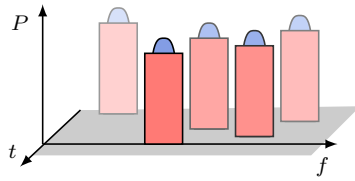
electronic countermeasures perspective, an ideal jamming attack would be highly energy efficient regardless of anti-jamming techniques a communication system uses and, at the same time, have a low probability of detection itself, so that the target would not realize the presence of an attacker. In general, to approach these objectives, the attack needs to be tailored for the targeted communication system. For that, the attacker needs to have a thorough understanding of the targeted system and a sophisticated enough jamming platform that can utilize this knowledge to optimize the attack. Against direct sequencing or frequency hopping spread spectrum techniques this means having some knowledge about the spreading code or frequency hopping sequence while also being able to spread the interference instantaneously or rapidly hop it around. Depending on the scenario, parameters of the targeted communication system may be readily available and fixed or unknown and adaptive to adverse conditions.



(a) FHSS under barrage jamming



(b) FHSS under sweep jamming



(c) FHSS under follower jamming

Figure 2.3 Common jamming techniques.

Consequently, various jamming techniques differ based on how much knowledge about the targeted system is expected to be known to the jammer at the time of the attack. Fig. 2.3 illustrates three common jamming techniques: barrage, sweep, and follower jamming. Barrage jamming is the simplest method in that it only assumes an approximate knowledge about the total frequency range used by the communication system. Barrage jammer transmits instantaneously wideband noise across that entire frequency range used by the targeted communication system. As the noise level at the receiver is increased, it makes it more difficult for the communication system

to function. The main limitation of barrage jamming is that it results in low power spectral density as limited jamming power is spread very wide. However, barrage jamming is often the best that a jammer can do when it knows nothing else about the targeted signal [16].

Sweep jamming is similarly simple in that it assumes some knowledge about the total frequency range used by the target, but instead of instantaneously spreading the interference across that entire bandwidth, it sweeps a narrowband interference signal across the frequency band of interest at some rate. Therefore, at any given time, the jamming signal is only affecting a small portion of the spectrum. Concentrating the full jamming power to a portion of the targeted signal in time can be sufficient to prevent the receiver from processing the entire signal. As such, this approach can be more effective than barrage jamming against frequency-hopped communications if the timing characteristic of the targeted communication systems are known and taken into consideration. The frequency sweep must be quick enough, so that the target system does not have a chance of avoiding being affected, but also not too quick to prevent spreading the power completely [17].

Follower jamming is a technique specifically to combat frequency hopping. A follower jammer tries to locate the frequency to which the target has hopped (while also making sure that the signal is not confused with anything else) and then jam that new frequency only. Frequency-hopped communication systems often use large bandwidths and short hop duration, which make it challenging for a follower jammer to detect and timely react to the changes in the communications carrier frequency. However, if implemented adequately, then follower jamming is the most efficient technique, as the jamming energy can be concentrated to only where the targeted signal is in the electromagnetic spectrum [1].

2.1.3 Detection & Interception

The more sophisticated a jamming attack is, the more it relies on target signal detection and interception, but detection and interception are valid electronic measures on their own too. Simply knowing that the communication is taking place can be valuable information, e.g., when trying to detect the physical presence of an adversary [18]. And accessing the communicated information even more so, e.g., to intercept the plans of an adversary. The anti-jam and anti-intercept techniques discussed

previously are equally challenging to detect and intercept as they are to jam. These techniques force the non-cooperative receiver to operate over a large bandwidth, increasing sensitivity to noise and placing greater demands on the receiver hardware capabilities. In order to deal with very large bandwidths, detectors often employ an RF front-end with modest bandwidth but with agile center frequency, scanning through the entire range of interest [14].

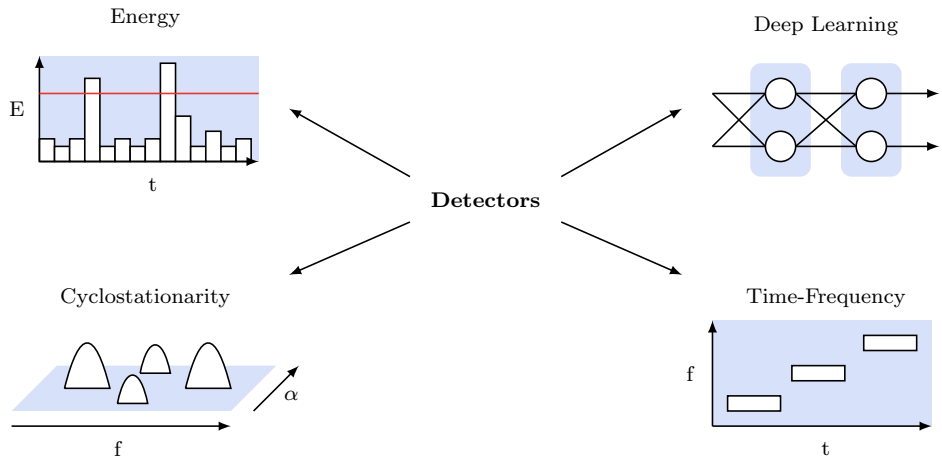


Figure 2.4 Detection and classification taxonomy.

Detection and interception are both valid electronic support measures in the context of electronic opposition, but the former is typically a prerequisite for the latter. This is because a signal of interest can only be intercepted (i.e., demodulated), if its presence and position in the electromagnetic spectrum have been identified. And, if prior knowledge about these is not available, then they need to be sensed. Furthermore, it is then also necessary to classify the signal's modulation type and extract the parameters that are essential for demodulation. Numerous methods exist for detecting and classifying wireless signals, with some of the most prevalent methods illustrated in Fig. 2.4 and discussed next.

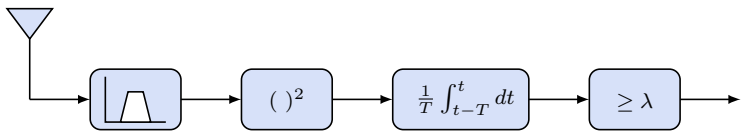


Figure 2.5 Block diagram of an energy detector.

For signal detection purposes, the input to the receiver can be considered to fall under one of the two hypotheses

$$H_0 : d(t) = n(t), \tag{2.4}$$

$$H_1 : d(t) = s(t) + n(t), \tag{2.5}$$

where $d(t)$ is the input to the receiver, $s(t)$ is the received signal of interest including channel effects and $n(t)$ is measurement noise. The objective of the detector is to make a decision on the binary hypothesis testing based on the receiver input, i.e., choose H_0 or H_1. When nothing is known about the signal to be detected and the noise is stationary, then the optimal detection technique is energy detection [14]. Energy detection is also the simplest technique, relying on filtering the input, integrating the received signal power over some time duration, which results in a test statistic $z(t)$, and comparing the test statistic to a predefined threshold λ (as illustrated in Fig. 2.5). In order to deal with frequency-hopped signals, it is also straightforward and common to combine multiple energy detectors in a channelized manner. Each of the individual outputs can then be compared to a separate threshold or the largest test statistic used only (as illustrated in Fig. 2.6) depending on the application.

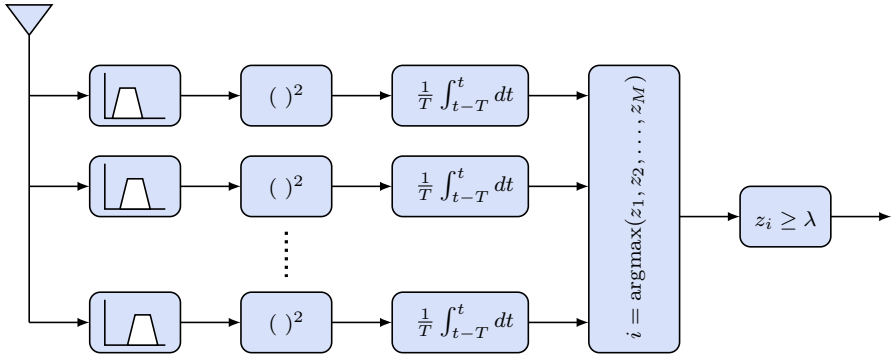


Figure 2.6 Block diagram of a channelized energy detector.

However, energy detection in itself does not provide insight about anything other than the signal's existence. In order to both detect and classify signals, the received signal needs to be analyzed using a more advanced approach. Time-frequency analysis methods (e.g., short-time Fourier transform, Wigner-Ville distribution, or Choi-Williams distribution) are popular basic tools that take advantage of different signals having different time-frequency representations [19]. The basic idea of time-

frequency analysis methods is to develop a joint function of both time and frequency that describes a signal's energy density simultaneously in both domains. The resulting distribution can then be used both for detection and classification.

Another aspect that can be exploited is the cyclostationarity of typical communication signals. Detection and classification is in that case performed by correlating the received signal with a portion of itself and analyzing the correlation output [20]. An advantage of cyclostationarity analysis is that AWGN noise is stationary and, therefore, the cyclostationary spectrum is noise free, which leads to increased sensitivity [21]. Finally, deep learning techniques have been gaining popularity for detecting and classifying low probability of intercept (LPI) signals and are demonstrating comparable or superior performance over other methods [22]. Deep learning-based method are especially interesting because they can be extended to not only classify signals but also identify specific transmitters based on their physical-layer attributes [23].

2.2 In-Band Full-Duplex Radio Technology

The ever-increasing demands on the limited wireless spectrum are driving the pursuit for systems with higher and higher spectral efficiency and among the various ways to achieve better spectral efficiency is the IBFD radio technology. While the nodes of most conventional wireless communication systems do operate as both transmitters and receivers, they do so in either HD mode or emulate FD mode by dividing the transmission and reception in time or frequency (i.e., time divison or frequency division duplexing). In contrast to these methods that emulate FD operation, IBFD entails wireless nodes transmitting and receiving simultaneously over the same frequency band. Compared to the time and frequency division methods, this offers potentially double the spectral efficiency, as measured by the number of information bits reliably communicated per second per Hz [11]. This makes IBFD radio technology of considerable interest for next-generation wireless networks.

2.2.1 Self-Interference Cancellation

The key obstacle that has prevented IBFD radio technology from being implemented in wireless communication systems thus far is the powerful SI from a node's own

transmission that submerges the signal of interest transmitted from any far-away node. And that SI cannot be simply subtracted from the total received signal during digital signal processing in the receiver, even if the receiver can accurately model the path of the SI from the digital-to-analog converter (DAC) to the analog-to-digital converter (ADC). That is because typically the powerful SI spans most of the ADC's dynamic range and significantly increases the quantization noise for the signal of interest [24]. However, recent research has demonstrated that by dividing the SIC into separate stages, both before and after digitization, the SI can be attenuated sufficiently such that the resulting IBFD wireless system can achieve better spectral efficiency than a system that emulates FD operation [25]. Typically, SIC is divided into three stages as illustrated in Fig. 2.7 and briefly explained in the following paragraphs.

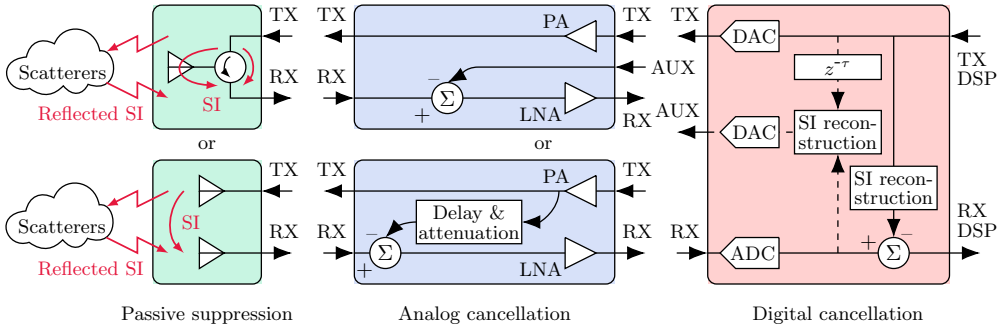


Figure 2.7 SI cancellation techniques at various stages (passive, analog, and digital). Passive suppression and analog cancellation can be approached broadly in two ways: passive isolation by using either a circulator or separate antennas and analog cancellation by filtering a replica of the transmitted signal in software or hardware to match it to the SI in the analog domain.

Passive suppression methods aim to isolate the transmit chain from the receive chain so that the SI does not reach the receive chain. This can be achieved to some extent by using separate antennas or a circulator that limits the amount of leakage from the transmit to receive chain. The main benefit of passive SI suppression is that these methods do not require complex signal processing algorithms nor additional special hardware to function. However, it is in general unfeasible that the SI is suppressed in its entirety using simply passive isolation. The effectiveness of such methods is limited by physical imperfections and the terminals' form-factor. Circulators unfortunately have some leakage while adjacently placed antennas exhibit some coupling and in smaller devices there is less room to implement isolation techniques altogether [11]. Furthermore, passive isolation techniques are inherently ineffec-

tive against reflected-path SI that is caused by the transmitted signal reflecting back into the device from the near-by environment. Handling SI that is affected by the environment, in which the device operates and that is typically subject to changes, requires active and channel-aware suppression techniques.

The analog domain methods aim to suppress the SI in the receive chain before the ADC digitizes the signal. It has been demonstrated that this can be achieved broadly in two ways. Firstly, by tapping a portion of the analog transmit signal before the transmit antenna, processing the tapped signal in analog domain to have an opposite phase to the SI in the receive chain, and feeding the processed signal into the receiver chain [26]. Secondly, by tapping a portion of the digital transmit signal, processing that signal in the digital domain to have an opposite phase to the SI in the receive chain, converting that digital processed signal to analog using an auxiliary transmit chain, and feeding that signal into the receiver chain before digitization [25]. Tapping the analog signal as close to the transmit antenna as possible has its advantage that it allows to capture the nonlinear distortions of the transmit chain, which when tapping the digital signal need to be explicitly modeled. Then again, tapping the digital signal potentially allows for far more elaborate channel modeling and does not require specific hardware for processing the tapped signal in the analog domain, but simply a separate transmit chain. Due to the complexity of analog signal processing and the imperfections of analog hardware, this SIC stage is still typically left with some residual SI. But, assuming that the reflections from nearby environment are not too powerful, this residual SI is typically weak enough that it does not cause the quantization noise to negatively impact the signal of interest.

The digital domain methods aims to suppress the SI in the received digitized signal, i.e., after the ADC, and essentially need to deal with the shortcomings of the two previous stages. The digital-domain methods have to account for everything that affects the signal between the DAC and ADC, whereas often the biggest challenge is modeling the nonlinearities caused by the power amplifier (PA). The limitation of working in the digital domain is that the dynamic range therein is restricted by the ADC and in order for digital methods to be effective, the previous stages will have needed to suppress the SI sufficiently beforehand. However, the advantage of working in the digital domain is that the algorithms are relatively easy to implement and develop. As such, there are numerous digital SI suppression methods that have been published, ranging from using polynomial models to machine learning [27].

2.2.2 Spectral Efficiency

Current state-of-the-art IBFD radio prototypes achieve total SIC in excess of 100 dB in proof-of-concept scenarios and environments [5] and, therefore, provide promising conditions for wireless applications aimed at information exchange [24]. It is clear that in a two-node system with adequate SIC, IBFD operation doubles the spectral efficiency compared to a HD system. However, typical wireless applications consist of more than two nodes, and the impact of IBFD operation mode in such scenarios is more multi-faceted. For example, IBFD operation mode allows terminals to be continuously cognitive, meaning that even during a transmission the terminal can detect a collision and immediately abort the transmission, which can lead to improved network throughput. Furthermore, IBFD operation mode allows forwarding a packet that is still being received, which has the potential to greatly reduce the end-to-end delay of a multi-hop network compared to conventional store-and-forward techniques employed in HD mode. Still, IBFD mode does not necessarily always outperform its HD counterpart, and, as such, it is quite often that hybrid schemes are considered that take advantage of IBFD capabilities when suitable, but otherwise rely on HD mode. Hybrid schemes typically outperform either of the individual schemes [24].

2.3 In-Band Co-Existing Radio Technology

Whereas IBFD radio technology applies to wireless nodes that carry out both the transmission and reception, thus knowing the transmitted signal and having the potential to cancel the transmitted signal in the receive path, there are many scenarios where it is not the same node that does the transmission and reception, but the receiving node nonetheless knows the transmitted signal, which is often referred to as known interference (KI). And in those scenarios, like in IBFD radios, it would be beneficial to estimate the wireless channel and the impairments that impact the signal so that the received signal could be suppressed. This section discusses the additional challenges that come with separating the transmit and receive functionality across different nodes compared to IBFD radios and also the benefits of suppressing KI across nodes.

2.3.1 Channel Estimation and Frequency Offsets

In works where the use of KI is considered, especially in information theoretic works, perfect known-interference cancellation (KIC) is often assumed [28, 29, 30]. However, because of hardware imperfections and the propagation environment, the received KI in practice significantly differs from that what is transmitted and even the SI cancellation methods of IBFD radios do not necessarily suffice. Fig. 2.8 illustrates some of the typical impairments between wireless transmitter and receiver pairs. Firstly, oscillator inaccuracies between different transmitters and receivers inevitably result in carrier and sampling frequency offsets, and oscillators generally exhibit long-term drifting and short-term fluctuations that make these frequency offsets time-varying. To make matters worse, in wireless propagation these frequency offsets can be further aggravated by the Doppler effect. If not compensated for, then time-varying frequency offsets are harmful to the performance of systems trying to suppress the KI [13, 31].

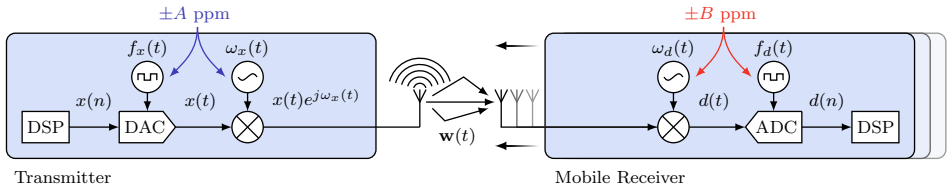


Figure 2.8 RF impairments that affect KIC between two nodes.

Compensating the frequency offsets so as to suppress their negative effects requires the offsets to be estimated and, due to their time-varying nature, continuously tracked. This must of course be done simultaneously to estimating and tracking the wireless channel itself too. In cases where the latter alone is sufficient, conventional adaptive filters have proven especially popular due to their robustness and simplicity. Practical use of adaptive filters is also supported by their well-understood behavior in steady and tracking states. However, frequency offsets tend to compromise the performance of classical adaptive filters [32]. As such, a robust-yet-simple adaptive filter with analytically well-understood behavior that can jointly and explicitly estimate and track both the wireless channel and frequency offsets is an appealing solution for KIC. Later in this work, such an adaptive filter is provided that further bridges the gap between KIC being theoretically desirable and practically viable.

2.3.2 Cooperative and Coexisting Operation

Although synchronizing known signals across wireless nodes has several applications, then using KI for cooperative jamming is an especially enticing way for improving physical layer security of wireless communications. The general idea behind such cooperative operation (as illustrated in Fig. 2.9) is that while a legitimate transmitter broadcasts a signal of interest to the legitimate receiver, a cooperative node simultaneously transmits an interference signal, which is known to the legitimate receiver. It is then highly challenging, albeit possible, for an eavesdropper to extract the signal of interest from the superposition of the two signals. The eavesdropper may still be successful if it can be positioned favorably or use beamforming to null out the jamming node. However, the legitimate receiver is envisioned to use its prior knowledge to suppress the interfering signal, therefore facilitating the processing of the signal of interest in a straightforward manner. Cooperative jamming has the potential to prevent eavesdropping without relying on upper layer encryption, and provides a welcome alternative for the upper layer security mechanism. Simulated and numerical results have demonstrated that cooperative jamming can improve the secrecy rate of wireless communications in scenarios ranging from simple two-way communications [33, 34] to relayed link [35]. Furthermore, experimental results with periodic KI have demonstrated the practical feasibility of using cooperative jamming for improving physical layer security [36]. However, a comprehensive and practical solution for use with any type of KI waveform still has been missing.

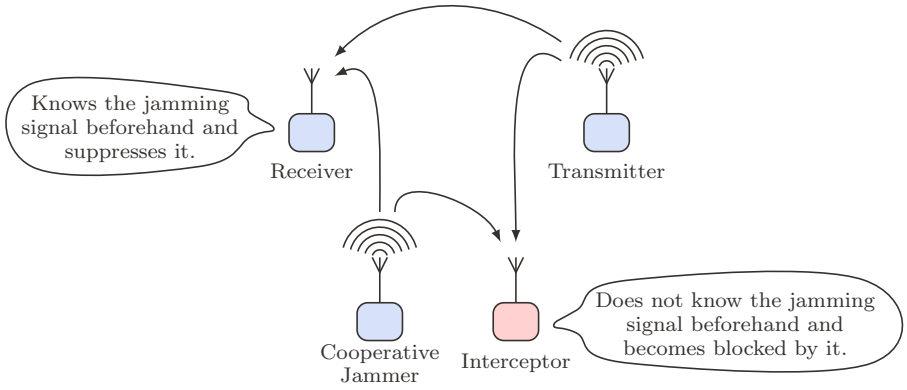


Figure 2.9 Cooperative jamming system model for improved physical layer security.

3 MULTIFUNCTION IN-BAND FULL-DUPLEX RADIOS

In this chapter, the contributions to multifunction radios are presented. Multifunction radio is a highly coveted concept [37, 38, 39, 40] and essentially an extension to that of the multistandard radio, which is already facilitated by software-defined radios [41, 42]. Both multifunction and multistandard radios address the desire to provide more flexibility and capabilities with overall fewer hardware components. However, while the multistandard radio concept assumes the capability to seamlessly adjust a wide range of parameters of a communication system, true multifunction operation assumes that the radio is capable of carrying out various different functions simultaneously and possibly even at the same frequency. For example, multifunction radios envision integrating RF functions such as radar, electronic countermeasures, and wireless communications into a single system utilizing a common set of hardware (as shown in Fig. 3.1) for which the functionality is programmed as necessary [6]. However, combining any such distinct set of RF operations on a common set of hardware simultaneously is complicated as the individual operations tend to interfere with one another.

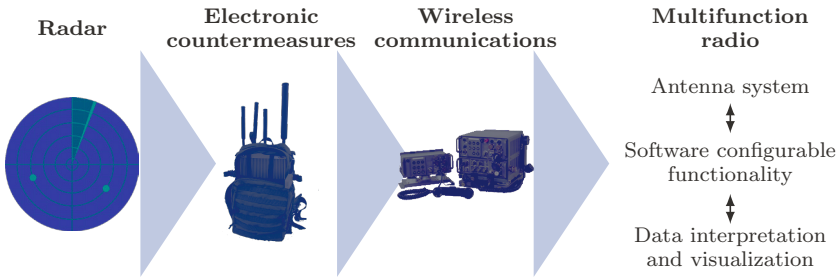


Figure 3.1 Multifunction radios envision integrating various functions, including radar, electronic countermeasures, and wireless communications, into a shared set of antennas and signal processing hardware to provide radio functionality as fitting for the situation.

Typical single-function HD systems are able to operate in the electromagnetic spectrum together and at peak performance by applying isolation techniques that are custom-suited to each individual system, but this approach cannot be used when a single aperture is tasked with performing multiple functions. So far, aspiring multifunction RF systems have therefore mostly relied on separating transmit and receive antennas to provide moderate isolation between the respective signal paths. However, providing adequate transmit-to-receive isolation is a key challenge in developing truly multifunction radios [37]. As such, IBFD radio technology can become a critical part of the multifunction radio concept because it allows the transmit and receive functions, whatever they are, to operate simultaneously **[2, 4, 5, 6]**.

In this work, the potential of multifunction IBFD radios is studied in the context of remote-controlled drones to show the impact that physical layer performance of wireless systems can have on the safety of cyber-physical systems. This is especially fitting as drones pose an increasingly large threat and RF-based counter-drone methods are the prominent tools for dealing with that threat **[1, 8]**, [43]. The study herein covers both the drone and counter-drone system perspectives, but fundamentally concerns a wireless system as illustrated in Fig. 2.1 and extends to any such system whether it involves a drone or not. In IBFD operation mode, an electronic counter-drone system can create an invisible electromagnetic dome, or a so called radio shield, around the IBFD node as illustrated in Fig. 3.2. The feasibility of implementing an IBFD radio shield has in numerous occasions been demonstrated in laboratory environments **[7]**, [44].

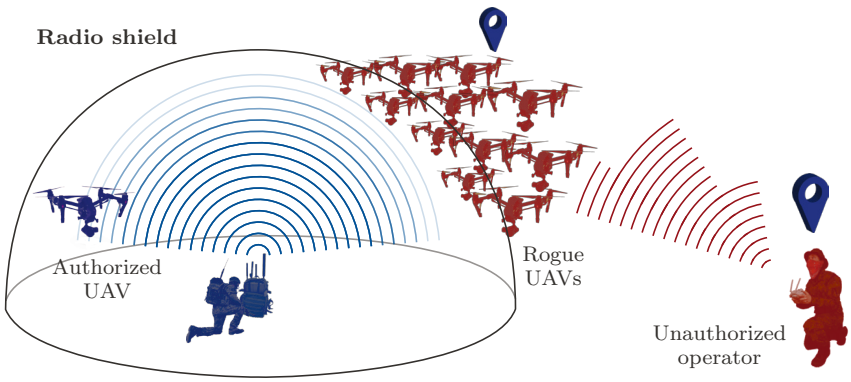


Figure 3.2 Defensive IBFD radio shield — simultaneously preventing unauthorized drones from accessing the defended airspace and monitoring the RF spectrum (e.g., locating the drones and their remote control station).

In practice, an IBFD radio shield could be used to prevent malicious drones in a drone swarm from wirelessly communicating with each other while at the same time allowing to monitor the drones' communication attempts — communication within a drone swarm is essential for its operation, and this effectively prevents the drone swarm from functioning as a coherent unit while still allowing to, e.g., track drones by their RF fingerprints (i.e., classify and locate individual drones) [**P4**]. Similarly, an IBFD radio shield could prevent drones in a swarm from positioning themselves relative to each other using RF-based method such as two-way ranging or radar-based positioning, while simultaneously allowing the IBFD node to detect those efforts [**P4**]. Another advantage is that the radio shield could prevent the malicious remote controller from directing malicious drones while at the same time allowing to intercept the remote control signals — this essentially means that inside the radio shield, the drone or drone swarm is completely disconnected from its operator, but the IBFD node can nonetheless observe (e.g., classify and locate) the remote control station [**P4**]. Finally, the radio shield could prevent drones from determining their location using GNSS-based positioning while at the same time retaining the IBFD node's own ability to do so [**P4**]. This would be especially valuable in case of a mobile IBFD node and radio shield. Of course, to some extent a similar effect could be achieved in some cases by using an HD system that intermittently transmits interference and processes the received signals. The following compares these two approaches in detail.

3.1 Drones vs. Counter-Drone Measures

The pros and cons of HD and IBFD operation in counter-drone conflicts are herein weighed in three different scenarios. Firstly, a counter-drone system's ability to restrict the airspace into which a remote-controlled drone can enter is evaluated. Secondly, a remote-controlled drone's ability to operate in an airspace that is guarded by a counter-drone system is examined. Thirdly, a drone's ability to detect jamming is studied. The scenarios are summarized in Table 3.1, where the highlighted background indicates the operation mode comparison in question.

Table 3.1 Drone vs. Counter-Drone System Scenarios

Scenario \ Operation	Transmit	Receive	Interfere	Detect	Device
Jamming and Classification	HD	HD			RC
	HD	HD			UAV
			HD/FD	HD/FD	CDS
Two-Way Communication	HD/FD	HD/FD			RC
	HD/FD	HD/FD			UAV
			HD/FD	HD/FD	CDS
Communication and Detection	HD	HD			RC
	HD/FD	HD		HD/FD	UAV
			HD/FD	HD/FD	CDS

3.1.1 System Description

The following parameters are used for the study in the three-node system model illustrated in Fig. 2.1. The parameters are close to what can be found in many remote-controlled drone and counter-drone systems **[1]**, [45] and represent the general capabilities of practical systems, but do not strictly correspond to any specific system. The total bandwidth that is used by the remote control link is taken to be 80 MHz and is divided into 160 equally spaced channels with bandwidths of 0.5 MHz. Both the remote controller and drone transmit a binary frequency-shift keying (BFSK) signal that has a frequency deviation of 200 kHz, encoded data rate of 25 kbps, and frequency hops 40 times per second. Output powers of the remote controller and drone are 20 dBm in HD mode and 17 dBm in FD mode so as to maintain the same energy-per-bit ratio as in HD mode.

The counter-drone system employs a channelized version of the energy detector (that is illustrated in Fig. 2.6) for signal detection. On top of that, the counter-drone system implements one of three strategies: constant, reactive, or follower jamming. In reactive mode the system does not use the specific detected channel information, but jams the entire band. For constant and reactive jamming strategies the system can use either barrage or sweep jamming signal. The counter-drone system output power is 40 dBm regardless of the operation mode in order to maximize its impact.

In case of the sweeping jammer, 2.5 kHz sweep rate is used. The signal detection and jamming times at the counter-drone system are 1.6 ms and the HD counter-drone system relies on a 50% duty cycle.

The noise floor is taken to be -90 dBm in a single channel and the radio link between remote controller and drone is considered to be functional as long as the channel-bit error rate is less than 1% in both ways. With a moderate coding rate, this would allow to reach an information-bit error rate of 10^{-5} that is sufficient for the repetitive nature of drone remote control communications [**P6**]. Furthermore, it is assumed that the drone is operated 100 m above ground level, while all other nodes are on the ground, unless stated otherwise. To take into account the different channels between the nodes without fading, this analysis relies on empirical studies that have characterized the air-to-air, ground-to-air, and ground-to-ground channels in wireless drone communications to have path loss exponents of 2.0, 2.2, and 3.3 respectively [46].

3.1.2 Verification of Analytical Expressions

In order to analyze the impact of operation mode and different strategies on the drone vs. counter-drone interactions, analytical functions were derived in [**P6**] for estimating the probabilities of detection and false alarm as well as of bit error in demodulating frequency-hopped BFSK signals under interference. The derivations are not reproduced here but are relied on and the reader is referred to [**P6**] for details. Herein, accuracy of the developed analytical techniques is first demonstrated by comparison to simulations. The detection and false alarm probabilities of frequency-hopped BFSK signals are checked using Propositions 1 through 4 from [**P6**]. The simulations consider a channelized energy detector that receives SI and signal of interest at specific power levels and makes a decision based on these. More details on the simulations are provided in [**P6**]. The resulting receiver operating characteristic (ROC) curves at the counter-drone system are plotted in Fig. 3.3 and demonstrate that the estimations agree with the simulation results, but also give some insight into the different strategies. For example, wideband detection ($\mathrm{RJ_n}$) or ($\mathrm{RJ_s}$) is assured to correctly detect the presence of the signal of interest when the threshold is low enough, but the channelized detector ($\mathrm{FJ_n}$) is not guaranteed to determine the correct channel. Furthermore, the ROC worsens with the increase in the SI level.

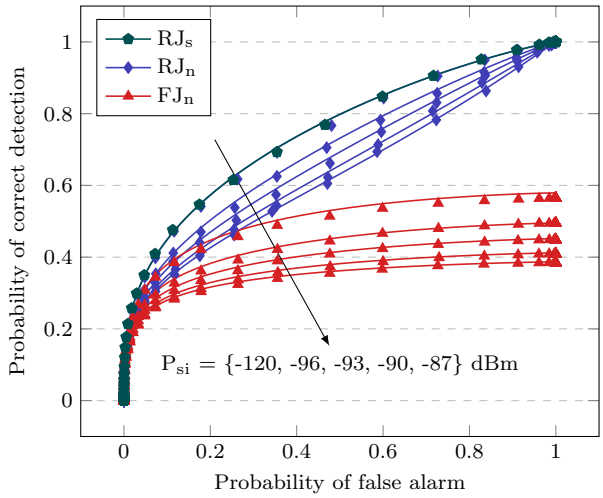


Figure 3.3 Counter-drone system receiver operating characteristic curves with different detection strategies and at varying levels of self-interference powers denoted with P_{si}. The detector considers 20 samples and the signal of interest power level is $\mathrm{P}_{\mathrm{soi}} = -91$ dBm. Analytical results are plotted with solid lines and simulated results with markers.

The detection results are extended by including also the demodulation analysis using Propositions 5 and 6 from [**P6**]. That is, the estimated and simulated channel-bit error rates (BERs) at the drone are compared, while the counter-drone system is detecting and interfering with the signal transmitted by the remote controller. The results are plotted in Fig. 3.4 and again demonstrate a good match between analytical estimations and simulations. Furthermore, it is evident that the follower jammer becomes effective at lower JSRs than the reactive jammer. This is because the follower jammer is able to overcome the processing gain of frequency hopping unlike the wideband reactive jammers. The reactive sweep jamming, however, has the potential to be more efficient than reactive noise jamming because the frequency-swept jammer concentrates its energy to just 10% of the total bandwidth during a single symbol transmission. This starts to degrade the BER at lower JSR, but at the same time limits the maximum BER at higher JSRs. Finally, it is also evident that jamming in IBFD mode is more effective than in HD mode because of the extra time spent in jamming mode. However, that benefit diminishes as the SNR at the counter-drone system drops. Altogether, the results in Fig. 3.3 and 3.4 indicate that the analytical functions accurately estimate the system interactions and this allows to proceed in the following sections by relying only on analytical expressions.

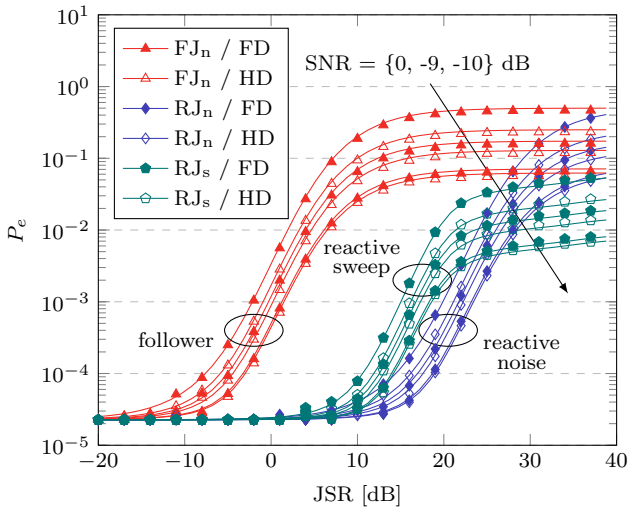


Figure 3.4 Bit error rate of a frequency-hopped BFSK transmission under reactive or follower jamming at different SNRs at the counter-drone system. The detection threshold at the counter-drone system is chosen to match a false alarm rate of 1%. Analytical results are drawn with solid lines and simulated results with markers.

3.2 Simultaneous Jamming and Classification

Firstly, a defensive counter-drone scenario is considered. The counter-drone system is used to minimize the area behind the system that a malicious remote-controlled drone can fly into (i.e., the area in which the remote control link has a BER below 1% in both ways). The counter-drone system could be, e.g., on a national border, prison or airport perimeter, or around some other critical infrastructure. Using the analytical functions derived in [**P6**], the efficiency of the strategies and operation modes from the counter-drone system perspective is here examined. The operable area of a remote-controlled drone depends not only on the strategy and mode but also on the position of the three nodes relative to each other. Fig. 3.5 shows how all of these affect the drone's operable area as the remote controller is moved closer to the counter-drone system. The results show that by using IBFD operation mode, the counter-drone system can limit the drone to a slightly smaller area, but also that the strategy selection essentially determines the jamming efficiency.

These results are summarized in Fig. 3.6 by showing the total area that a remote-controlled drone can operate in based on the distance between its remote controller and the counter-drone system. Because of the differing ground-to-air and ground-

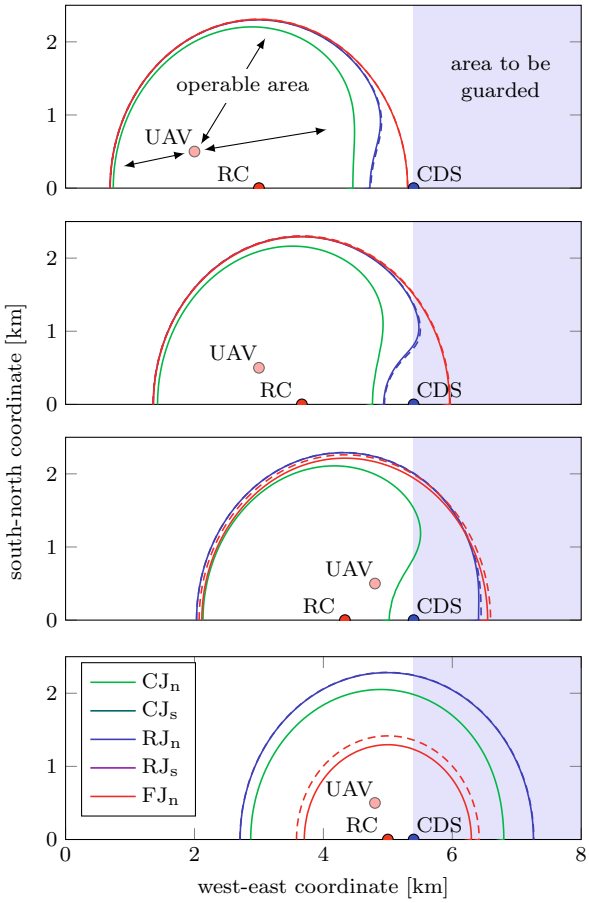


Figure 3.5 Remote-controlled drone's operable area against counter-drone system. Counter-drone system performance in FD mode is shown in solid lines and HD mode in dashed lines.

to-ground channels, it is more challenging for the counter-drone system to process the remote control signals. Consequently, when there is a large distance between the counter-drone system and the remote controller, constant jamming outperforms other strategies that rely on detecting the remote control signals. As such, constant jamming with frequency-swept interference is the safest choice to reduce the drone's operable area. The results also show that the IBFD operation mode helps reduce the operable area over HD mode somewhat — specifically by 4% to 17% percent depending on the strategy. This is again due to the extra time that an IBFD counter-drone system can spend jamming the communications.

The main feature that distinguishes counter-drone operations from most other detection and jamming attacks is the difference in the channels between all three nodes.

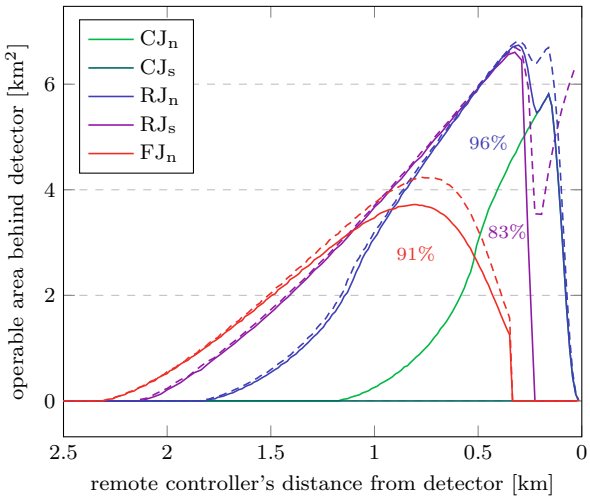


Figure 3.6 Area behind the counter-drone system in which a unauthorized drone can be controlled. The non-constant jammers are operated with a constant false alarm rate of 10%. Results for IBFD counter-drone system are plotted in solid and HD in dashed lines.

The ground-to-air channel between a drone and its remote controller is much more robust than the ground-to-ground channel between a counter-drone system and the remote controller. In the preceding analysis it was presumed that the counter-drone system is located on the ground. And this is reasonable assumption for most counter-drone scenarios. However, it is also conceivable that the counter-drone system is elevated to a similar altitude as the drone. This could be achieved using, e.g., a tethered drone carrying the system or by placing the system on an antenna tower. Fig. 3.7 shows how much air- and ground-based counter-drone systems reduce the drone's operable area depending on the remote controller's distance from the counter-drone system. The results show that elevating the counter-drone system clearly levels the playing field, in the sense that the counter-drone system can better detect the targeted signals and act correspondingly. Of course this also affects the jamming stage positively in that the interference reaching the drone and its remote controller are less attenuated. Furthermore, when the counter-drone system is lifted up, continuous jamming is not anymore the best-performing strategy, as follower jamming significantly outperforms it. Altogether, a counter-drone system that has been lifted up in the air considerably outperforms it terrestrial counterpart regardless of their operation modes and strategies.

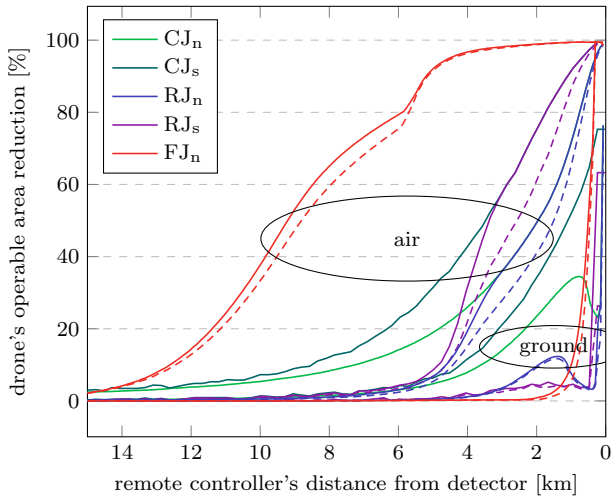


Figure 3.7 Comparison of terrestrial and airborne counter-drone system performances.

3.2.1 Deep Learning-based Prototype

The analytical results have shown that simultaneous detection and jamming can in theory at least somewhat improve the efficiency of a counter-drone system. Although these results do not demonstrate any other benefits that the counter-drone system might gain from IBFD operation, such as improved situational awareness. Herein a proof of concept practical implementation of such a system is also presented. This implementation not only takes advantage of IBFD radio technology but also deep learning [**P3**], which has proven hugely successful in various research areas that focus on feature extraction from raw input data [47, 48]. These include wireless communications research, where it has been applied for modulation recognition [49], radar classification [50], and drone classification from radar micro-Doppler signatures [51], to name a few. Several signal representation and preprocessing methods have been considered for deep learning-based feature extraction from wireless signals. For example, simply feeding the complex-sampled time series directly into the model without any preprocessing [52], extracting the amplitude and phase from the complex signal [53], and computing a spectrogram from the complex signal [53]. The latter, spectrogram-based representation, is especially suitable for classifying typical remote control systems that frequency-hop over a wide bandwidth, have different channel frequencies, channel bandwidths, and transmission times across dif-

ferent protocols. Therefore, herein a convolutional neural network (CNN) model is presented that assumes a spectrogram-based input of 64×64 pixels (as illustrated in Fig. 3.8) spanning 6.5 ms in time and 5 MHz in frequency. Such time-frequency coverage is enough for all the drone remote control signals analyzed in this work.

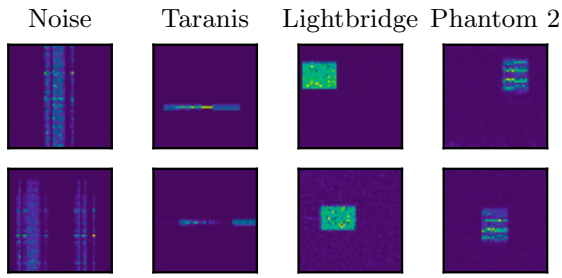


Figure 3.8 Spectrogram-based representation of signals for classification in a convolutional neural network model.

The architecture of the CNN model proposed in this work is depicted in Fig. 3.9. It is similar to various other object recognition models in that the spectrogram is processed by a stack of convolutional layers that have filters with very small receptive fields [48]. In order to decide into which of the categories (noise or one of the remote control signals) the spectrogram belongs, it is passed through three convolutional layers and two fully connected layers. The convolutional layers are fitted with rectifiers for speeding up the training and with max-pooling layers for spatial pooling. The fully connected layers are succeeded by a softmax classifier, which computes the likelihood of each class over all the classes.

3.2.2 Measurement Results

To confirm the feasibility of simultaneously jamming and classifying drone remote control signals, the following experiment was carried out in a controlled environment. The experiment imitated a scenario where a IBFD radio is used to neutralize a malicious remote-controlled drone through simultaneous jamming and interception as illustrated in Fig. 3.10. The devices were connected through coaxial cables, instead of using antennas, to provide a controlled environment with precise control of the power levels, remove all sources of external interference, and make sure that the jammer does not interfere with other devices in its vicinity.

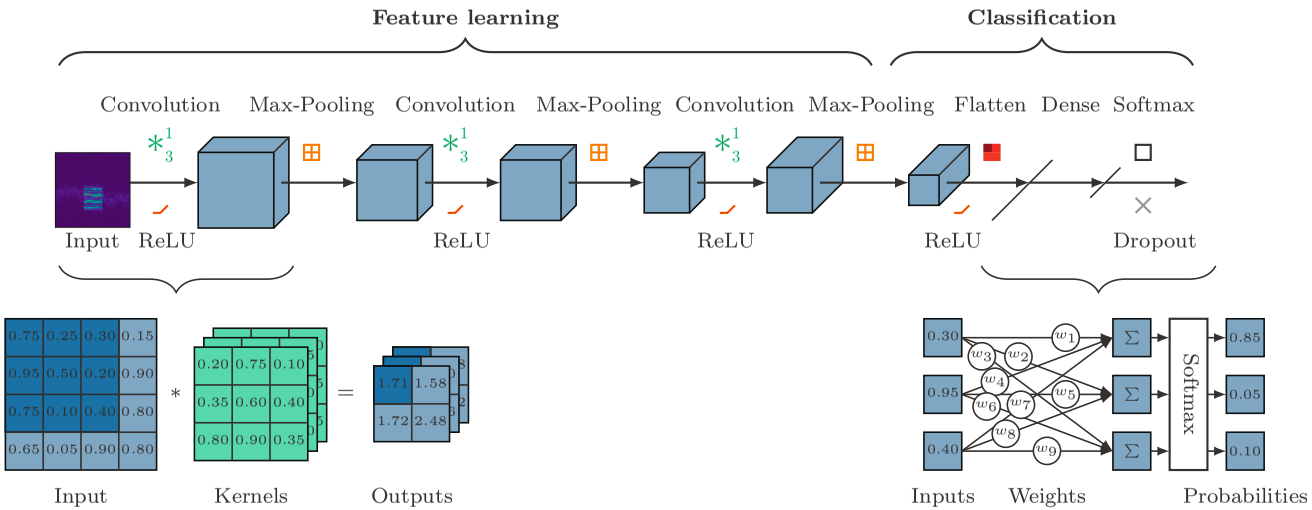


Figure 3.9 Architecture of the convolutional neural network proposed and used in this work to detect and classify drone remote control signals in multifunction IBFD radios.

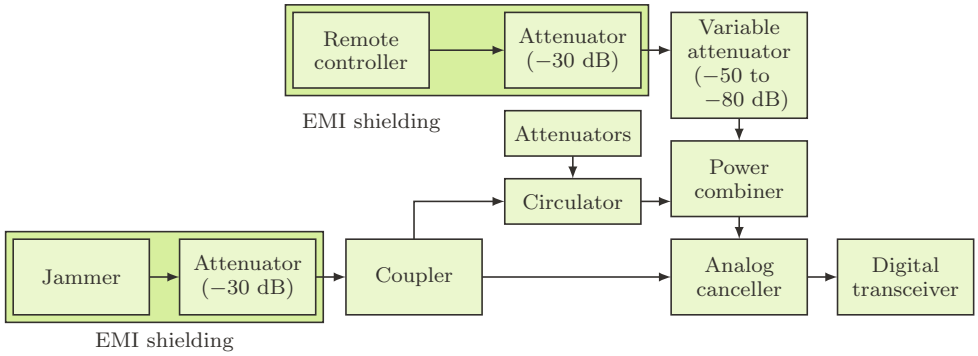


Figure 3.10 Measurement setup for evaluating the performance of CNN-based drone classification while at the same time jamming the remote control link. Jammer signal estimation, its cancellation, and drone signal classification is implemented in the digital transceiver.

The IBFD radio prototype was built using a high-quality vector signal transceiver (PXIe-1073) and an actual drone jammer. The vector signal transceiver received and recorded signals with a 120 MHz sampling rate and duration of 50 ms while the jammer transmitted a 80 MHz wide sweep jamming signal with output power of 43 dBm that acted as SI for the vector signal transceiver. In order to facilitate processing the drone remote control signals at the receiver, the SI from jamming was canceled in three stages. As drone jammers typically use directional antennas, it is plausible that transmit–receive antenna isolation of up to 60 dB could be achieved in practice [54]. Therefore, a circulator together with an attenuator was used to mimic transmit–receive antenna isolation to that extent. The passive isolation stage was followed by an analog SI canceler [55] and, lastly, the residual SI was suppressed digitally **[3]**.

Three different remote control systems were used one by one to generate the signals of interest. The remote controllers were *FrSky Taranis X9D Plus*, *DJI Phantom 2*, and *DJI Phantom 3 Advanced*. Each of these utilizes in full the 2.4 GHz industrial, scientific, and medical (ISM) frequency band by way of frequency hopping, but they do so using different patterns. They also used different channel bandwidths, modulation rates, and transmission durations. Differences in these parameters are what allow the CNN model to classify between the remote control systems based on the spectrograms. All of the remote controllers' output powers respect the 20 dBm limit of the ISM band and, in order to emulate varying link distances, a variable attenuator between the remote controller and the receiver was used. The attenuator was varied in the range of −80 dB to −110 dB with 5 dB steps.

Both the analog and digital SI cancellation stages contributed about 40 dB to 45 dB of cancellation on top of the passive isolation **[3]** and the analysis herein focuses on the impact that these cancellation stages have on the signal classification. Fig. 3.11 illustrates the *DJI Phantom 2* remote controller signal classification at different stages. For reference, the case without SI is also included. It is evident that without SI, the model easily detects the remote-control packets. However, when the jamming is turned on and the SI is present, then the situation is not always as clear. When relying only on passive isolation for dealing with the SI, the model is completely blinded. By including analog SI cancellation, the model is able to detect and classify the signals of interest in certain frequency ranges but not others. This is because of the analog canceler's frequency selectivity. However, after digital SI cancellation the remote control packets are accurately detected across the entire frequency range and the situation resembles that of without any SI.

These results are next considered in more detail over the entire power level range and for all studied remote control systems. In order to verify and gain insight into the measurements, we compared in [**P3**] the measurement results to simulations and found that the simulated and measured results are in close agreement. For visual clarity, only the simulated results are shown in Fig. 3.12. Again, the results illustrate the inability of correctly detecting any of the remote control signals when only passive isolation is relied on. That probability increases when analog cancellation is introduced and when the received remote control signals are relatively powerful. Still, it can be seen that without any SI the CNN model is able to correctly detect the remote control signals at typically 20 dB lower signal-to-interference-plus-noise ratio (SINR). This gap is significantly reduced by also introducing digital cancellation. Then the detection penalty compared to the case without SI is only couple dBs.

Finally, accuracy of the classification model is shown in Fig. 3.13. These results combine the measurements with good SNR to demonstrate the effect of residual SI at different stages. Again, the results show that without active SIC, the model cannot detect any of the remote control signals. After analog cancellation the model is already somewhat successful in classifying the signals, but after digital cancellation the model's accuracy is only slightly below that without any SI. The results also demonstrate that the proposed model is quite robust and regardless of the SI level, the false alarm probability and incorrect classification rate remain low. This is aided by the fact that the measurements were carried out through cables without the presence

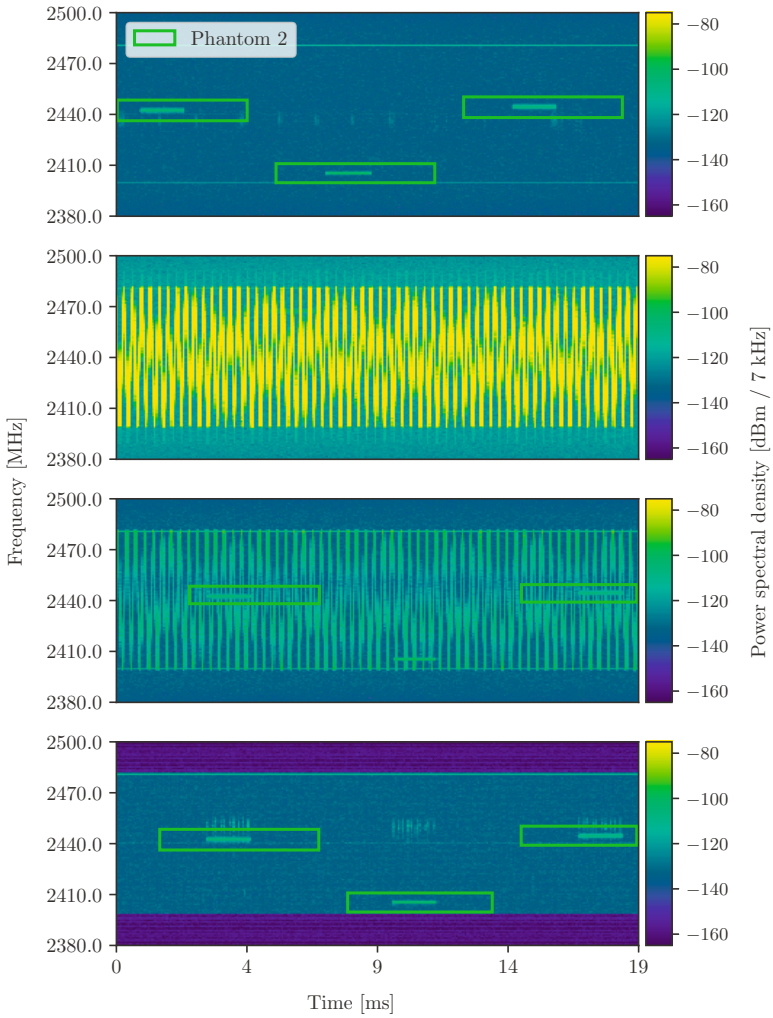
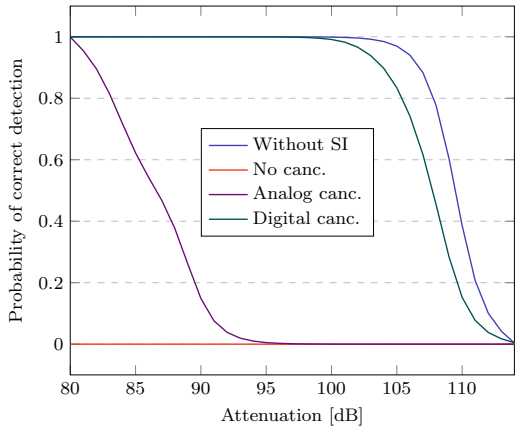


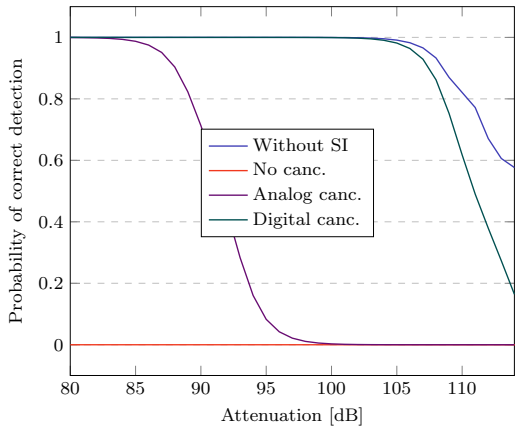
Figure 3.11 From top to bottom: Example signal classification (a) without SI, (b) with SI and only passive isolation, (c) after analog SI cancellation, and (d) after digital SI cancellation. Classification is indicated by the bounding boxes.

of other signals that could trigger false alarms.

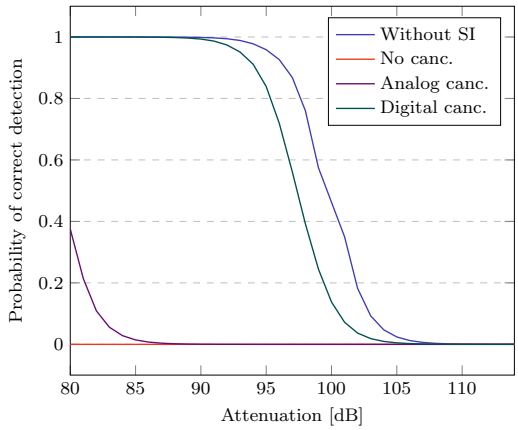
The results demonstrate that combining simultaneous jamming and reconnaissance of drone remote control signals using IBFD radio technology and deep learning is feasible in practice. The residual SI degrades the classification accuracy to some extent, but, bearing in mind that the classification in IBFD mode comes at almost no cost to the jamming efficiency, the IBFD operation mode is an attractive way to enhance the situational awareness of a counter-drone system.



(a) Phantom 2

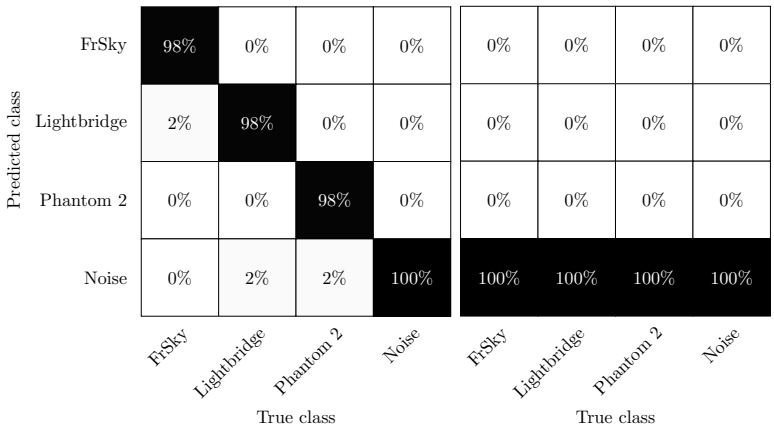


(b) Taranis

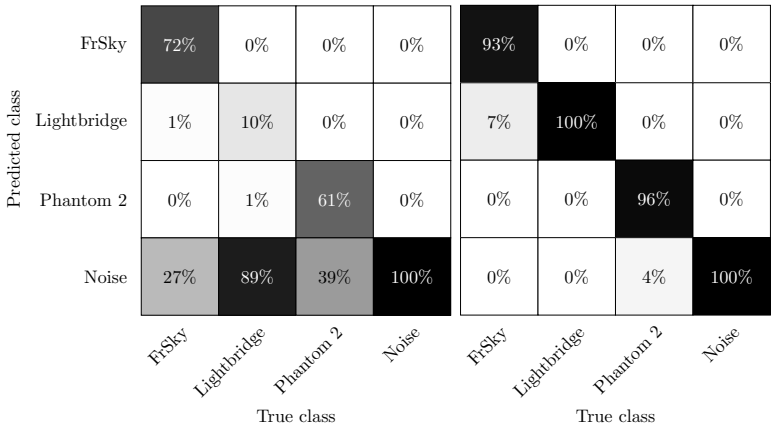


(c) Lightbridge

Figure 3.12 Correct detection probability of different remote control signals while simultaneously jamming and using various levels of SI cancellation.



(a) Without self-interference **(b)** With passive isolation



(c) After analog cancellation **(d)** After digital cancellation

Figure 3.13 Classification accuracy of the CNN model under relatively good SNRs.

3.3 Simultaneous Two-Way Communication

In the second scenario, the impact that the two-way communication operation mode of a drone has on its ability to fly in the presence of a malicious counter-drone system is analyzed. This scenario applies to situations where a remote-controlled drone is flying over an area that it surveys. Similarly to the previous scenario, this could be, e.g., a national border or the perimeter of any restricted area. The counter-drone system is used to limit the area that the drone can survey in order to carry out some activity in the area unseen. It is worth reminding here that, in order to retain the

energy-per-bit ratio across operation modes, the remote controller and drone use half of the output power and double the transmission duration in IBFD mode compared to HD mode.

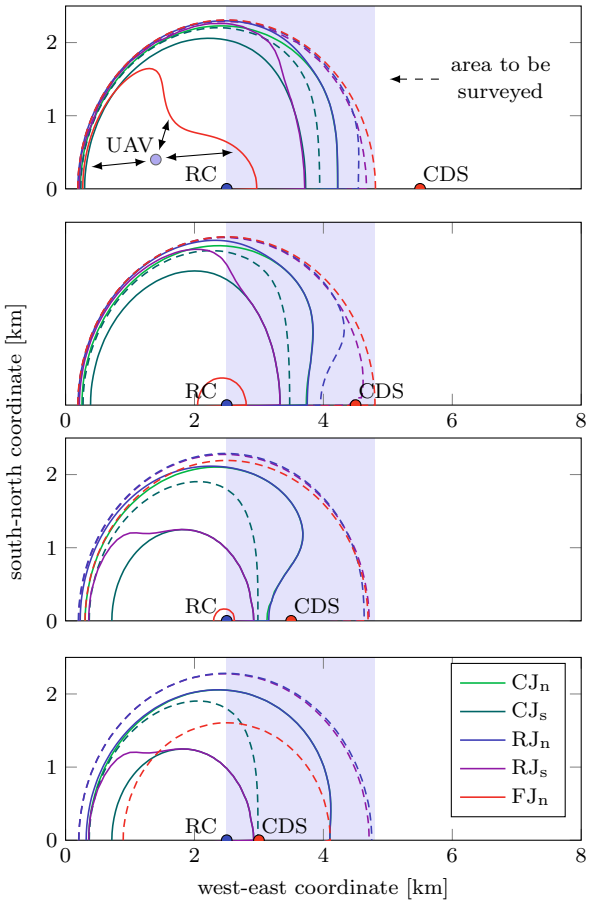


Figure 3.14 Operable area of a drone depending on the two-way communication mode between the drone and remote controller. Operable area in HD mode is shown with dashed lines and in FD mode with solid lines. The counter-drone system uses a false alarm rate of 10%.

Fig. 3.14 shows the area that a drone can be remotely controlled in for some counter-drone system placements. The results show, as expected, that when the counter-drone system moves closer to the remote controller, the operable area decreases regardless of the two-way communication operation mode between the remote controller and drone. However, if the drone is transmitting and receiving at the same time (i.e., in IBFD mode), then the area that it can cover is much reduced compared to time divided communication (i.e., HD mode). This is largely because

of the different channel models between the three nodes. In IBFD mode, the drone becomes a much more convenient target for the counter-drone system than in HD mode, since in IBFD mode the drone is essentially letting the counter-drone system know about its presence and also which channel it is currently using. In HD mode the counter-drone system is much more reliant on receiving signals from the remote controller through the unfavorable ground-to-ground channel. The operable areas depending on the distance between counter-drone system and remote controller are summarized in Fig. 3.15. The results show that the operable area in IBFD mode is always reduced compared to that in HD mode in the presence of an attacker. This is a substantial issue concerning many of the potential IBFD drone application.

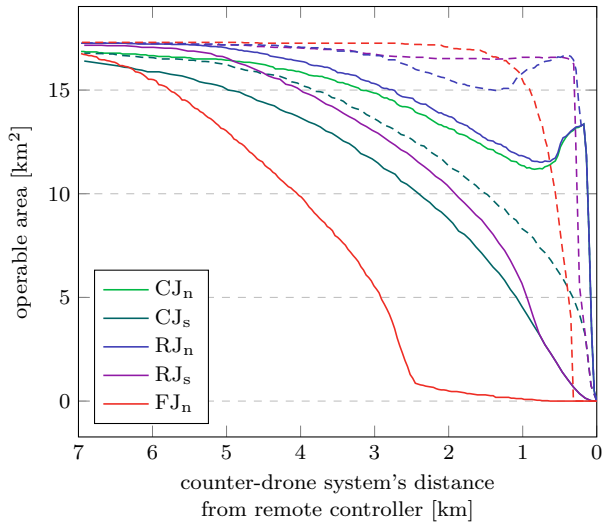


Figure 3.15 Operable area of a drone depending on the distance between the remote controller and counter-drone system. Operable area in HD mode is shown with dashed lines and in FD mode with solid lines. The counter-drone system uses a false alarm rate of 10%.

3.4 Simultaneous Communication and Detection

In the third and final scenario, the defensive drone perspective is continued. However, instead of focusing on two-way communications, herein the drone's ability to detect interference from the counter-drone system, depending on whether the drone has IBFD capabilities or is limited to HD operation, is analyzed. With IBFD capabilities, the drone is taken to be able to detect interference on all channels, including

the one that it is currently transmitting on, while with HD capabilities it is assumed to only be able to detect interference on channels that it is not transmitting on. It is especially interesting if the drone in either mode can reliably detect the jamming before being paralyzed by it. This scenario is again of interest in situations where the remote-controlled drone is surveying an area and where the adversary looks to escape or limit the surveillance. Only the follower jammer is considered in this scenario as this type of jamming is the most difficult to detect and in other cases the operation mode used by the drone probably will not limit its capability to detect the interference.

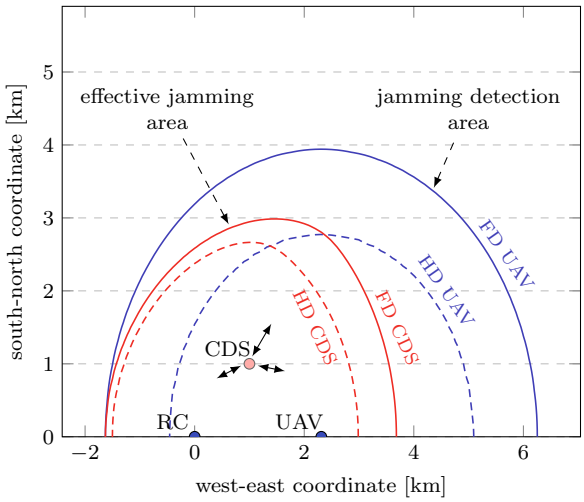


Figure 3.16 Comparison of HD and FD drone's capability to detect jamming. Also the effective jamming area is shown.

The third scenario is illustrated in Fig. 3.16, where the drone and its remote controller are located at some fixed positions. The figure shows the area in which the counter-drone system needs to be placed in order to be effective and the area from which the counter-drone system can be detected by the drone. The results show that a IBFD-enhanced drone can detect the jamming already at a much greater range than a HD-limited drone. This is because simultaneous transmission and detection allows the drone to detect jamming attacks that have been triggered by the drone's own transmission (i.e., at the correct channel). Therefore leading to more consistent jamming detection. The HD-limited drone, on the other hand, can only detect attacks that target the wrong channel or that are too late in attacking a recently vacated channel. In summary, IBFD radio technology enables jamming detection with much

improved performance and, depending on the position of the three nodes, detection of jamming in IBFD mode possibly allows to detect the presence of a counter-drone system before becoming paralyzed by it.

4 KNOWN-INTERFERENCE CANCELLATION

In this chapter, the contributions to KI cancellation are presented. First, Section 4.1 provides a brief analysis about the necessity to combine different stages of interference suppression in co-site radios. Then, Section 4.2 presents a digitally assisted analog domain method for suppressing strong interference before its digitization and Section 4.3 presents a fully digital method for suppressing KI after its digitization. Finally, extensive measurement results are presented in Section 4.4 with application to GNSS and Internet of Things.

4.1 Stages of Suppression

For an IBFD radio that forms a single physical device it is usually clear that SI needs to be canceled in both analog and digital domains due to the typically poor achievable passive isolation **[9]**, [11]. However, the same does not necessarily apply when canceling interference from separate devices that are positioned nearby. For such co-site devices, mitigation of interference in the analog domain prior to digitization is not required nor sensible under all circumstances, but does potentially offer an opportunity to improve the receiver sensitivity depending on how close physically the interfering radio is. Here, the circumstances under which analog mitigation of interference between co-site devices becomes useful are briefly analyzed.

In a typical receiver, the automatic gain control (AGC) maintains the ADC input at a constant full range level, meaning that a powerful interference will dictate the ADC input range. This results in reduced effective resolution for the signal of interest, which consequently may limit the receiver performance [56]. The final SINR after all stages of interference cancellation can be calculated from

$$\gamma = \frac{\rho}{\frac{P_S L_S}{P_I L_I/\Delta_a} + \rho/\Delta_d + 1} \cdot \frac{P_S L_S}{P_I L_I/\Delta_a}, \tag{4.1}$$

where $P_S L_S/(P_I L_I/\Delta_a)$ represents the SINR after the respective path losses L_S and L_I as well as analog cancellation Δ_a, ρ is the ADC's effective dynamic range, and Δ_d is the amount of digital cancellation. Then, whether analog and digital cancellation both are required or if digital cancellation alone is enough depends on the targeted SINR γ_t. The minimum level of digital cancellation that is needed to achieve $\gamma \geq \gamma_t$ given $P_S L_S/P_I L_I$, Δ_a, and ρ can be solved from (4.1) from

$$\Delta_d \geq \frac{\rho}{\frac{P_S L_S}{P_I L_I/\Delta_a} \cdot (\frac{\rho}{\gamma_t} - 1) - 1} \tag{4.2}$$

if $\Delta_a \cdot \frac{P_S L_S}{P_I L_I} \geq \frac{\gamma_t}{\rho}$, otherwise the target SINR cannot be reached despite the level of digital cancellation [57].

Fig. 4.1 illustrates the maximum SINR that can be achieved after perfect digital interference cancellation ($\Delta_d = \rho$) depending on the distances between the three nodes. The results account only for the free-space path loss, assume no analog interference cancellation, and the effective dynamic range of the receiver is assumed to be $\rho = 48$ dB. The output power ratio of the signal of interest and interference is taken to be $P_S/P_I = -23$ dB. The plotted results illustrate to which extent an interference transmitter limits the receiver's sensitivity if the receiver only mitigates the interference using digital methods — whether or not digital cancellation alone is sufficient depends on the specific scenario, the SINR requirement and placement of the nodes.

4.2 Analog Suppression of Periodic Interference

To suppress interference before digitization in scenarios that call for it, a digitally assisted analog interference mitigation scheme is proposed as part of this work [**P1**]. The method relies on first estimating the instantaneous frequency of the narrowband interference $x(n)$, then producing a digital replica $\hat{x}(n)$ of that signal, and finally using an auxiliary transmit chain to inject an opposite-phase replica of the received interference as illustrated in Fig. 4.2. Of course, the signal of interest acts as noise for the interference estimation and this approach is feasible only if the received interference is sufficiently more powerful than the received signal of interest **[3]**. If that is not the case and the received signal of interest is more powerful than the received interference signal, then analog interference mitigation is unnecessary anyway.

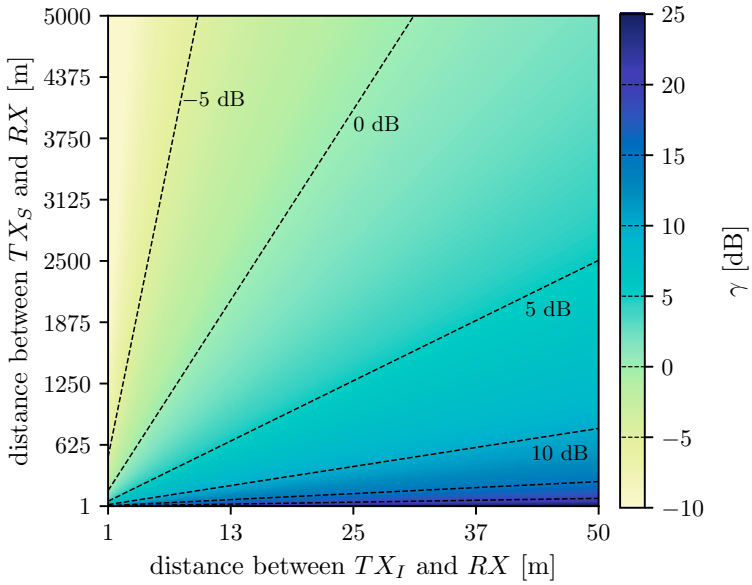


Figure 4.1 The maximum attainable SINR with ideal digital interference mitigation in terms of distances between the transmitters of the desired and interfering signals and the receiver. Assuming no analog interference mitigation, effective dynamic range $\rho = 48$ dB, $P_S/P_I = -23$ dB, and considering only free-space path loss. TX_S is the transmitter of signal of interest, TX_I is the transmitter of interference, and RX is the receiver.

In the proposed scheme, the received signal that is corrupted by interference is employed as reference signal for the adaptive filter and the estimated interference signal as input for the adaptive filter. The adaptive mechanism tunes the filter coefficients so that the filter output approximates the interference signal, forcing the error signal $e(n)$ to contain mostly the signal of interest. The proposed scheme relies on coupling some of the input signal energy to a secondary receiver chain that is not subject to interference cancellation, and therefore enables estimating the interference signal while at the same time mitigating it in the primary receiver path.

It is inevitable that the interference reconstruction in digital domain takes some time and therefore the computational delay in generating the interference replica $\hat{x}(n)$ becomes most probably longer than the path delay in the primary receiver chain for the actual interference $x(n)$. As a consequence, the system is effectively only capable of canceling periodic interference. Compared to strictly digital methods, analog interference mitigation is further complicated by the necessity to compensate for the transfer function of the secondary path $S(z)$, which includes everything in the signal path going through the auxiliary transmit chain to the primary receive chain.

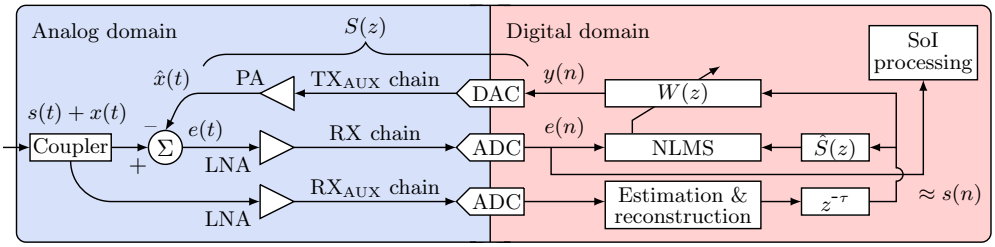


Figure 4.2 Digitally assisted analog interference mitigation scheme for signal of interest (SoI) processing. The PA in the auxiliary transmitter chain may be unnecessary depending on the received signal powers and the rest of the hardware.

Therefore, a filtered-x version of the least mean squares (LMS) algorithm is used to account for the transfer function in the secondary path [58]. The proposed scheme can potentially be repurposed to function with wideband interference, such as, e.g., pseudorandom jamming. However, this would require replacing the narrowband interference reconstruction with a respective signal generator and the filtered-x LMS algorithm would need to be extended to account for frequency offsets.

4.3 Digital Suppression of Known Interference

In order to provide a method for suppressing KI in scenarios where digital interference mitigation alone is sufficient, a novel algorithm is in this work proposed that is able to estimate and track a wireless channel under frequency offsets [**P5**], which is the main challenge in KI cancellation.

4.3.1 Estimating Wireless Channels under Frequency Offsets

In alignment with the system model illustrated in Fig. 2.8, the following starting point is formulated. The relative sampling frequency offset between the two devices is defined as $\eta+\beta(n)$, where $\eta=\Delta T/T_x$ represents the fundamental time-invariant sampling frequency offset, $\Delta T=1/f_d-1/f_x$ is the difference between the sampling periods at the receiver and transmitter, f_d is the sampling frequency at the receiver, f_x is the sampling frequency at the transmitter, and $\beta(n)$ is the time-varying offset, including sampling jitter. The carrier frequency offset is defined as $\epsilon+\phi(n)$, where ϵ denotes the fundamental time-invariant carrier frequency offset $\epsilon=\omega_d-\omega_x$ be-

tween the receiver and transmitter, ω_d is the carrier frequency at the receiver, ω_x is the carrier frequency at the transmitter, and $\phi(n)$ is the time-varying offset that also includes phase noise. Lastly, the complex-valued channel impulse response with order M is denoted as $\mathbf{w}$.

The transmitter broadcasts a complex signal $x(n)$ that is known to the receiver in its discrete-time form. However, because of noise, channel, and mismatches between carrier and sampling frequencies at the transmitter and the receiver, the digitized discrete-time signal at the receiver becomes

$$d(n) = \mathbf{w}^H \mathbf{y}_n e^{j\sum_{i=1}^{n}\epsilon(i)} + v(n), \tag{4.3}$$

where $v(n)$ is the measurement noise with variance σ_v^2, $\mathbf{y}_n$ accounts for sampling $x(t)$ with frequency offset $\eta + \beta(n)$ so that

$$\mathbf{y}_n = \left[x\left(\sum_{i=1}^{n-M+1}(1+\eta+\beta(i))\right), \ldots, x\left(\sum_{i=1}^{n}(1+\eta+\beta(i))\right)\right] \tag{4.4}$$

and $e^{j\sum_{i=1}^{n}\epsilon+\phi(i)}$ accounts for the carrier frequency offset. The received noise $v(n)$ can be considered to contain an unknown signal of interest that is uncorrelated to the known signal $x(n)$. Suppressing the known signal then makes it possible to process the signal of interest.

To derive an adaptive algorithm for estimating and tracking these system parameters, a cost function is defined as the mean squared error (MSE)

$$J(n) = E\left[|e(n)|^2\right] = E\left[e(n)e^*(n)\right] \tag{4.5}$$

of the estimation error

$$e(n) = d(n) - \hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{4.6}$$

where $\hat{\mathbf{w}}_{n-1}$, $\hat{\epsilon}(n-1)$, and $\hat{\eta}(n-1)$ are respectively the estimates of the channel's impulse response $\mathbf{w}$, carrier frequency offset ϵ, and sampling frequency offset η at iteration n, and $\hat{\mathbf{y}}_n$ is the result of resampling $x(n)$ with $\hat{\eta}(n-1)$. The purpose of the adaptive filter is then to iteratively update the parameter estimates so that the positive cost function $J(n)$ is successively reduced. This will in general ensure that the adaptive filter improves its parameter estimates after every iteration.

Applying the stochastic gradient descent method for sequential computation of the model parameters based on the cost function in (4.5) leads to the following update rules

$$\hat{\mathbf{w}}_n = \hat{\mathbf{w}}_{n-1} + \mu_w \hat{\mathbf{y}}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)} e^*(n), \tag{4.7a}$$

$$\hat{\epsilon}(n) = \hat{\epsilon}(n-1) + \mu_\epsilon \Im\left\{\hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)} e^*(n)\right\}, \tag{4.7b}$$

$$\hat{\eta}(n) = \hat{\eta}(n-1) + \mu_\eta \Re\left\{\hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}'_n e^{j\sum_{i=1}^{n}\epsilon(i-1)} e^*(n)\right\}, \tag{4.7c}$$

where $\hat{\mathbf{w}}_0$, $\hat{\epsilon}(0)$, and $\hat{\eta}(0)$ are initial guesses, μ_w, μ_ϵ, and μ_η are fixed positive step size parameters that influence the algorithm's performance, and $\hat{\mathbf{y}}'_n$ is the derivative of $\hat{\mathbf{y}}_n$. The adaptive algorithm presented in this work for jointly and explicitly estimating and tracking a channel impulse response, carrier frequency offset, and sampling frequency offset is listed as Algorithm 1 and its operation is illustrated in Fig. 4.3. An implementation of the algorithm is open-sourced as part of an adaptive filters toolkit[1] for GNU Radio.

Algorithm 1 LMS-type frequency offsets tracking

procedure FO-LMS($x, d, \mu_w, \mu_\varepsilon, \mu_\eta, M$)
  $\hat{\mathbf{w}}_0 \leftarrow \mathbf{0}_{1,M}$
  $\hat{\epsilon}(0) \leftarrow 0$, $\hat{\eta}(0) \leftarrow 0$
  $\phi(1) \leftarrow 0$, $t(1) \leftarrow 0$

  for $n \leftarrow 1$ to N **do**
    $\hat{\mathbf{y}}_n \leftarrow [x(t(n)), x(t(n)-(1+\eta(n-1))), \ldots,$
      $x(t(n)-(M+1)(1+\eta(n-1)))]$
    $e(n) \leftarrow d(n) - \hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\phi(n)}$
    $\hat{\mathbf{w}}_n \leftarrow \hat{\mathbf{w}}_{n-1} + \mu_w \hat{\mathbf{y}}_n e^{j\phi(n)} e^*(n)$
    $\hat{\epsilon}(n) \leftarrow \hat{\epsilon}(n-1) + \mu_\epsilon \Im\left\{\hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}_n e^{j\phi(n)} e^*(n)\right\}$
    $\hat{\eta}(n) \leftarrow \hat{\eta}(n-1) + \mu_\eta \Re\left\{\hat{\mathbf{w}}_{n-1}^H \hat{\mathbf{y}}'_n e^{j\phi(n)} e^*(n)\right\}$
    $\phi(n+1) \leftarrow \phi(n) + \hat{\epsilon}(n)$
    $t(n+1) \leftarrow t(n) + (1+\hat{\eta}(n))$
  end for
end procedure

[1] `https://github.com/karel/gr-adapt`

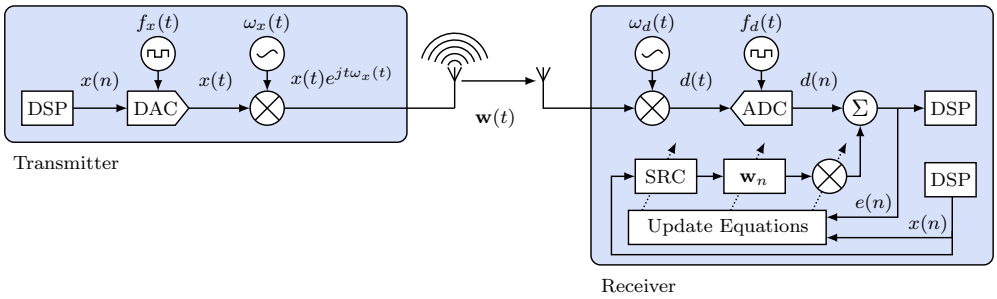


Figure 4.3 Estimation of a wireless channel under frequency offsets with the FO-LMS adaptive filter.

4.3.2 Steady-State Analysis under Self-Induced Nonstationarities

A crucial performance measure of adaptive filters that is often relied on in literature and that aids the practical use of these filters is the steady-state excess mean-square error (EMSE). This is the excess error of the MSE on top of the noise floor

$$\zeta = \text{MSE} - \sigma_v^2. \tag{4.8}$$

The steady-state performance of conventional adaptive filters is well understood and can be analyzed using the energy conservation relation method [59]. However, the adaptive filter proposed here is unique in the sense that the three update equations are coupled and the update equations self-inflict a nonstationarity among themselves. As such, the conventional steady-state analysis methods do not directly apply for the proposed filter. The well-known energy conservation relation method was extended in [**P5**] to account for those two issues and this provides an improved steady-state analysis framework. The full derivation is not reproduced here, but instead a brief overview of the final results is given.

Using the standard energy conservation relation method, the EMSE of conventional LMS adaptive filter with Gaussian white input signal can be show to be

$$\zeta^w = \frac{\mu_w M \sigma_x^2 \sigma_v^2}{2 - \mu_w (M+1)\sigma_x^2}, \tag{4.9}$$

where σ_x^2 is the input signal variance. Using the extended energy conservation relation method, the EMSE of the proposed FO-LMS adaptive filter is given by the sum

of the EMSEs related to each of the three update equations

$$\zeta^{w} = \frac{2\mu_{w} M \sigma_x^2 \sigma_v^2}{\gamma} + \frac{\frac{\mu_\epsilon}{\mu_w M}||\mathbf{w}||^2\sigma_v^2 + \frac{\mu_\eta}{\mu_w M} 2||\mathbf{w}||^2\sigma_v^2}{\gamma}, \tag{4.10a}$$

$$\zeta^{\epsilon} = \frac{2\mu_\epsilon \sigma_x^2 ||\mathbf{w}||^2 \sigma_v^2}{\gamma}, \tag{4.10b}$$

$$\zeta^{\eta} = \frac{4\mu_\eta \sigma_x^2 ||\mathbf{w}||^2 \sigma_v^2}{\gamma}, \tag{4.10c}$$

where the denominator γ is

$$\begin{aligned}\gamma = 4 &- 2\mu_w(M+1)\sigma_x^2 \\ &- 2\mu_\epsilon(1+\frac{1}{M})\sigma_x^2||\mathbf{w}||^2 - \frac{\mu_\epsilon}{\mu_w}(1+\frac{1}{M})||\mathbf{w}||^2 \\ &- 4\mu_\eta(1+\frac{1}{M})\sigma_x^2||\mathbf{w}||^2 - 2\frac{\mu_\eta}{\mu_w}(1+\frac{1}{M})||\mathbf{w}||^2.\end{aligned} \tag{4.11}$$

It can be seen that if the step sizes μ_ϵ and μ_η are set to zero, i.e., when only the channel estimation is activated, the EMSE given by (4.10) simplifies to the EMSE of the conventional LMS filter given in (4.9).

For any given system, the choice of step sizes is effectively the only way to steer the algorithm's performance. It might be desirable, e.g., to quicken the initial adaptation process with large step sizes that minimize the instantaneous error at every iteration as much as possible. However, step sizes that are too large will cause the algorithm to diverge and therefore it would be useful to have an easy-to-use and practical guideline for determining the suitable step size ranges without extensive steady-state analysis. Using Taylor series expansion-based analysis of the instantaneous error [60], in [**P5**] the following upper bounds for each step size were derived

$$0 < \mu_w \leq \frac{2 - \mu_\epsilon |\mathbf{w}_{n-1}^H \mathbf{y}_n|^2 - \mu_\eta |\mathbf{w}_{n-1}^H \mathbf{y}_n'|^2}{||\mathbf{y}_n||^2}, \tag{4.12a}$$

$$0 < \mu_\epsilon \leq \frac{2 - \mu_w ||\mathbf{y}_n||^2 - \mu_\eta |\mathbf{w}_{n-1}^H \mathbf{y}_n'|^2}{|\mathbf{w}_{n-1}^H \mathbf{y}_n|^2}, \tag{4.12b}$$

$$0 < \mu_\eta \leq \frac{2 - \mu_w ||\mathbf{y}_n||^2 - \mu_\epsilon |\mathbf{w}_{n-1}^H \mathbf{y}_n|^2}{|\mathbf{w}_{n-1}^H \mathbf{y}_n'|^2}. \tag{4.12c}$$

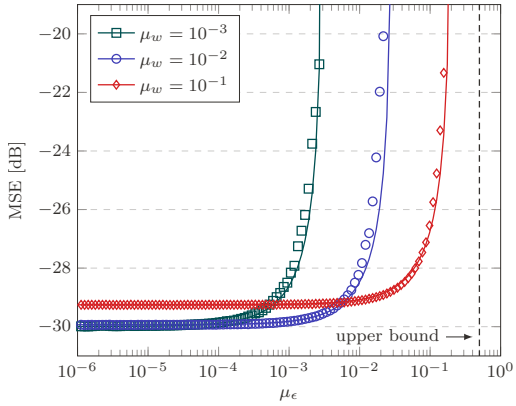
The upper bound limits above are necessary conditions for the stability of the proposed algorithm but not strictly sufficient. The actual values of the step sizes need to be slightly smaller because of the approximations used in their derivation. Also, the step sizes need to be selected collectively as their upper bounds are coupled through the step sizes. Still, they provide a useful guide for selecting the step sizes in practice.

To verify the theoretical steady-state EMSE expressions, the theoretical results are herein briefly compared to steady-state simulations, where the channel impulse response and frequency offsets are assumed known to the algorithm and time-varying terms are omitted. The simulations are carried out with varying channel impulse responses $\mathbf{w}$ of length $M = 3$ with a rather flat frequency response. The input signal $\mathbf{x}_n$ is Gaussian of unit variance and the noise $v(n)$ is Gaussian with variance $\sigma_v^2 = 10^{-3}$. The carrier frequency is taken to be 2.4 GHz and sampling frequency 2 MHz. The frequency offsets are equivalent to a 2.5 ppm oscillator inaccuracy, which is common in low cost software-defined radio platforms. Each simulation result is the steady-state statistical average of 1024 runs with 5000 iterations of the proposed algorithm in every run.

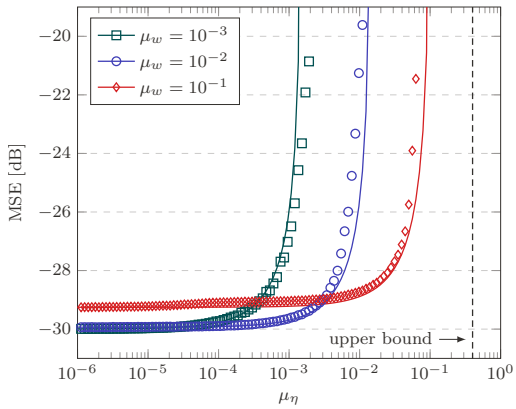
Fig. 4.4 compares the theoretical MSE obtained from (4.10) with the simulated MSE for various step size combinations and ranges. The results show that the theoretical and simulated results match closely, especially at smaller step sizes when the assumptions made during the derivation of (4.10) are better justified. The results also demonstrate the applicability of the upper bounds and how the step sizes need to be selected with some back-off from these in order for the algorithm to remain stable.

4.4 Results

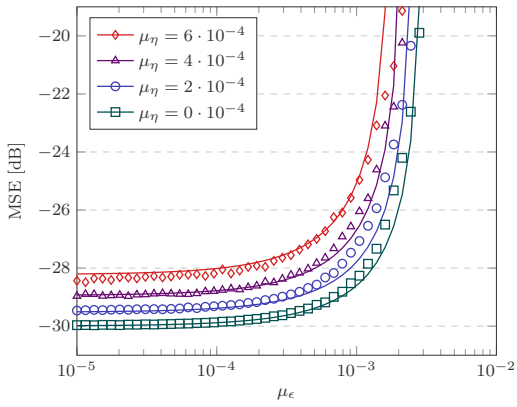
In this section, performance of both the digitally assisted analog interference and fully digital interference cancellation methods are studied based on measurements with practical hardware.



(a) No sampling frequency offset and $\mu_\eta = 0$



(b) No carrier frequency offset and $\mu_\epsilon = 0$



(c) All impairments and $\mu_w = 10^{-3}$

Figure 4.4 Steady-state analysis of FO-LMS.

4.4.1 Analog Interference Mitigation for Improved GNSS Reception

The impact of digitally assisted analog interference mitigation is in this work studied on GNSS signal processing [**P2**]. This is a fitting choice because the GNSS signals are typically received quite weakly, at around −130 dBm when acquired outdoors in open-sky conditions [61], and any in-band interference can easily saturate a GNSS receiver's front-end. Also, GNSS has become ubiquitous and it is essential to guarantee its functionality even in adverse conditions. One of the most widespread attacks against GNSS receivers is frequency-modulated jamming [62]. As such, the proposed scheme is well positioned to improve reception under common jamming attacks against GNSS. Specifically, the impact of frequency-modulated interference and its mitigation is analyzed on GPS L1 and Galileo E1 reception by combining the proposed interference mitigation scheme and a commercial off-the-shelf GNSS receiver.

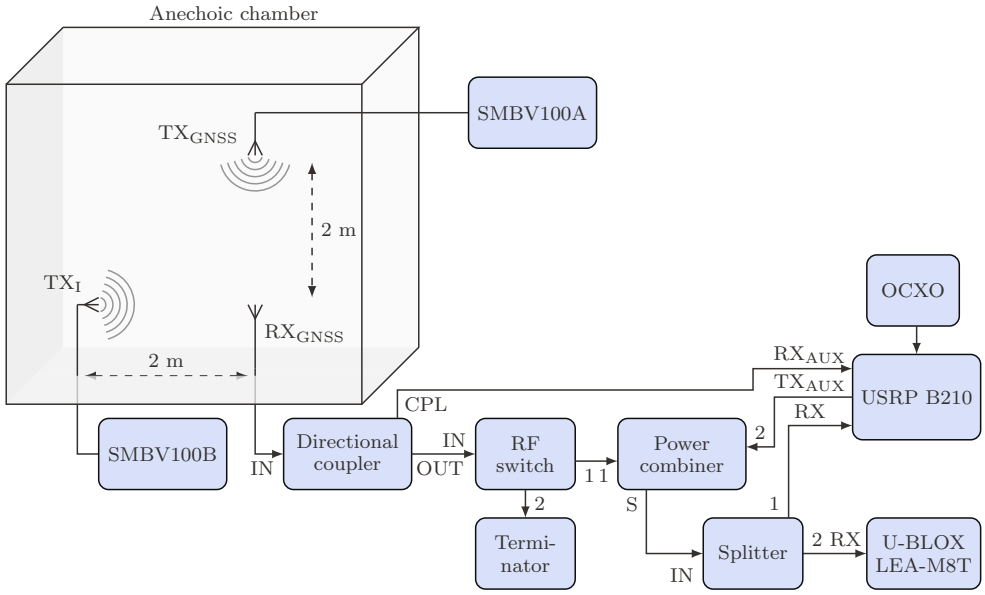


Figure 4.5 The setup for measuring the over-the-air performance of the digitally assisted analog interference mitigation scheme using GPS L1 and Galileo E1 as signals of interest.

The experiment was carried out using the measurement setup that is illustrated in Fig. 4.5 and described in more detail in **[P1]** and **[P2]**. The interference suppression scheme was implemented using an USRP B210 software-defined radio and the

scheme's performance was evaluated using a commercial GNSS receiver *U-Blox LEA-M8T*. The scheme's performance was also verified using an open-source software-defined GNSS signal processing toolbox *GNSS-SDR* [63] that processed the IQ samples from the USRP B210 directly. However, the two sets of results match rather closely and herein only the former are presented, while the combined set of results is available in [**P2**]. The GNSS receiver was restarted between each measurement to avoid it relying on or take advantage of previously acquired parameters. Otherwise, gradual increase in the JSR could potentially not immediately impact the positioning accuracy in the measurements.

In order to avoid interfering with other GNSS receivers in the vicinity and to be able to use a controlled GNSS source, the measurements were carried out in an anechoic chamber. An SMBV100A signal generator was used as a controlled GNSS source, which transmitted GPS L1 C/A and Galileo E1 signals simulating six satellites with specific location, time, and power. At the same time, a SMBV100B signal generator was used for transmitting a sinusoidally frequency-modulated interference with a frequency deviation of 125 kHz, modulation rate of 1 kHz, and center frequency of 1575.42 MHz. To receive the transmitted signals, an active GNSS antenna with 27 dBi gains and 1.5 dB noise figure was used. The antenna was connected to the interference mitigation platform after which the signals passed on to the commercial GNSS receiver.

The first GNSS receiver stage that is affected by the in-band interference is the AGC. The interference power level determines how well the AGC is able to minimize the quantization error of the GNSS signals in the ADC. The gain level set by the AGC in the U-Blox receiver with respect to the received JSR with and without interference mitigation is plotted in Fig. 4.6. As expected, these results show that, as the power of the received interference increases, the AGC decreases the gain to prevent saturating the ADC. It is also evident that with interference mitigation, the gain is decreased at a considerably higher pre-suppression JSR. The used GNSS receiver also has a built-in interference detector, which provides an interference detection confidence level. That interference confidence level is plotted in Fig. 4.6 alongside the AGC data for the same conditions. The interference detection does a formidable job and the interference detection confidence level increases with the increase of the interference power. Both of these metrics, the AGC and interference confidence levels, are improved to a similar extent by the proposed interference mitigation scheme

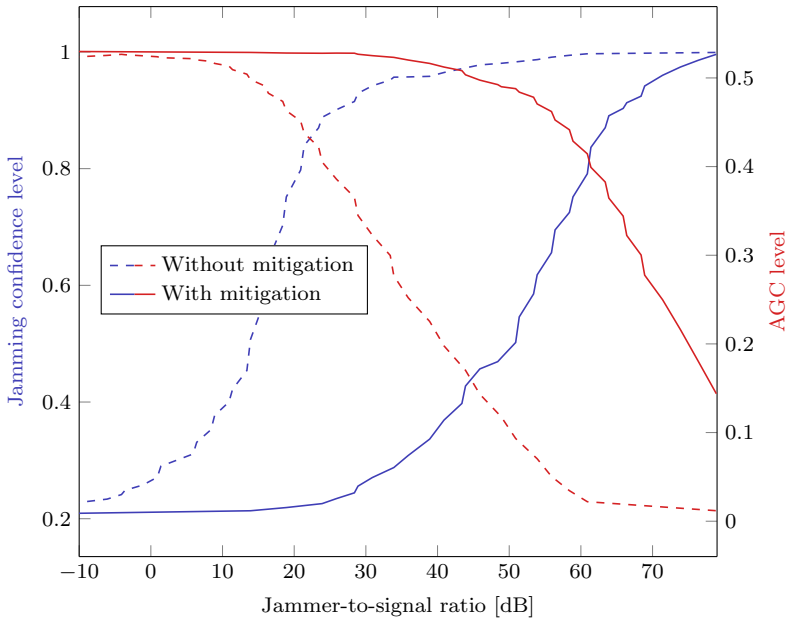


Figure 4.6 U-Blox LEA-M8T hardware monitoring results under jamming with and without its mitigation.

and indicate that the mitigation scheme extends the operational range of the GNSS receiver by 30 dB to 40 dB under frequency-modulated interference. However, this is only the first stage of GNSS signal processing and the question remains about how does the interference and its mitigation affect the successive processing stages and finally the positioning accuracy.

Analysis of the intermediate signal processing stages is covered in [**P2**], but are omitted here for brevity and focus is directly shifted to the positioning accuracy. Fig. 4.7 shows the average positioning accuracy of the GNSS receiver for both GPS L1 and Galileo E1 under interference with and without its mitigation. The interference suppression clearly allows the receiver to operate under much higher JSRs even though GPS L1 and Galileo E1 are affected differently by the interference mitigation, presumably because of the different modulations used therein. Altogether, the results demonstrate that the proposed interference mitigation scheme has the ability to prevent the RF front-end from saturating and subsequently enhance the positioning accuracy for both GPS L1 and Galileo E1 processing. The results also indicate that the operational JSR range of the GNSS receiver is extended proportionally to the amount of interference suppression, suggesting that the scheme itself does not produce considerable negative side-effects.

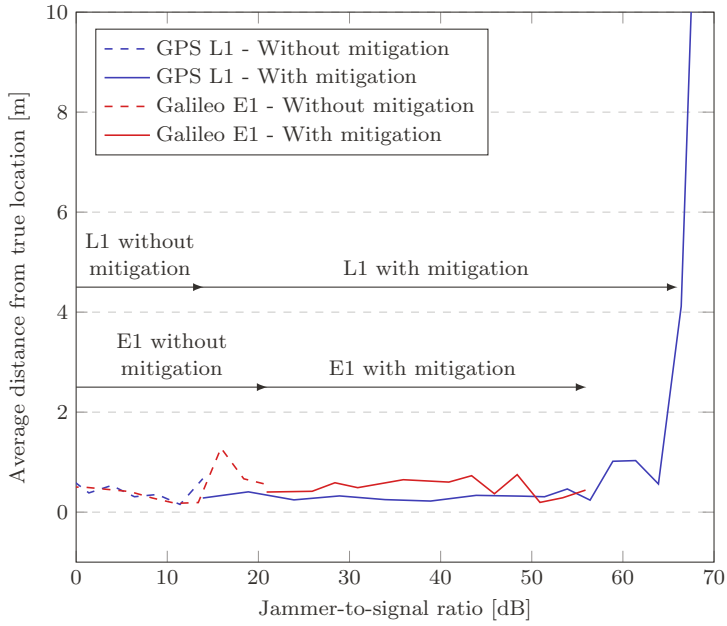
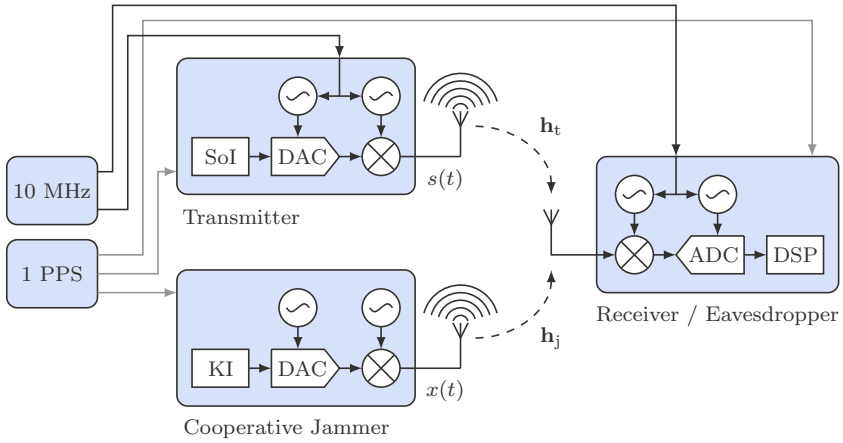


Figure 4.7 GPS L1 and Galileo E1 positioning accuracy with and without interference mitigation with regards to the received jammer-to-signal ratio (JSR).

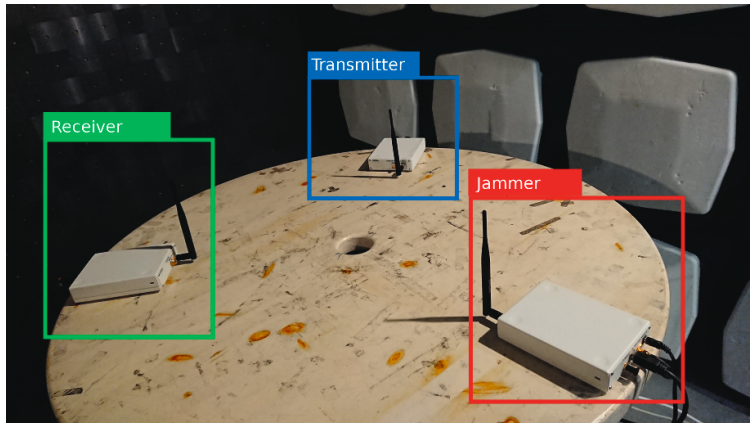
4.4.2 Digital Interference Mitigation for Securing Internet of Things

Impact of the proposed digital interference mitigation method is herein studied in the context of securing Internet of Things applications. These are a highly relevant group of applications which have seen explosive growth recently and where reliability and security are of major importance. As such, the signal of interest was implemented according to the IEEE 802.15.4 standard that specifies the physical layer and medium access control layer for low data rate wireless connectivity applications with limited energy consumption requirements [64]. Several widely used Internet of Things communications protocols, such as, e.g., Zigbee and 6LoWPAN, use IEEE 802.15.4 standard as the basis, making it a suitable target for this study. The standard specifies several physical layer implementations, from which the 2.4 GHz variant was chosen. That variant uses O-QPSK modulation and direct sequence spectrum spreading with about 9 dB of processing gain, offering 250 kbit/s data rate in a 2 MHz channel bandwidth. For KI, 4 MHz bandlimited Gaussian noise signal was used.

A comprehensive experiment [**P7**] was carried out using the setup illustrated and photographed in Fig. 4.8. The measurements were carried out in an anechoic cham-



(a) Diagram of the KIC experiment setup.



(b) Photograph of the KIC experiment setup.

Figure 4.8 KIC experiment setup.

ber and the three nodes were implemented using USRP-2900 software-defined radios with about 0.5 m between any two devices. The experiment was carried out on 2.45 GHz center frequency with 8 MHz sampling rate. The transmitter gains of both the transmitting nodes were varied over the roughly 90 dB gain range provided by the radios with a 5 dB step. Some additional measurements were also done with a 2.5 dB step. The measurements were recorded on disk by the receiver and the receiver gain was fixed at a level that took full advantage of the DAC dynamic range when both transmitting nodes were transmitting at their highest output power. In order to promote further research into this topic, the recorded measurements are published in [10].

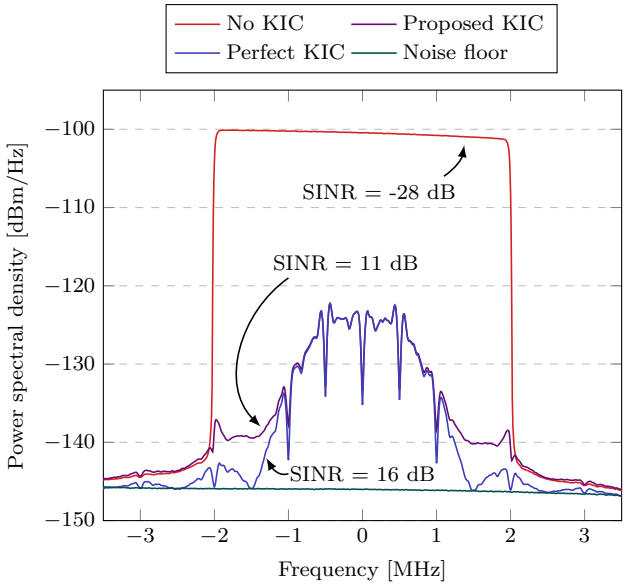
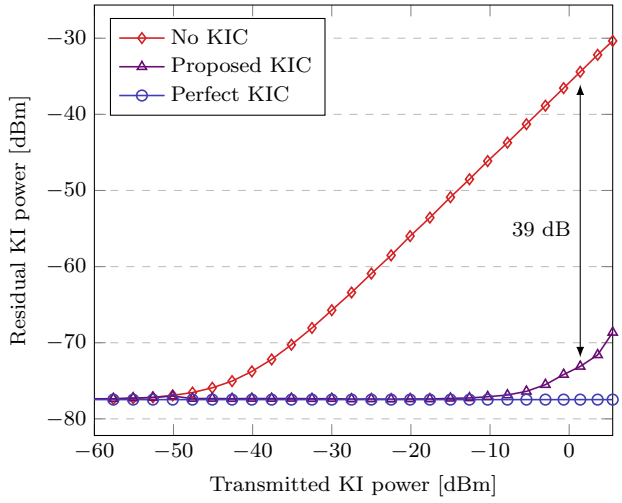


Figure 4.9 Power spectral densities of the superposed KI and signal of interest without KIC, with proposed KIC, and with perfect KIC.

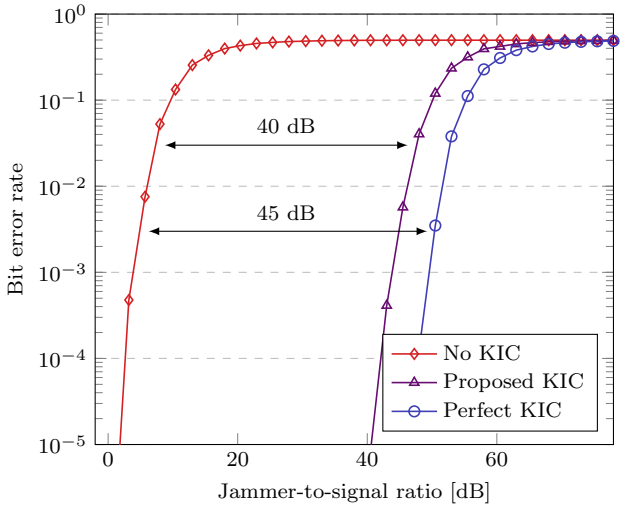
The power spectral density of the received superposition of the signal of interest and KI is plotted in Fig. 4.9. This plot shows the received signal without KIC, after the proposed KIC, and after perfect KIC (i.e., the signal of interest received without the KI). The signal transmit gains in this case are such that the received KI is much more powerful than the received signal of interest, hiding the latter completely when KIC is not used. The results with these gain settings already indicate that the proposed KIC method is able to suppress the KI considerably, although not perfectly, as the SINR does not reach quite of that as when the KI is not transmitted at all.

The residual KI power levels before and after cancellation and without a signal of interest are shown in Fig. 4.10a. These results provide an approximate upper limit on how well the KIC method can potentially perform if there is a signal of interest involved. Based on these measurements, the proposed FO-LMS algorithm is able to suppress the KI at most by about 39 dB. From that point, the algorithm becomes limited by the nonlinearities, phase noise, and sampling jitter within the KI. The measurements results also show that the algorithm is practical already with rather low interference-to-noise ratios.

The extended analysis, including the signal of interest and considering its BER, is captured in Fig. 4.10b. In this case, the gain of the signal of interest is varied and



(a) Without signal of interest.



(b) With signal of interest.

Figure 4.10 Performance of the proposed KIC method.

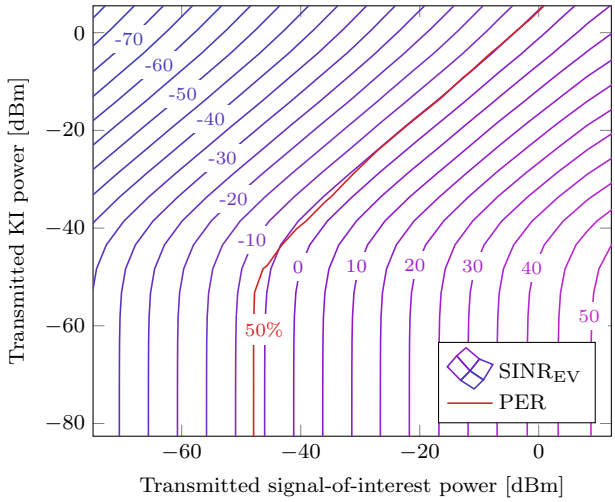
the gain of the KI is set to either 85 dB or 0 dB. Setting the KI gain to 85 dB allows to get the results with and without KIC, while setting the KI gain to 0 dB provides a reference case that would be achieved with perfect KIC. Firstly, the measurement results show that the BER curve is considerably impacted by the powerful interference signal, as expected. Secondly, the results show that KI suppression rather directly translates to improved signal-of-interest BER, i.e., the results in Fig. 4.10a and Fig. 4.10b are consistent, despite the added signal of interest. Finally, the consistency of these results also means that the residual KI prevents the BER from reaching that as after the perfect KIC.

Fig. 4.11 illustrates comprehensively the entire captured measurement set by plotting the SINRs before and after KIC for all the measured gain configurations. The figure also shows the 50% packet error rate threshold. The results show that without KIC there is a significant portion of the measurement grid where the SINR is too low to successfully demodulate most of the packets, but KIC improves the SINR sufficiently to facilitate successful demodulation. The results are also aligned with the previous results, showing that for powerful KI, the proposed KIC method is not able to cancel the KI all the way to the noise floor. This is evident in the SINR degradation. Altogether, the proposed KIC facilitates a significant improvement in the SINR and has the potential to therefore provide security already at the physical layer.

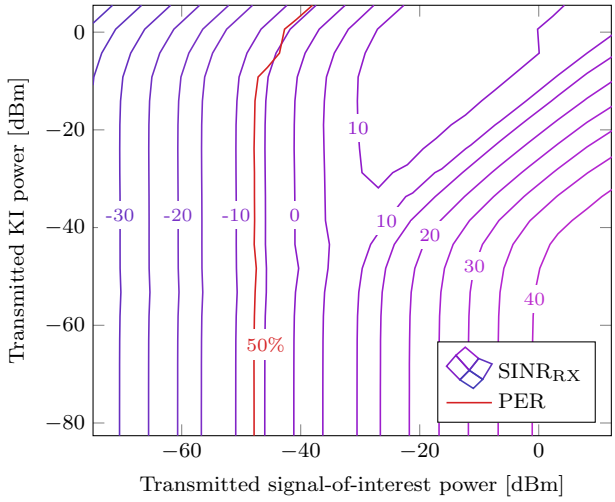
That potential becomes evident by calculating the secrecy capacity that the legitimate receiver has over the eavesdropper given that the receiver has either the proposed or perfect KIC. The secrecy capacity

$$C_s = \max\{\log_2(1+\mathrm{SINR}_{\mathrm{RX}}) - \log_2(1+\mathrm{SINR}_{\mathrm{EV}}), 0\} \tag{4.13}$$

that results then, is plotted in Fig. 4.12. In alignment with the previous results, it is evident that the proposed KIC does not always lead to the same secrecy capacity as the perfect KIC does. At low signal-of-interest and high KI powers, this happens because the reference method is not able to deal with the nonlinearities and noise in the KI. At high signal-of-interest and low KI powers, this happens because the signal-of-interest hampers the reference KIC. Still, the physical layer security provided by the reference KIC method is significant, especially when considering that without KIC the secrecy capacity is zero because then $\mathrm{SINR}_{\mathrm{RX}} = \mathrm{SINR}_{\mathrm{EV}}$ in the experiments.



(a) No KIC.



(b) Proposed KIC.

Figure 4.11 SINRs at the eavesdropper and receiver (i.e., without and with KIC) along with the PERs. P_{KI} and P_{SOI} are the transmitted signal powers.

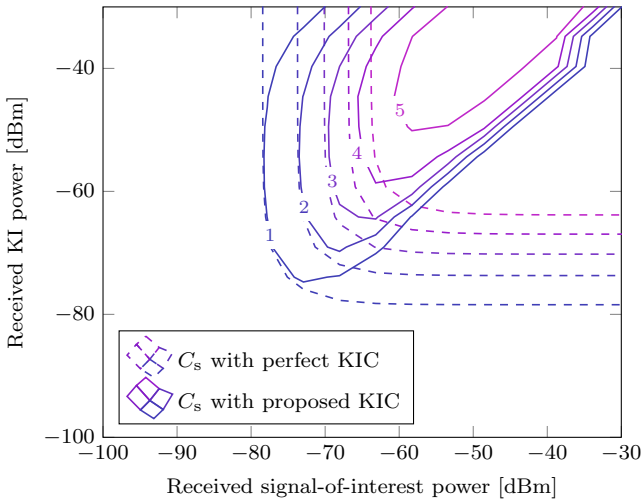


Figure 4.12 Secrecy capacity, C_s, in bps/Hz with perfect and proposed KIC.

5 CONCLUSIONS

In this final chapter, the contributions of this thesis to the physical layer security and reliability of wireless communications are summarized along with discussing possible future research directions.

5.1 Main Results

Chapter 3 built on the publications [**P3**], [**P4**], and [**P6**] to focus on the potential of multifunction IBFD radios by considering various simultaneous combinations of wireless operations, such as transmitting, receiving, detecting, and jamming. Initially, the potential impact of multifunction radios from an operational viewpoint was considered [**P4**]. Various use cases were presented where IBFD radio technology looks promising to improve the reliability and robustness of electronic countermeasure systems through simultaneous operation and multifunctionality. The concrete impact of multifunction radios on a technical level was studied from physical layer security and reliability viewpoint using an analytical framework revolving around two-way communications, signal detection, and jamming in a three-node system model [**P6**]. Each of the nodes within that system model were considered to possess either conventional HD or enhanced IBFD capabilities for achieving its objectives.

The benefits of multifunction IBFD radios in such scenarios have for long been speculated over, including the potential use cases presented in this work, but the analytical and experimental results provide a concrete understanding on the system-level benefits of some IBFD multifunction combinations. The results show that IBFD operation is not always beneficial to physical layer security and reliability, but that it can considerably improve the performance of certain systems that otherwise rely on separating wireless functions in time. Specifically, it can be concluded that combining signal detection and jamming on the same frequency simultaneously for smart

jamming is more effective than alternating between these functions in time, although the efficiency gain is rather limited. Still, to demonstrate the feasibility of such combinations in practice, a deep learning-based RF signal classification method was proposed and combined with simultaneous jamming on an IBFD prototype [**P3**]. The practical study reinforced that while residual SI does negatively impact signal classification, it comes at almost no cost to the jamming efficiency and can improve the situational awareness during jamming.

Chapter 4 expanded on the publications [**P1**], [**P2**], [**P5**], and [**P7**] and concentrated on cancellation of interference and purposefully using interference to provide physical layer security. This began by analyzing the relevance of interference mitigation in the analog and digital signal processing stages of the receiver and illustrated that, depending on the signal powers and node positions, it is either necessary to handle the interference already in the analog domain or it is sufficient to suppress the interference in the digital domain only [**P1**]. Then, two separate methods were proposed that mitigate interference in either of these domains — a method for mitigating periodic narrowband interference in the analog domain by using digitally assisted adaptive filtering [**P1**] and a method for mitigating known interference in the digital domain using a novel adaptive filter FO-LMS that, in addition to the channel, also estimates the frequency offsets [**P5**]. For the latter method, a novel approach was derived to analyze its theoretical steady-state performance, which is complicated due to the coupling of the algorithms update equations and self-induced nonstationarity. Also, an open-source implementation was provided.

Performance of both of the interference mitigation methods was studied in depth through measurements and both methods demonstrated the ability to significantly suppress received interference while ultimately becoming limited by nonlinearities, phase noise, and sampling jitter [**P2**], [**P7**]. Still, the practical analysis showed that interference mitigation with both methods directly translates to improvement in the signal of interest processing to the same extent that the methods suppressed the interference. Furthermore, this then results in a positive secrecy capacity that effectively allows securing wireless communications from unauthorized receivers by using cooperative jamming together with interference cancellation [**P7**]. Conclusively, these methods effectively allow to extend the IBFD radio concept to multiple radios and, through simultaneous information and interference transmission, provide security at the physical layer of wireless systems. In the advent of the quantum era, this can

provide a welcome alternative to encryption on which the security of most wireless systems relies. Furthermore, synchronization of known signals across devices does not only facilitate cooperative jamming but potentially also various other applications, one of those being bistatic radar setups [**P5**].

5.2 Future Research Directions

While this work has made various contributions to the research of enhancing the security and reliability of wireless communications, numerous challenges remain that need to be addressed to propel the technology to a level that satisfies the requirements of commercial systems. Among these is the need to advance the technical readiness level of SIC technology such that it would be usable in practice. For many applications, this means translating the existing technology to frequencies other than the 2.4 GHz where academic IBFD radio prototypes typically operate, extending the power range that the current state-of-the-art technology can handle, and reducing the form factor of the proof-of-concept SI cancellation hardware to fit into compact devices. Also, while 100 dB of SI cancellation is often considered enough for wireless communication systems, then combining electronic warfare (EW) tasks, as envisioned in form of multifunction radios, will require much better cancellation to be achieved.

The interference cancellation measurement results in this work demonstrated that co-site or known interference can be to a large extent mitigated by estimating and compensating for the channel and frequency offsets. However, the results also showed that by considering only these aspects, the interference cannot be always mitigated completely, as RF front-end nonlinearities, phase noise, and sampling jitter can ultimately limit performance. In order to suppress the interference further, interference cancellation methods need to be developed to also account for these impairments. Furthermore, the digital FO-LMS algorithm presented in this work was run offline on recorded measurements. In order to facilitate KIC in practical applications, the interference will need to be suppressed in real-time and this is a challenge that needs to be overcome in future algorithm development and implementations. Fortunately, the proposed FO-LMS algorithm is computationally inexpensive and, therefore, potentially lends itself well for implementation in real-time.

REFERENCES

[1] K. Pärlin, M. M. Alam and Y. Le Moullec. Jamming of UAV Remote Control Systems Using Software Defined Radio. *Proc. Int. Conference on Military Communications and Information Systems*. May 2018. DOI: 10.1109/ICMCIS.2018.8398711.

[2] K. Pärlin, T. Riihonen, R. Wichman and D. Korpi. Transferring the Full-Duplex Radio Technology from Wireless Networking to Defense and Security. *Proc. 52nd Asilomar Conference on Signals, Systems and Computers*. Oct. 2018, 2196–2201. DOI: 10.1109/ACSSC.2018.8645445.

[3] K. Pärlin, T. Riihonen and M. Turunen. Sweep Jamming Mitigation Using Adaptive Filtering for Detecting Frequency Agile Systems. *Proc. Int. Conference on Military Communications and Information Systems*. May 2019. DOI: 10.1109/ICMCIS.2019.8842761.

[4] M. Adrat, R. Keller, M. Tschauner, S. Wilden, V. Le Nir, T. Riihonen, M. Bowyer and K. Pärlin. Full-Duplex Radio Technology – Increasing the Spectral Efficiency for Military Applications. *Proc. Int. Conference on Military Communications and Information Systems*. May 2019. DOI: 10.1109/ICMCIS.2019.8842748.

[5] M. Adrat, R. Keller, S. Wilden, V. Le Nir, T. Riihonen, M. Bowyer and K. Pärlin. *Full Duplex Radio Technology – Increasing the Spectral Efficiency for Military Applications*. Tech. rep. NATO, Jan. 2020.

[6] K. Pärlin and T. Riihonen. Full-Duplex Transceivers for Defense and Security Applications. *Full-Duplex Communications for Future Wireless Networks*. Ed. by H. Alves, T. Riihonen and H. A. Suraweera. Springer, Apr. 2020. Chap. 9, 249–274. DOI: 10.1007/978-981-15-2969-6_9.

[7] T. Riihonen, M. Turunen, K. Pärlin, M. Heino, J. Marin and D. Korpi. Full-duplex operation for electronic protection by detecting communication jamming at transmitter. *Proc. 31st Annual Int. Symposium on Personal, Indoor and Mobile Radio Communications*. Sept. 2020. DOI: 10.1109/PIMRC48278.2020.9217316.

[8] J. Marin, K. Pärlin, M. Bernhardt and T. Riihonen. Neural networks in the pursuit of invincible counter-drone systems. *IEEE Potentials* 41.1 (Jan. 2022), 14–21. DOI: 10.1109/MPOT.2021.3113639.

[9] M. Tschauner, M. Adrat, V. Le Nir, K. Pärlin and T. Riihonen. Crosstalk and Self-Interference Cancellation in Full-Duplex Communication Systems. *Proc. Int. Conference on Military Communications and Information Systems*. May 2023.

[10] K. Pärlin, T. Riihonen, M. Turunen, V. Le Nir and M. Adrat. *Securing the Physical Layer of IEEE 802.15.4 Through Cooperative Jamming*. June 2023. DOI: 10.21227/9mty-pf96. URL: https://dx.doi.org/10.21227/9mty-pf96.

[11] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan and R. Wichman. In-band full-duplex wireless: Challenges and opportunities. *IEEE Journal on Selected Areas in Communications* 32.9 (Sept. 2014), 1637–1652. DOI: 10.1109/JSAC.2014.2330193.

[12] K. E. Kolodziej, B. T. Perry and J. S. Herd. In-band full-duplex technology: Techniques and systems survey. *IEEE Transactions on Microwave Theory and Techniques* 67.7 (July 2019), 3025–3041. DOI: 10.1109/TMTT.2019.2896561.

[13] W. Guo, C. Li, H. Zhao, R. Wen and Y. Tang. Comprehensive effects of imperfect synchronization and channel estimation on known interference cancellation. *IEEE Transactions on Vehicular Technology* 69.1 (Jan. 2020), 457–470. DOI: 10.1109/TVT.2019.2950046.

[14] R. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House, 2011.

[15] D. Torrieri. *Principles of spread-spectrum communication systems*. Springer, 2005. DOI: 10.1007/978-3-319-70569-9.

[16] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer and J. H. Reed. A Communications Jamming Taxonomy. *IEEE Security & Privacy* 14.1 (Feb. 2016), 47–54. DOI: 10.1109/MSP.2016.13.

[17] H. Saarnisaari. Sweep jamming hit rate analysis for frequency agile communications. *Proc. Int. Conference on Military Communications and Information Systems*. May 2016. DOI: 10.1109/ICMCIS.2016.7496578.

[18] B. A. Bash, D. Goeckel, D. Towsley and S. Guha. Hiding information in noise: Fundamental limits of covert wireless communication. *IEEE Communications Magazine* 53.12 (Dec. 2015), 26–31. DOI: 10.1109/MCOM.2015.7355562.

[19] P. E. Pace. *Detecting and classifying low probability of intercept radar*. Artech house, 2009.

[20] J. D. Vlok. Detection of direct sequence spread spectrum signals. PhD thesis. University of Tasmania, 2014.

[21] R. Poisel. *Introduction to communication electronic warfare systems*. Artech House, Inc., 2008.

[22] S.-H. Kong, M. Kim, L. M. Hoang and E. Kim. Automatic LPI radar waveform recognition using CNN. *Ieee Access* 6 (Jan. 2018), 4207–4219. DOI: 10.1109/ACCESS.2017.2788942.

[23] K. Merchant, S. Revay, G. Stantchev and B. Nousain. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing* 12.1 (Feb. 2018), 160–167. DOI: 10.1109/JSTSP.2018.2796446.

[24] Z. Zhang, K. Long, A. V. Vasilakos and L. Hanzo. Full-duplex wireless communications: Challenges, solutions and future research directions. *Proceedings of the IEEE* 104.7 (July 2016), 1369–1409. DOI: 10.1109/JPROC.2015.2497203.

[25] M. Duarte, C. Dick and A. Sabharwal. Experiment-driven characterization of dull-duplex wireless systems. *IEEE Transactions on Wireless Communications* 11.12 (Dec. 2012), 4296–4307. DOI: 10.1109/TWC.2012.102612.111278.

[26] J. Tamminen, M. Turunen, D. Korpi, T. Huusari, Y.-S. Choi, S. Talwar and M. Valkama. Digitally-controlled RF self-interference canceller for full-duplex radios. *Proc. 24th European Signal Processing Conference*. Aug. 2016, 783–787. DOI: 10.1109/EUSIPCO.2016.7760355.

[27] A. Balatsoukas-Stimming. Non-linear digital self-interference cancellation for in-band full-duplex radios using neural networks. *Proc. 19th Int. Workshop on Signal Processing Advances in Wireless Communications*. June 2018. DOI: 10.1109/SPAWC.2018.8445987.

[28] R. H. Louie, Y. Li and B. Vucetic. Practical physical layer network coding for two-way relay channels: performance analysis and comparison. *IEEE Transactions on Wireless Communications* 9.2 (Feb. 2010), 764–777. DOI: 10.1109/TWC.2010.02.090314.

[29] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng and F. Gong. Improving physical layer security of uplink NOMA via energy harvesting jammers. *IEEE Transactions on Information Forensics and Security* 16 (Sept. 2020), 786–799. DOI: 10.1109/TIFS.2020.3023277.

[30] L. Sun, Y. Zhang and A. L. Swindlehurst. Alternate-jamming-aided wireless physical-layer surveillance: Protocol design and performance analysis. *IEEE Transactions on Information Forensics and Security* 16 (Dec. 2020), 1989–2003. DOI: 10.1109/TIFS.2020.3046880.

[31] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu and Y. Tang. Effect of frequency offset on cooperative jamming cancellation in physical layer security. *Proc. IEEE Globecom Workshops*. Dec. 2018. DOI: 10.1109/GLOCOMW.2018.8644513.

[32] N. R. Yousef and A. H. Sayed. Ability of adaptive filters to track carrier offsets and channel nonstationarities. *IEEE Transactions on Signal Processing* 50.7 (July 2002), 1533–1544. DOI: 10.1109/TSP.2002.1011194.

[33] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li and F. Lin. Wireless powered cooperative jamming for secure OFDM system. *IEEE Transactions on Vehicular Technology* 67.2 (Sept. 2017), 1331–1346. DOI: 10.1109/TVT.2017.2756877.

[34] M. Liu and Y. Liu. Power allocation for secure SWIPT systems with wireless-powered cooperative jamming. *IEEE Communications Letters* 21.6 (June 2017), 1353–1356. DOI: 10.1109/LCOMM.2017.2672660.

[35] A. El Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir and R. Hamila. Securing untrusted RF-EH relay networks using cooperative jamming signals. *IEEE Access* 5 (Nov. 2017), 24353–24367. DOI: 10.1109/ACCESS.2017.2768508.

[36] W. Guo, H. Zhao and Y. Tang. Testbed for cooperative jamming cancellation in physical layer security. *IEEE Wireless Communications Letters* 9.2 (Feb. 2020), 240–243. DOI: 10.1109/LWC.2019.2950303.

[37] G. C. Tavik, C. L. Hilterbrick, J. B. Evins, J. J. Alter, J. G. Crnkovich, J. W. de Graaf, W. Habicht, G. P. Hrin, S. A. Lessin, D. C. Wu et al. The advanced multifunction RF concept. *IEEE Transactions on Microwave Theory and Techniques* 53.3 (Mar. 2005), 1009–1020. DOI: 10.1109/TMTT.2005.843485.

[38] D. Gupta, D. E. Kirichenko, V. V. Dotsenko, R. Miller, S. Sarwana, A. Talalaevskii, J. Delmas, R. J. Webber, S. Govorkov, A. F. Kirichenko et al. Modular, multi-dunction digital-RF receiver systems. *IEEE Transactions on Applied Superconductivity* 21.3 (Dec. 2010), 883–890. DOI: 10.1109/TASC.2010.2095399.

[39] P. M. McCormick, S. D. Blunt and J. G. Metcalf. Simultaneous Radar and Communications Emissions from a Common Aperture, Part I: Theory. *Proc. IEEE Radar Conference*. May 2017, 1685–1690. DOI: 10.1109/RADAR.2017.7944478.

[40] P. M. McCormick, B. Ravenscroft, S. D. Blunt, A. J. Duly and J. G. Metcalf. Simultaneous Radar and Communication Emissions from a Common Aperture, Part II: Experimentation. *Proc. IEEE Radar Conference*. May 2017, 1697–1702. DOI: 10.1109/RADAR.2017.7944480.

[41] M. Brandolini, P. Rossi, D. Manstretta and F. Svelto. Toward multistandard mobile terminals—Fully integrated receivers requirements and architectures. *IEEE Transactions on Microwave Theory and Techniques* 53.3 (Mar. 2005), 1026–1038. DOI: 10.1109/TMTT.2005.843505.

[42] T. Ulversoy. Software defined radio: Challenges and opportunities. *IEEE Communications Surveys & Tutorials* 12.4 (May 2010), 531–550. DOI: 10.1109/SURV.2010.032910.00019.

[43] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu and D. Matolak. Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine* 56.4 (Apr. 2018), 75–81. DOI: 10.1109/MCOM.2018.1700455.

[44] T. Riihonen. Military Applications. *In-Band Full-Duplex Wireless Systems Handbook*. Ed. by K. E. Kolodziej. Artech House, Mar. 2021. Chap. 17.

[45] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir and I. Guvenc. Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference. *IEEE Open Journal of the Communications Society* 1 (Nov. 2019), 60–76. DOI: 10.1109/OJCOMS.2019.2955889.

[46] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini and P. Dobbins. A survey of channel modeling for UAV communications. *IEEE Communications Surveys & Tutorials* 20.4 (July 2018), 2804–2821. DOI: 10.1109/COMST.2018.2856587.

[47] A. Krizhevsky, I. Sutskever and G. E. Hinton. ImageNet classification with deep convolutional neural networks. *Communications of the ACM* 60.6 (June 2017), 84–90. DOI: 10.1145/3065386.

[48] K. Simonyan and A. Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (Sept. 2014). DOI: 10.48550/arXiv.1409.1556.

[49] T. J. O'Shea, T. Roy and T. C. Clancy. Over-the-air deep learning based radio signal classification. *IEEE Journal of Selected Topics in Signal Processing* 12.1 (Feb. 2018), 168–179. DOI: 10.1109/JSTSP.2018.2797022.

[50] C. Wang, J. Wang and X. Zhang. Automatic radar waveform recognition based on time-frequency analysis and convolutional neural network. *Proc. Int. Conference on Acoustics, Speech and Signal Processing*. Mar. 2017, 2437–2441. DOI: 10.1109/ICASSP.2017.7952594.

[51] B. K. Kim, H.-S. Kang and S.-O. Park. Drone classification using convolutional neural networks with merged Doppler images. *IEEE Geoscience and Remote Sensing Letters* 14.1 (Jan. 2016), 38–42. DOI: 10.1109/LGRS.2016.2624820.

[52] T. J. O'Shea, J. Corgan and T. C. Clancy. Convolutional radio modulation recognition networks. *Proc. Int. Conference on Engineering Applications of Neural Networks*. Sept. 2016, 213–226. DOI: 10.1007/978-3-319-44188-7_16.

[53] A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle and L. A. DaSilva. Spectrum monitoring for radar bands using deep convolutional neural networks. *Proc. IEEE Global Communications Conference*. Dec. 2017. DOI: 10.1109/GLOCOM.2017.8254105.

[54] E. Everett, A. Sahai and A. Sabharwal. Passive self-interference suppression for full-duplex infrastructure nodes. *IEEE Transactions on Wireless Communications* 13.2 (Feb. 2014), 680–694. DOI: 10.1109/TWC.2013.010214.130226.

[55] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y.-S. Choi, L. Anttila, S. Talwar and M. Valkama. Full-duplex mobile device: Pushing the limits. *IEEE Communications Magazine* 54.9 (Sept. 2016), 80–87. DOI: 10.1109/MCOM.2016.7565192.

[56] D. Korpi, T. Riihonen, V. Syrjälä, L. Anttila, M. Valkama and R. Wichman. Full-duplex transceiver system calculations: Analysis of ADC and linearity challenges. *IEEE Transactions on Wireless Communications* 13.7 (July 2014), 3821–3836. DOI: 10.1109/TWC.2014.2315213.

[57] T. Riihonen and R. Wichman. Analog and digital self-interference cancellation in full-duplex MIMO-OFDM transceivers with limited resolution in A/D conversion. *Proc. 46th Asilomar Conference on Signals, Systems and Computers*. Nov. 2012, 45–49. DOI: 10.1109/ACSSC.2012.6488955.

[58] D. R. Morgan and C. Sanford. A control theory approach to the stability and transient analysis of the filtered-X LMS adaptive notch filter. *IEEE Transactions on Signal Processing* 40.9 (Sept. 1992), 2341–2346. DOI: 10.1109/78.157237.

[59] N. R. Yousef and A. H. Sayed. A unified approach to the steady-state and tracking analyses of adaptive filters. *IEEE Transactions on Signal Processing* 49.2 (Feb. 2001), 314–324. DOI: 10.1109/78.902113.

[60] E. Soria-Olivas, J. Calpe-Maravilla, J. F. Guerrero-Martinez, M. Martinez-Sober and J. Espi-Lopez. An easy demonstration of the optimum value of the adaptation constant in the LMS algorithm [FIR filter theory]. *IEEE Transactions on Education* 41.1 (Feb. 1998), 81. DOI: 10.1109/13.660794.

[61] J. S. Warner and R. G. Johnston. GPS spoofing countermeasures. *Homeland Security Journal* 25.2 (Jan. 2003), 19–27.

[62] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell and B. W. O'Hanlon. Signal characteristics of civil GPS jammers. *Proc. Radionavigation Laboratory Conference*. Sept. 2011, 1907–1919.

[63] C. Fernández–Prades, J. Arribas, P. Closas, C. Avilés and L. Esteve. GNSS-SDR: An open source tool for researchers and developers. *Proc. 24th Int. Technical Meeting of The Satellite Division of the Institute of Navigation*. Sept. 2011, 780–794.

[64] IEEE Standard for Low-Rate Wireless Networks. *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)* (2020), 1–800. DOI: 10.1109/IEEESTD.2020.9144691.

PUBLICATIONS

PUBLICATION 1

Digitally Assisted Analog Mitigation of Narrowband Periodic Interference

K. Pärlin and T. Riihonen

In *Proc. Int. Symposium on Wireless Communication Systems*, Aug. 2019, 682–686
DOI: 10.1109/ISWCS.2019.8877336

Digitally Assisted Analog Mitigation of Narrowband Periodic Interference

Karel Pärlin* and Taneli Riihonen†
*Rantelon, Tallinn, Estonia
†Electrical Engineering, Tampere University, Finland
e-mail: karel.parlin@rantelon.ee, taneli.riihonen@tuni.fi

***Abstract*—Interference mitigation in radio-frequency (RF) receivers has been studied extensively in various contexts. And although most of the in-band interference mitigation techniques rely on suppressing the interference in the digital domain, strong in-band interference can saturate a receiver's front-end and, thus, prevent it from receiving comparatively weak signals of interest. This is especially so in case of the self-interference (SI) encountered in enclosed full-duplex (FD) radios, but also in case of co-located jammers or radars and signals intelligence receivers. This work presents a digitally assisted method and its implementation for the mitigation of narrowband periodic interference before quantization in order to improve the sensitivity of receivers co-located with strong interference sources. Experimental results are provided and the potential for mitigating more complex waveforms, e.g., pseudorandom jamming, is discussed.**

I. Introduction

Impelled by the threat of adversarial jamming and the increased congestion of the radio-frequency (RF) spectrum, the mitigation of in-band interference in RF receivers has received considerable attention in defense and security research. Based on their usage domain, the mitigation techniques fall into two categories. Digital interference mitigation can be sufficient against adversarial jamming [1], whereas high-power interference from co-located transmitters can lead to adjusting the receiver's analog-to-digital converter (ADC) range to prevent overloading. Thus, the receiver would benefit from suppressing the interference in the analog domain before quantization to improve the effective resolution of the signal of interest [2].

The interference problem encountered in the case of co-located transmitters and receivers is similar to the self-interference (SI) challenge in full-duplex (FD) radios that operate in same-frequency simultaneous transmit and receive (SF-STAR) mode [3]. Such operation is expected to increase the spectral efficiency in wireless communications but SF-STAR has also been envisioned to reshape both the wireless defense and security domains, e.g., in the form a so-called FD radio shield [4]. Inside the radio shield, a central node would be capable of receiving wireless signals while jamming the reception of those or other malign signals for others. The concept can be further elaborated to include pseudorandom jamming signals, which the authorized users inside the FD radio shield can suppress. This again potentially raises the receiver overloading issue.

This research work was partly supported by the Academy of Finland under the grant 315858 "Radio Shield Against Malign Wireless Communication."

The aim of this work is to develop a method for mitigating narrowband interference in receivers co-located with high power transmitters as envisioned in Fig. 1, i.e., without having direct access to a copy of the interfering transmission as opposed to FD radios. We propose a digitally assisted analog interference cancellation technique using a single input antenna and adaptive filtering by extending our previous work on digital cancellation [5]. Experimental results characterize the performance of the proposed method in a laboratory environment and reveal that phase noise, which in the case of FD radios with a shared local oscillator (LO) is inherently mitigated [6], is one of the main limiting factors for interference mitigation. With co-located devices, sharing the LO can be impractical, otherwise the interfering signal could also be shared to simplify its mitigation.

The remainder of this paper is organized as follows. In Section II, the interference mitigation technique is introduced. The experimental setup that was used assess this method is discussed in Section III and the results are presented in Section IV. Finally, the paper is concluded in Section V.

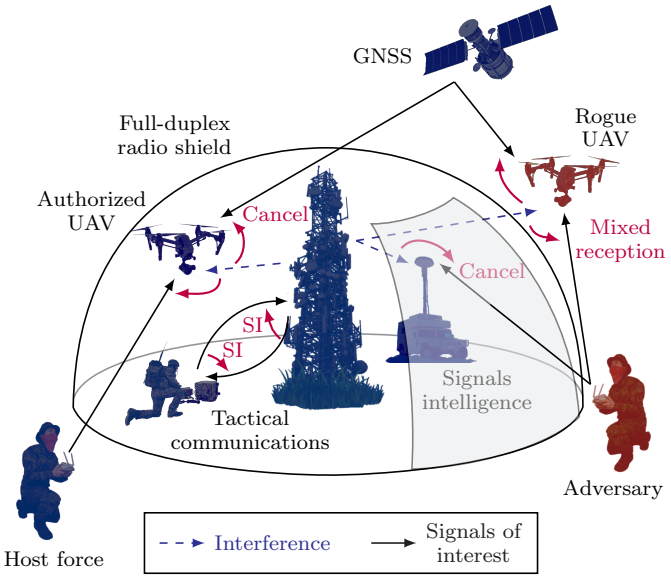


Fig. 1. The mitigation of co-located interference facilitates, e.g., the remote control of unmanned aerial vehicles (UAVs), the reception of global navigation satellite system (GNSS) signals, tactical wireless communications, and many other radio systems in the electronic battlefield as well as in civilian security.

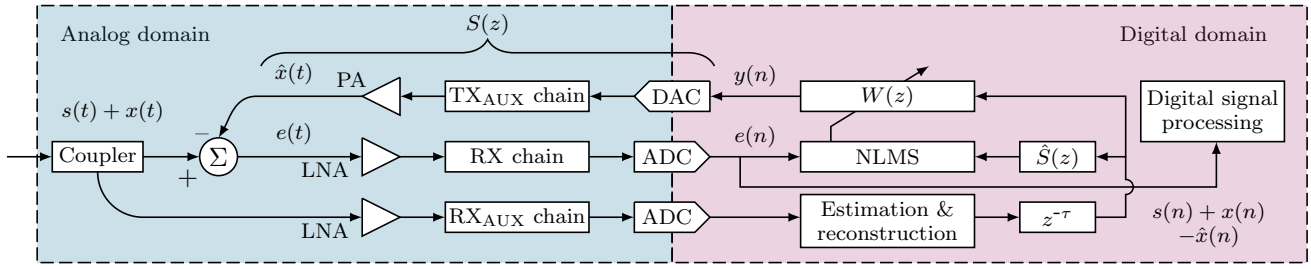


Fig. 2. Digitally assisted analog mitigation of instantaneously narrowband periodic interference based on adaptive filtering.

II. Narrowband Interference Mitigation

The mitigation of co-located interference in the analog domain prior to digitization offers an opportunity to improve the receiver sensitivity of co-located radios [7]–[9]. This section briefly analyzes the circumstances under which analog interference mitigation becomes necessary and proposes a digitally assisted analog interference mitigation technique (Fig. 2).

A. SINR Analysis

As the receiver's automatic gain control (AGC) keeps the total ADC input at constant full range level, high interference power means more ADC dynamic range is consumed by the interference signal. This leads to reduced effective resolution for the signal of interest, which may limit the receiver's performance [10]. The signal-to-interference-plus-noise ratio (SINR) can be calculated [11] as follows:

$$\gamma = \frac{\rho}{\frac{P_S L_S}{P_I L_I/\Delta_a} + \rho/\Delta_d + 1} \cdot \frac{P_S L_S}{P_I L_I/\Delta_a}, \tag{1}$$

where $P_S L_S/(P_I L_I/\Delta_a)$ represents SINR after path losses and analog cancellation, ρ is the effective dynamic range, and Δ_d is the amount of digital cancellation. Whether or not digital cancellation is sufficient depends on the targeted SINR γ_t of the application. The minimal level of digital suppression needed to achieve $\gamma \geq \gamma_t$ given $P_S L_S/P_I L_I$, Δ_a, and ρ can be solved from (1) as

$$\Delta_d \geq \frac{\rho}{\frac{P_S L_S}{P_I L_I/\Delta_a} \cdot (\frac{\rho}{\gamma_t} - 1) - 1}, \tag{2}$$

if $\Delta_a \cdot \frac{P_S L_S}{P_I L_I} \geq \frac{\gamma_t}{\rho}$, otherwise the target SINR cannot be achieved regardless of the level of digital suppression [11].

Taking free-space path loss into account and assuming no analog cancellation, Fig. 3 illustrates the maximum attainable SINR after ideal digital interference cancellation ($\Delta_d = \rho$) in terms of distances between the transmitters of the signals of interest TX_S and interference TX_I from the receiver RX. The output power ratio between the transmitters is taken to be $P_S/P_I = -23$ dB and the effective dynamic range of the receiver is assumed to be $\rho = 48$ dB, corresponding to a 12-bit ADC with effective number of bits (ENOB) equalling 10 [3]. The calculated results illustrate the extent to which a co-located transmitter limits the receiver's sensitivity if only digital interference mitigation is used.

B. Digitally Assisted Analog Interference Mitigation

Expanding on our previous work in digital narrowband interference mitigation, which relies on estimating the instantaneous frequency of the strong interfering signal, reconstructing such a signal, and using adaptive filtering to suppress the interference [5], we propose to use an auxiliary transmit chain to subtract the reconstructed, delayed, and filtered interference from the received signal in the analog domain as illustrated in Fig. 2. Similar methods have been successfully applied in FD radio prototypes to cancel the SI [12], in adaptive noise control (ANC) to suppress acoustic noise by introducing "antinoise" of equal amplitude and opposite phase [13], and have also been considered in theory for evading radars by cancelling their echoes [14]. However, this work combines RF interference estimation and its mitigation before quantization and provides experimental results.

The proposed method is based on the estimating the instantaneous frequency of the narrowband jamming signal $x(n)$ and constructing a digital representation $\hat{x}(n)$ of the jamming signal such that it exactly follows the estimated frequencies. As previously shown in [5], it is possible to estimate the instantaneous frequency of narrowband interference as long as

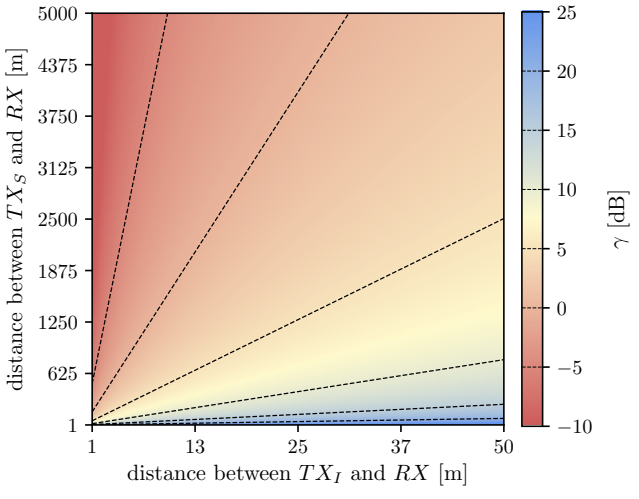


Fig. 3. The maximum attainable SINR in terms of distances between the transmitters of the desired and interfering signals and the receiver. Assuming no analog interference mitigation and ideal digital interference mitigation. Here $P_S/P_I = -23$ dB and only free-space path loss is considered.

the interference is sufficiently more powerful than the signal of interest. In order to obtain an interference-free version of $s(n)$, the clean input signal corrupted by interference $s(n)+x(n)$ is employed as the reference signal for the adaptive filter, whose input is the estimated jamming signal $\hat{x}(n)$ that is strongly correlated to the actual jamming signal $x(n)$. The adaptive mechanism adjusts the filter coefficients of $W(z)$ in such a manner that the filter output $y(n)$ approximates the jamming signal $x(n)$, thus forcing the error signal $e(n)$ to resemble the signal of interest $s(n)$. The system uses a directional coupler to direct some of the input signal energy to a secondary receiver port RX_{AUX} that is not affected by the cancellation and thus allows to continue estimating the interfering signal simultaneously to its mitigation in the primary path RX.

Unfortunately, the digital interference reconstruction takes a considerable amount of time and consequently the computational delay in generating the $\hat{x}(n)$ becomes longer than the path delay in the primary receiver chain for the actual interference $x(n)$. Therefore, the system's response is noncausal and the system is capable of effectively canceling only narrowband or periodic interference [13]. Furthermore, for the interference estimation, the actual signals of interest act as noise.

Compared to digital interference mitigation, the use of adaptive filtering for analog interference mitigation is further complicated by the fact that the summation of signals represents RF superposition and it is necessary to compensate for the secondary-path transfer function $S(z)$, which includes the digital-to-analog converter (DAC), TX_{AUX} chain, power amplifier (PA), power combiner, low-noise amplifier (LNA), RX chain, and ADC. Thus, the purely digital adaptive filter based on the normalized least mean squares (LMS) algorithm is extended to a filtered-x version, where a transfer function is present in the cancellation path.

The filtered-x least mean squares (FxLMS), however, becomes unstable at step sizes much lower than without the secondary path, thus limiting the convergence speed [15]. That is because the secondary path influences the dynamic response of the cancellation system by reducing the maximum step size in the FxLMS algorithm. On the other hand, the FxLMS algorithm is rather tolerant to errors made in the estimation of $S(z)$ by the filter $\hat{S}(z)$, as within the limit of slow adaptation, the algorithm converges with nearly 90° of phase error between $S(z)$ and $\hat{S}(z)$ [13]. Therefore, offline modeling can be used to estimate $S(z)$ during an initial training stage as the signal path from the auxiliary transmitter TX_{AUX} to the primary receiver RX can be considered static.

A single-frequency reference based adaptive canceller using the LMS algorithm has the properties of a notch filter at the reference frequency and the level of interference is reduced at the expense of introducing some distortion on the desired signal [16]. The same applies to the FxLMS with an intervening transfer function in the cancellation path [15]. The system in general can possibly be repurposed to work with broadband interference, such as pseudorandom jamming, e.g., by replacing the narrowband interference reconstruction with a respective signal generator.

III. Experimental Setup

In order to characterize the performance of the proposed RF interference mitigation technique, we carried out experiments in a laboratory environment. The experimental setup as illustrated in Fig. 4 simulates a scenario, in which a co-located jammer is interfering with a receiver, omitting any signals of interest. All the devices involved in the measurements were connected through coaxial cables, thus providing a controlled environment in which all other sources of interference, besides the devices under test, were eliminated. This also ensured precise control of the power levels during the measurements. Furthermore, effects in the radio channel, such as multipath propagation and fading, do not have an effect on the measurement results and a wide frequency range from 100 MHz to 2400 MHz could be studied without restrictions.

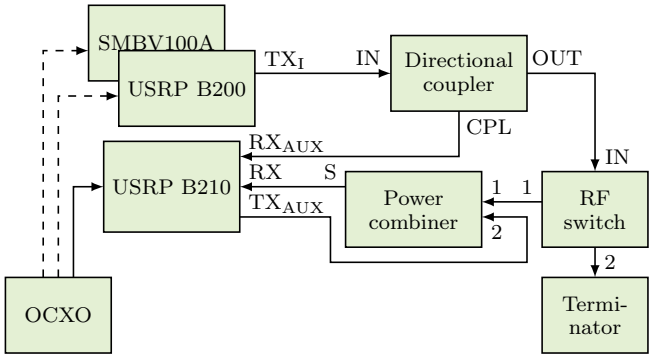


Fig. 4. The measurement setup in which either the SMBV100A vector signal generator or the USRP B200 software-defined radio is used to generate the interference. An oven-controlled crystal oscillator (OCXO) is used as an external reference either for the receiver only or for both the interference generator and the receiver.

A. Experimental Receiver

The receiver prototype used in the measurements is built using the USRP B210 commercial off-the-self (COTS) dual-channel software-defined radio (SDR) that receives signals in a 2 MHz bandwidth. In order to improve its phase noise characteristics, a 10 MHz oven-controlled crystal oscillator (OCXO) based reference clock is used as an external reference. Furthermore, in order to examine the effect of using a shared reference clock for both the receiver and the interference generator, as is typically the case in FD radios, measurements were carried out by using the OCXO as reference for only the receiver or both the receiver and the interference generator.

The input signal, i.e., the interference, is split in two using a directional coupler and a wideband electromechanical RF switch is used to control the input signal flow into the primary receiver path RX. This allows to carry out offline secondary path modelling during an initial training stage. A two-way power combiner is used to combine the received signal and the generated cancellation signal. The resulting signal path from the interference generator's TX_I to the receiver's RX attenuates the signal by 5 dB to 8 dB in the frequency range of 100 MHz to 2400 MHz.

B. Interference

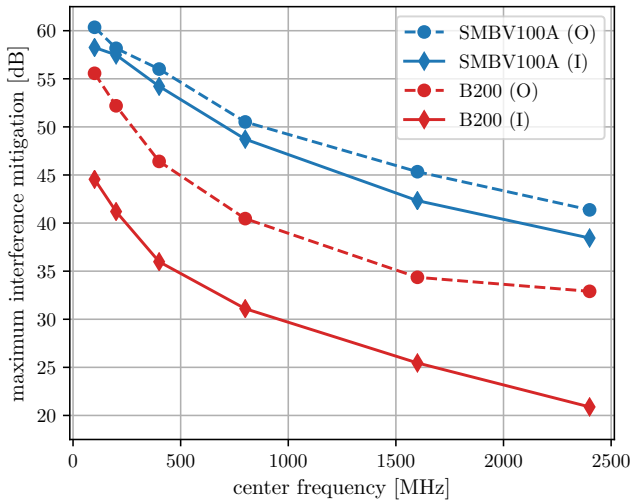
The interference was generated at center frequencies of 100, 200, 400, 800, 1600, and 2400 MHz with two different methods. Using a Rohde & Schwarz vector signal generator SMBV100A and using an Ettus USRP B200 SDR. Also two different kind of interference were used, a single-tone signal and a sinusoidally frequency-modulated (FM) signal with frequency deviation of 125 kHz and modulation rate of 1 kHz. The frequency deviation and modulation rate were chosen based on the limitations imposed by the SMBV100A at 100 MHz and applied at all of the measured center frequencies with both interference generators. In either case the interference is instantaneously narrowband and periodic. The interference power was limited to -20 dBm, which is close to the specified maximum input level of the USRP B210.

IV. Experimental Results

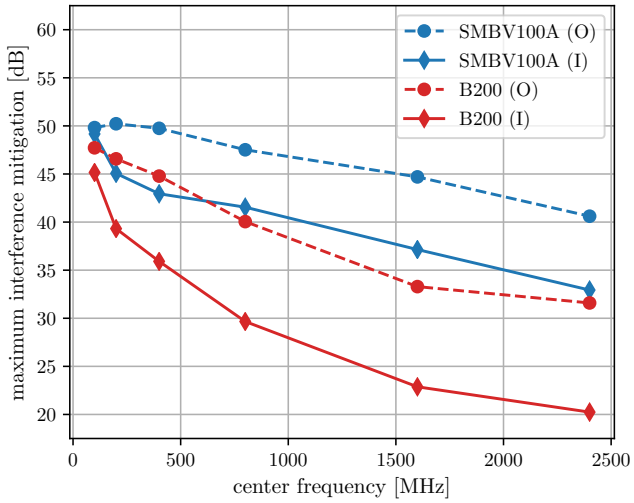
The interference cancellation results, i.e., the measured power reduction after cancellation, over the examined frequency range for both single-tone and FM interference are plotted in Fig. 5. The vector signal generator has considerably lower phase noise of the two tested interference sources, which explains the better efficiency of the interference cancellation. Specifically, the AD9364 transceiver chip used in the USRP B200 has specified integrated phase jitter of 58.9 ps at 2400 MHz, whereas the SMBV100A has phase jitter of only 3.9 ps at 1000 MHz. The single-tone interference cancellation results are thus in agreement with the active cancellation studies with regards to the variance of phase noise in FD radios with non-matched LOs [17].

Furthermore, the interference cancellation results demonstrate an exponential dependence on the center frequency. This is also explained by the differences in phase noise. Ideally, frequency multiplication by N results in phase noise increase by $20 \cdot \log_{10} N$, i.e., 6 dB in the case of frequency doubling. Measurement results for the single-tone interference cancellation are consistent with the 6 dB per octave performance degradation. In the case of FM interference, the maximum achievable suppression rate is further limited by the frequency stability of the FM source and by the ability of the interference mitigation system to exactly estimate and regenerate the periodic interference.

From the results, it also becomes evident that sharing a common external reference between the interference generator and the interference mitigating receiver improves the active cancellation efficiency. This is in accordance with the studies on phase noise effects in FD radios, whereas sharing the LO between the transmit and receive chains inherently mitigates the performance hampering effect of phase noise. These results stress the importance of using high-precision oscillators in co-located radios in order to lower the phase noise and achieve efficient interference cancellation. When considering the mitigation of broadband or pseudorandom interference, the jamming waveforms could perhaps be designed to facilitate digital estimation and suppression of phase noise likewise to recent advances in FD radios [18].



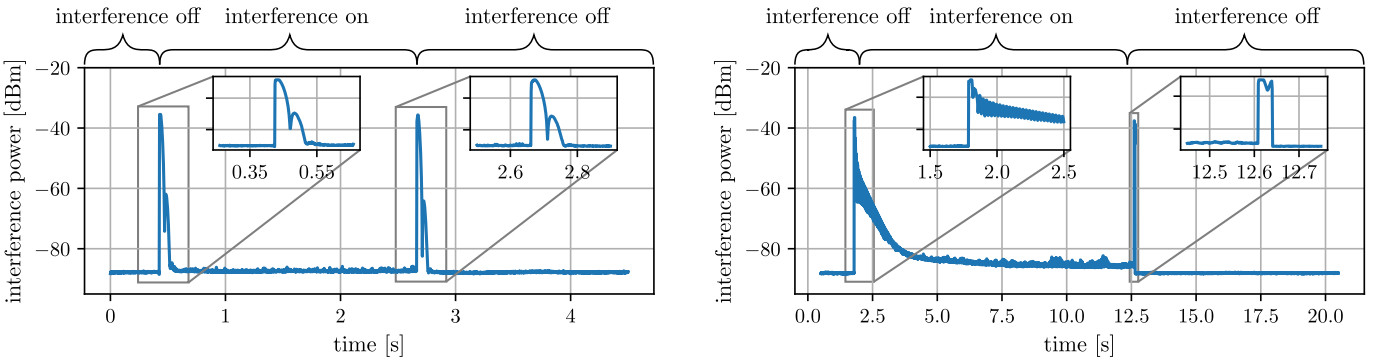
(a) under single-tone interference



(b) under sinusoidally frequency-modulated interference

Fig. 5. Analog interference mitigation achieved in the 100 MHz to 2400 MHz frequency range using the different measurement setup configurations. The interference generator was referenced either by its internal clock (I) or the oven-controlled crystal oscillator based external reference clock (O), which was also used as an external reference for the receiver.

Another important aspect of adaptive filtering is the learning rate by which the interference can be cancelled. The learning rate of the analog RF interference cancellation for single-tone and FM interference is visualized in Fig. 6. For the single-tone interference, the adaptive filter converges in approximately 100 µs, whereas for the FM interference, the filter converges typically in a matter of seconds. Furthermore, such predictive interference cancellation method inherently produces a short burst of interference by itself when the actual interference in the input signal disappears. All of the measurements were made with a small step size that was empirically found to be close to (but still below) the upper bound beyond which the adaptive filter becomes unstable. As mentioned previously, this is affected by the imposed delay of the secondary path.



(a) under single-tone interference

(b) under sinusoidally frequency-modulated interference

Fig. 6. Learning curves of the adaptive digitally assisted analog radio-frequency interference mitigation system as measured for a single-tone and a sinusoidally frequency-modulated interference in a closed and static laboratory environment. Whenever no interference is present the system reaches noise level of -88 dBm.

V. Conclusion

Analog interference mitigation, as opposed to plain digital solutions, becomes necessary in case the interference starts to limit the receiver's sensitivity due to the limited dynamic range of the analog-to-digital converter (ADC) as, e.g., in the case of co-located jammers or radars and signals intelligence receivers. In this paper, we proposed a method for mitigating narrowband interference in the analog domain by using digitally assisted adaptive filtering and provided experimental results on suppressing such interference in a static laboratory environment. The experimental results show promising performance in terms of interference cancellation and the convergence speed of the adaptive interference canceller over a broad frequency range including the very high frequency (VHF) and ultra high frequency (UHF) bands.

However, the results have also illustrated how phase noise, one of the main performance limiting factors, degrades the interference cancellation efficiency. The presented results are limited to a closed experimental setup in a laboratory environment at moderate transmission powers and require further study to assess the feasibility of co-located analog interference mitigation under realistic channel conditions, mobile scenarios, together with signals of interest, and higher output powers. The proposed interference mitigation method could possibly be extended to work with broadband pseudorandom jamming signals, e.g., in the case of a full-duplex (FD) radio shield, if the narrowband interference reconstruction can be replaced with a pseudorandom interference generator.

References

[1] J. Laster and J. Reed, "Interference rejection in digital wireless communications," *IEEE Signal Processing Magazine*, vol. 14, no. 3, pp. 37–62, May 1997.

[2] P. Ödling, O. P. Börjesson, T. Magesacher, and T. Nordström, "An approach to analog mitigation of RFI," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 5, pp. 974–986, Jun. 2002.

[3] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[4] K. Pärlin, T. Riihonen, R. Wichman, and D. Korpi, "Transferring the full-duplex radio technology from wireless networking to defense and security," in *Proc. 52nd Asilomar Conference on Signals, Systems and Computers*, Oct. 2018, pp. 2196–2201.

[5] K. Pärlin, T. Riihonen, and M. Turunen, "Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[6] V. Syrjälä, M. Valkama, L. Anttila, T. Riihonen, and D. Korpi, "Analysis of oscillator phase-noise effects on self-interference cancellation in full-duplex OFDM radio transceivers," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 2977–2990, Jun. 2014.

[7] D. A. Rich, S. Bo, and F. A. Cassara, "Cochannel FM interference suppression using adaptive notch filters," *IEEE Transactions on Communications*, vol. 42, no. 7, pp. 2384–2389, Jul. 1994.

[8] A. Raghavan, E. Gebara, E. M. Tentzeris, and J. Laskar, "Analysis and design of an interference canceller for collocated radios," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 11, pp. 3498–3508, Nov. 2005.

[9] S. Ayazian and R. Gharpurey, "Feedforward interference cancellation in radio receiver front-ends," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 54, no. 10, pp. 902–906, Oct. 2007.

[10] D. Korpi, T. Riihonen, V. Syrjälä, L. Anttila, M. Valkama, and R. Wichman, "Full-duplex transceiver system calculations: Analysis of ADC and linearity challenges," *IEEE Transactions on Wireless Communications*, vol. 13, no. 7, pp. 3821–3836, Jul. 2014.

[11] T. Riihonen and R. Wichman, "Analog and digital self-interference cancellation in full-duplex MIMO-OFDM transceivers with limited resolution in A/D conversion," in *Proc. 46th Asilomar Conference on Signals, Systems and Computers*, Nov. 2012, pp. 45–49.

[12] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Proc. 44th Asilomar Conference on Signals, Systems and Computers*, Nov. 2010, pp. 1558–1562.

[13] S. M. Kuo and D. R. Morgan, "Active noise control: A tutorial review," *Proceedings of the IEEE*, vol. 87, no. 6, pp. 943–973, Jun. 1999.

[14] L. Xu, D. Feng, Y. Liu, X. Pan, and X. Wang, "A three-stage active cancellation method against synthetic aperture radar," *IEEE Sensors Journal*, vol. 15, no. 11, pp. 6173–6178, Nov. 2015.

[15] D. R. Morgan and C. Sanford, "A control theory approach to the stability and transient analysis of the filtered-X LMS adaptive notch filter," *IEEE Transactions on Signal Processing*, vol. 40, no. 9, pp. 2341–2346, 1992.

[16] B. Widrow, J. R. Glover, J. M. McCool, J. Kaunitz, C. S. Williams, R. H. Hearn, J. R. Zeidler, J. E. Dong, and R. C. Goodlin, "Adaptive noise cancelling: Principles and applications," *Proceedings of the IEEE*, vol. 63, no. 12, pp. 1692–1716, Dec. 1975.

[17] A. Sahai, G. Patel, C. Dick, and A. Sabharwal, "On the impact of phase noise on active cancelation in wireless full-duplex," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4494–4510, Nov. 2013.

[18] E. Ahmed and A. M. Eltawil, "On phase noise suppression in full-duplex systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1237–1251, Mar. 2015.

PUBLICATION 2

Analog Mitigation of Frequency-Modulated Interference for Improved GNSS Reception

K. Pärlin and T. Riihonen

In *Proc. Int. Conference on Localization and GNSS*, June 2020
DOI: 10.1109/ICL-GNSS49876.2020.9115518

Analog Mitigation of Frequency-Modulated Interference for Improved GNSS Reception

Karel Pärlin* and Taneli Riihonen†
*Rantelon, Tallinn, Estonia
†Tampere University, Finland
e-mail: karel.parlin@rantelon.ee, taneli.riihonen@tuni.fi

***Abstract*—Powerful in-band interference can saturate a receiver's front-end and limit the usefulness of digital interference suppression methods that are bounded by the receiver's limited dynamic range. This is especially true for the self-interference (SI) encountered in full-duplex (FD) radios, but also in the case of strong interference between co-located radios. However, unlike in FD radios, receivers co-located with interference sources do not typically have direct access to the transmitted interference. This work analyzes the performance of a digitally-assisted analog interference mitigation method and its implementation for the suppression of frequency-modulated (FM) interference before quantization in global navigation satellite system (GNSS) receivers that are co-located with interference sources. Over-the-air measurement results are presented that illustrate the effects of interference mitigation on GPS L1 and Galileo E1 reception in a commercial off-the-shelf GNSS receiver and a software-defined GNSS receiver. The analysis covers the effects of the interference mitigation on the radio frequency (RF) front-end, acquisition, tracking, and positioning stages.**

I. Introduction

Radios with full-duplex (FD) capabilities are expected to increase the spectral efficiency of wireless communications as a result of the advances in self-interference (SI) cancellation techniques, which enable FD radios to simultaneously transmit and receive on the exact same frequency [1]. In addition, FD radios have the potential to reshape both wireless defense and security domains, e.g., in the form of a so-called FD radio shield [2], [3]. Inside the radio shield, a central node would be capable of receiving wireless signals while jamming the reception of those signals for others. Elaborating this concept further, it would be highly desirable for authorized co-located receivers to also be capable of receiving signals-of-interest inside the radio shield as illustrated in Fig. 1. Similarly to the SI cancellation in FD radios, co-located receivers would in some cases benefit from suppressing the interference in the analog domain before quantization to improve the effective resolution of the signal-of-interest [4].

To that end, we have proposed a digitally-assisted analog interference cancellation technique relying on a single input antenna and adaptive filtering [5]. Previously presented experimental results have characterized the performance of the proposed method in a laboratory environment and demonstrated that phase noise of the interference source is one of the main limiting factors for interference mitigation [5].

This research work was supported by the Academy of Finland, the Finnish Scientific Advisory Board for Defence, and the Estonian Defence Forces.

However, our previous experiments have lacked any signals-of-interest besides the interference. In this work, we take them to be global navigation satellite system (GNSS) signals because received GNSS signals are typically quite weak, around $-130\,\mathrm{dBm}$ when acquired outdoors in open-sky conditions [6], and in-band interference can quickly saturate a GNSS receiver's front-end. We present measurements and analyze the impact of frequency-modulated (FM) interference and its cancellation on Global Positioning System (GPS) L1 and Galileo E1 reception using a commercial off-the-shelf GNSS receiver and a software-defined GNSS receiver. The analysis is also fitting due to the widespread use of FM jamming against GNSS receivers [7], [8] and complements works on FM interference mitigation in the digital domain [9].

The work is presented as follows. First, the digitally-assisted analog interference mitigation method from [5] is briefly reintroduced in Section II. The laboratory setup used for assessing the impact of the interference mitigation on processing GNSS signals is presented in Section III, while the discussion and analysis of the experimental results is carried out in Section IV. Finally, Section V concludes the paper.

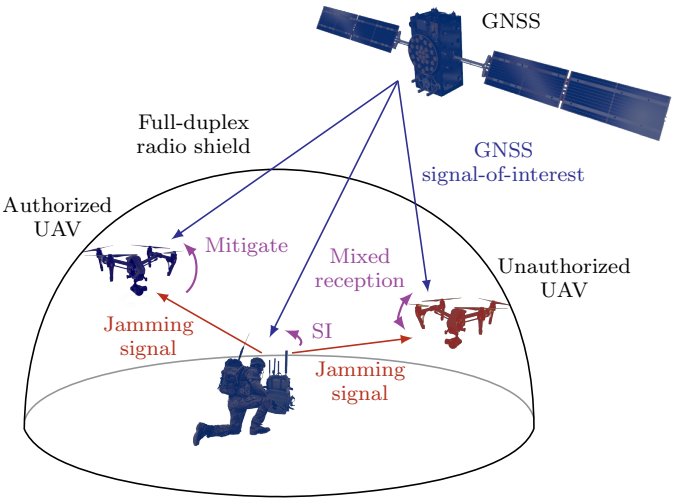


Fig. 1. Full-duplex (FD) radio technology enables radio shields where only the FD-capable jamming node is able to receive signals-of-interest in the jammed frequency. However, adequate interference mitigation enables co-located radios to also receive the signals-of-interest. This could be limited to authorized receivers through pseudorandom jamming.

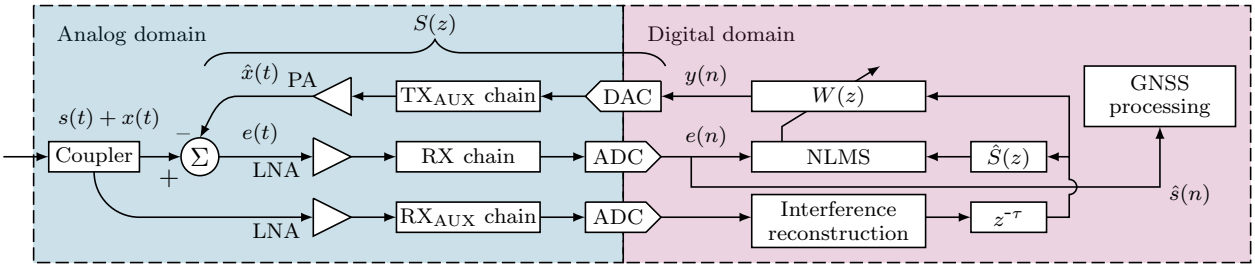


Fig. 2. Digitally-assisted analog mitigation of frequency-modulated interference [5] applied to recover GNSS signals-of-interest.

II. Narrowband Interference Mitigation

The interference mitigation method used and analyzed herein has previously been published in [5]. In essence, the method is based on using an auxiliary transmit chain, similarly to some of the proposed FD radio architectures [10], to suppress the interference in the received signal before quantization as illustrated in Fig. 2. The implementation requires estimating the instantaneous frequency of the narrowband interference signal $x(n)$ and constructing a digital representation $\hat{x}(n)$ of the interference such that it exactly follows the estimated frequencies. Of course, it is only possible to precisely estimate the instantaneous frequency of the interference as long as the interference is sufficiently more powerful than the signal-of-interest. However, this is exactly the situation this work focuses on with powerful co-located interference. Also, when considering GNSS as signals-of-interest, estimation of the interference's instantaneous frequency is aided by the spread spectrum nature of the GNSS signals.

In order to obtain an interference-free version of the signal-of-interest $s(n)$, the input signal $s(n)+x(n)$ is employed as the reference signal for the adaptive filter. The estimated jamming signal $\hat{x}(n)$, which is strongly correlated to the actual jamming signal $x(n)$, is employed as the input for the adaptive filter. The adaptive mechanism adjusts the filter coefficients of $W(z)$ in such a manner that the filter output $y(n)$ approximates the jamming signal, thus forcing the error signal $e(n)$ to resemble the signal-of-interest $s(n)$.

The use of adaptive filtering for analog interference mitigation is complicated by the fact that the summation of signals represents radio-frequency (RF) superposition and it is necessary to compensate for the secondary-path transfer function $S(z)$, which includes a digital-to-analog converter (DAC), a power amplifier (PA), a power combiner, a low-noise amplifier (LNA), and an analog-to-digital converter (ADC). Thus, the adaptive filter needs to imitate the secondary-path transfer function $S(z)$ with a transfer function $\hat{S}(z)$ applied to the input [11]. Fortunately, offline modeling can be used to estimate $S(z)$ during an initial training stage as the signal path from the auxiliary transmitter $\mathrm{TX_{AUX}}$ to the primary receiver RX can be considered static. Still, due to the computational delays involved in estimating the instantaneous frequency, filtering etc., the system's response is non-causal and the system is capable of effectively canceling only narrowband pseudorandom or periodic interference [11].

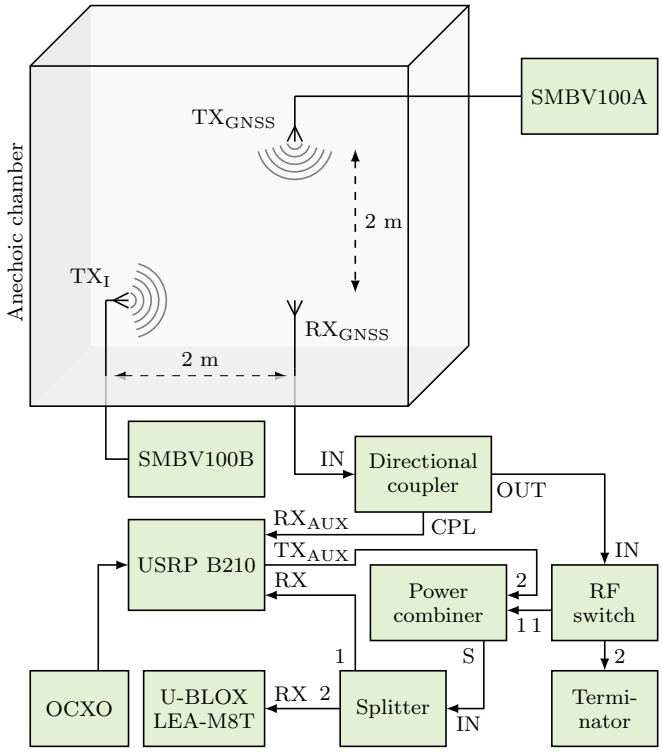


Fig. 3. The setup for measuring the over-the-air performance of the interference mitigation platform using GPS L1 and Galileo E1 as signals-of-interest.

III. Experimental Setup

The measurement setup is outlined in Fig. 3. The interference mitigation prototype is built using an USRP B210 software-defined radio (SDR) and the prototype's performance is analyzed by using simultaneously a commercial GNSS receiver U-Blox LEA-M8T and an open-source GNSS software-defined receiver (GNSS-SDR) [12] that processes IQ samples from the SDR. The measurements are carried out in an anechoic chamber to avoid interfering with GNSS receivers in the vicinity and to be able to use a controlled GNSS source. A signal generator SMBV100A is used for transmitting GPS L1 C/A and Galileo E1 signals that simulate six satellites with predefined location, time, and power. A separate signal generator SMBV100B is used for transmitting a sinusoidally FM interference with deviation of $125\,\mathrm{kHz}$, modulation rate of $1\,\mathrm{kHz}$, and center frequency of $1575.42\,\mathrm{MHz}$.

An active GPS antenna with 27 dBi gain and 1.5 dB noise figure (Trimble 39265-50) is used to receive the GNSS and interference signals, whereas directional log-periodic antennas are used for transmitting the signals. The signal after interference mitigation is split between the U-Blox receiver and the receiver for GNSS-SDR. The U-Blox receiver logs National Marine Electronics Association (NMEA) and U-Blox proprietary messages. The SDR is used for the interference mitigation but also for recording IQ samples with sampling rate of $4.096\,\mathrm{MHz}$. The sampling rate is chosen to be slightly above an integer multiple of the chipping rate as using a multiple of the chipping rate leads to poor accuracy in the estimation of pseudoranges [13].

For each measurement, $4\,\mathrm{min}$ of U-Blox logs and IQ samples are recorded so that both the U-Blox receiver and GNSS-SDR could acquire the position from a cold-start situation. In order to have a fair comparison between the U-Blox receiver and the GNSS-SDR toolbox, the U-Blox receiver is restarted before each measurement. In that way, every U-Blox recording and IQ recording represents a standalone unit for analysis without *a priori* information on satellites' pseudoranges, etc.

IV. Experimental Results

When receiving the combination of a GNSS signal and FM interference, the platform provides about $35\,\mathrm{dB}$ of interference suppression as illustrated in Fig. 4 (where GPS cases are omitted as they are very similar to the Galileo ones). Those results closely resemble the previous findings achieved without any signals-of-interest [5]. But does this lead to improvements in GNSS reception? In the following subsections, we provide in-depth analysis into how the interference mitigation affects actual GPS L1 and Galileo E1 reception in the RF front-end, acquisition, tracking, and positioning stages.

A. RF Front-End

The first stage of a GNSS receiver is the RF front-end, which is typically used to filter the input signal down to the bandwidth of interest, downconvert, amplify using automatic gain control (AGC), and finally quantize using an ADC. In-band interference, however, by-passes such filtering and affects the AGC, consequently determining how well the AGC is capable of minimizing quantization errors of the GNSS signals in the ADC. The gain level set by the AGC in the U-Blox receiver with respect to the jammer-to-signal ratio (JSR) is plotted in Fig. 5. It is evident that as the power of the interference increases, the AGC decreases the gain level to prevent from overflowing the ADC, which is exactly the purpose of the AGC. Because AGC is typically the first in line to be affected by adversarial interference, AGC is potentially well suited for interference detection [14].

The U-Blox receiver also features an internal interference detector that provides an interference detection confidence level, although it is unclear, whether the interference indicator takes the AGC information into account in this case. The interference confidence level is plotted alongside the AGC data

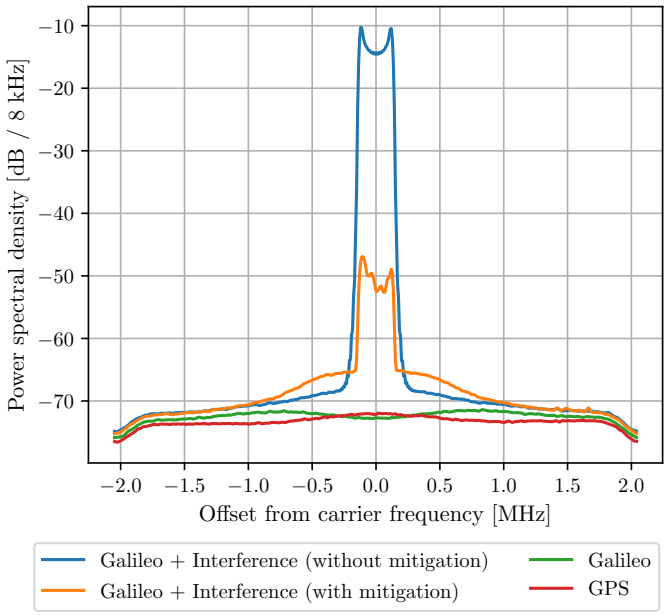


Fig. 4. Power spectral density of the received GNSS and interference signals.

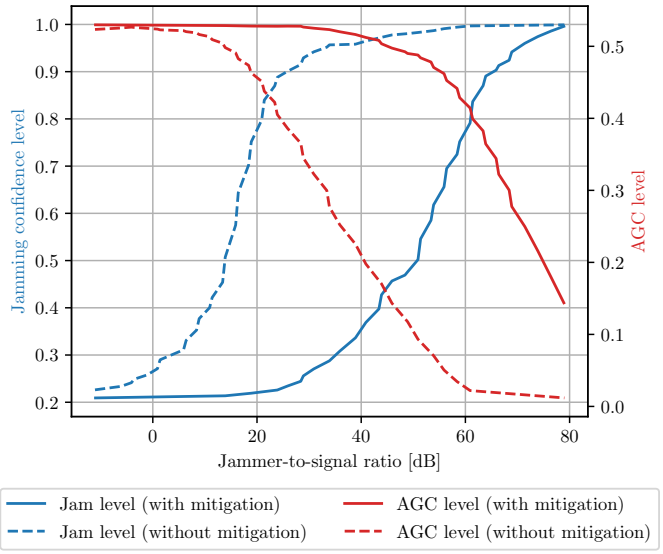


Fig. 5. U-Blox LEA-M8T hardware monitoring results.

in Fig. 5. As the interference power increases so does the interference detection confidence level. The reported AGC level and interference confidence level are not exactly reciprocal, yet both of these metrics seems to be similarly affected by the interference mitigation. Comparing the AGC and interference confidence levels with and without interference mitigation indicates that interference mitigation extends the normal working range of the U-Blox receiver RF front-end by $30\,\mathrm{dB}$ to $40\,\mathrm{dB}$. As such, analog interference mitigation might also turn useful for improving the reception quality of systems, for which baseband digital signal processing is not accessible.

B. Acquisition

Acquisition stage is the first digital stage in GNSS reception and it is tasked with detecting the presence of GNSS signals and providing coarse estimates of the signals' code phase and Doppler frequency for the tracking stage [15]. Acquisition is essentially achieved by correlating the received signal with locally generated replicas, which are characterized by specific code delays and Doppler frequencies.

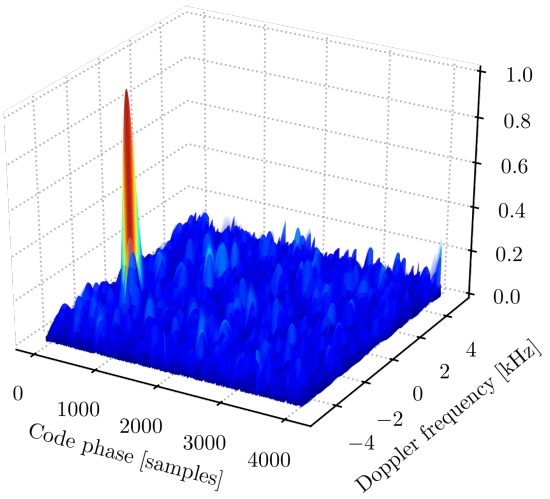
Figure 6 illustrates how the acquisition search space for GPS L1 is affected by interference at JSR of $50\,\mathrm{dB}$ with and without interference mitigation. The acquisition search space is calculated using $1\,\mathrm{ms}$ of integration time and $2\,\mathrm{Hz}$ Doppler frequency step in the GNSS-SDR toolbox. Galileo E1 acquisition search space exhibits similar behaviour and has not been included for brevity.

Without interference (cf. Fig. 6a), a single predominant peak appears in the cross-ambiguity function (CAF) that indicates the presence of the signal and its code delay and Doppler shift. With interference, the separation between the cross-correlation peak and the noise floor decreases drastically (cf. Fig. 6b), leading to increased probability of false alarms or even providing inaccurate code phase and Doppler frequency estimates [16]. Interference mitigation improves the CAF significantly (cf. Fig. 6c) and a single dominant peak is distinguishable from the noise floor again.

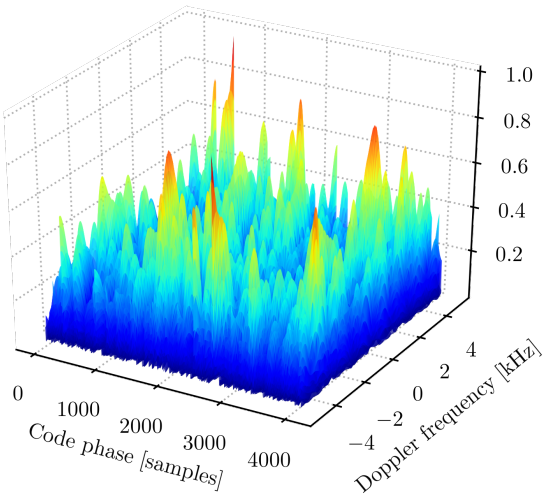
C. Tracking

Tracking stage uses the coarse estimates from the acquisition stage to provide fine estimates of the GNSS signal parameters, which in turn are used for generating pseudoranges [16]. The tracking stage typically relies on a closed-loop architecture where tracking loops are used to track the different signal components. Loop discriminators use correlator outputs to provide a measure of error between the actual and estimated signal parameters. In good signal-to-noise ratio (SNR) conditions, the discriminator outputs (Δ_{phase} and Δ_{code}) are guided close to zero by the tracking loops. However, as the SNR deteriorates, the standard deviation of the discriminator outputs increase (σ_{phase} and σ_{code}), lending themselves for analyzing the interference impact, as illustrated in Fig. 7. Based on the measurement results, the tracking stage is more likely to provide erroneous values with the interference mitigated as opposed to without mitigation. Although the operational range is extended similarly to the previous stages.

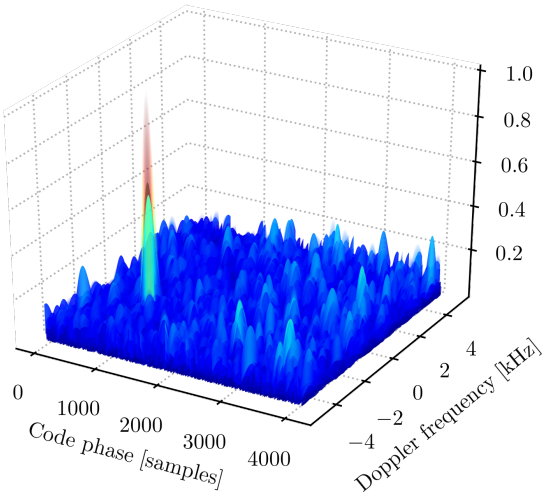
Besides the discriminator outputs, another aspect to analyze at this stage is the estimated carrier-to-noise ratio C/N_0. The estimation of the C/N_0 depends on both the signal power estimation and the noise power estimation and several methods exist for these estimations [17]. The estimates are of course affected by interference and therefore they can also be an indication of adversarial interference [18]. The measured effect of FM interference on the estimation of C/N_0 with and without mitigation is plotted in Fig. 8. The C/N_0 measurement results are in line with the results presented in RF front-end and acquisition stages, i.e., the interference mitigation extends the normal C/N_0 estimation range by $30\,\mathrm{dB}$ to $40\,\mathrm{dB}$.



(a) GPS acquisition without interference



(b) GPS acquisition with interference



(c) GPS acquisition with interference mitigation

Fig. 6. Comparison of the cross ambiguity function for GPS L1 acquisition search space without interference, with frequency-modulated interference (jammer-to-signal ratio of $50\,\mathrm{dB}$) and with the interference suppressed.

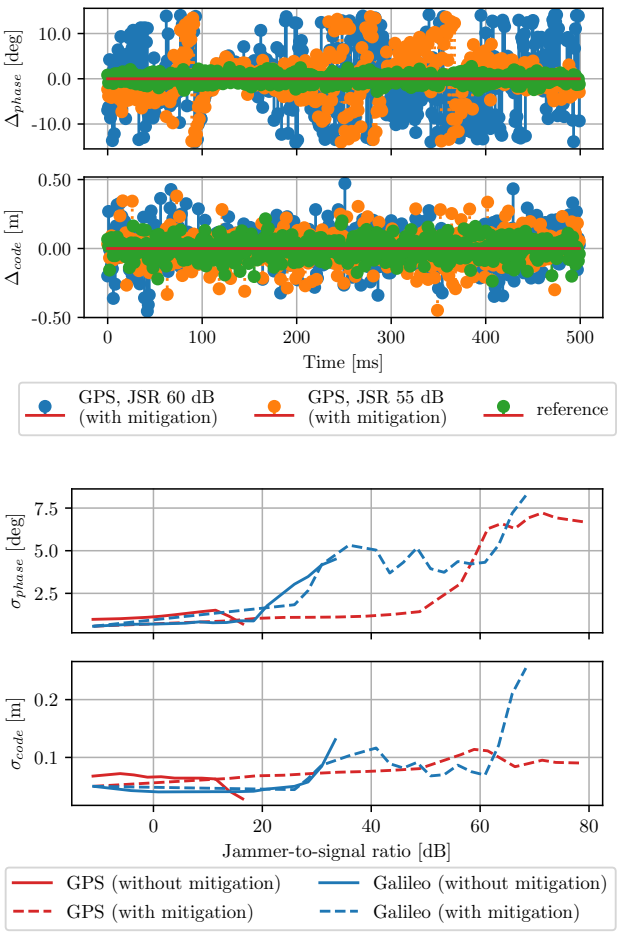


Fig. 7. Carrier and code discriminator outputs and standard deviations thereof. Phase-locked loop bandwidth is 15 Hz, delay-locked loop bandwidth is 2 Hz, and spacing between the early and late replicas is set to 0.5 code chips.

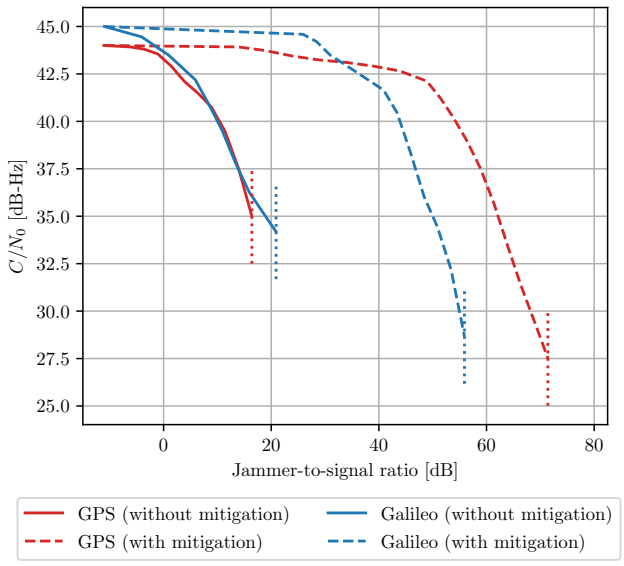


Fig. 8. Estimated C/N_0 values from the U-Blox receiver with and without interference mitigation. The dotted vertical lines indicate the jammer-to-signal ratio (JSR) from which on the receiver is unable to estimate C/N_0.

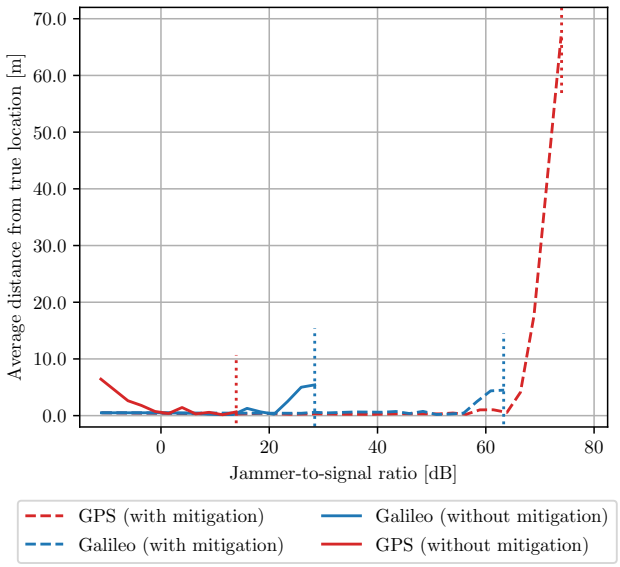


Fig. 9. GPS and Galileo positioning accuracy with regards to the jammer-to-signal ratio (JSR). Average of the U-Blox and GNSS-SDR distances is plotted for brevity as U-Blox and GNSS-SDR provide comparable accuracy. The dotted vertical lines indicate the JSR from which on the receivers are unable to acquire any position.

D. Positioning

If the GNSS signals can be acquired and tracked despite the interference, then the GNSS receiver can estimate its position. However, the position estimate may be degraded by the inaccuracies in pseudorange estimates caused by the interference. Figure 9 shows the average positioning accuracy of the U-Blox and GNSS-SDR receivers for both GPS L1 and Galileo E1 under interference with and without mitigation. It is evident that interference suppression allows the receivers to operate under much higher jammer-to-signal ratio (JSR), even though the effect is slightly different for GPS L1 and Galileo E1 positioning accuracy, presumably because of the different modulations used in GPS L1 and Galileo E1. During the 4 min measurements, poor SNR conditions tend to prevent the receivers from acquiring any positional fix rather than lead to very large positioning errors. In poor SNR conditions, the position is available for a fraction of the total measurement time whereas in good JSR conditions the position is available most of the time after acquiring the satellite parameters.

In a relatively small JSR range, the interference is severe enough to drastically decrease the GNSS receiver performance but not severe enough to force the receiver to prevent the acquisition of satellite signals or lose its lock on the satellite signals. For four such interference cases, the horizontal GPS positioning accuracy is illustrated in Fig. 10. The horizontal error ranges from couple meters to hundreds of meters. Such intermediate JSR ranges can perhaps be the most dangerous because of the difficulty to detect the interference [19]. In case the users fail to detect that the GNSS service is being interfered with, the positional inaccuracies may have a significant impact on the users' safety and security [20].

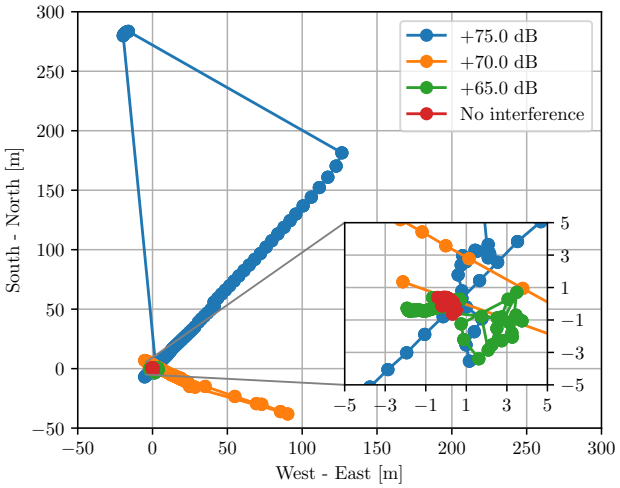


Fig. 10. GPS horizontal positioning accuracy with respect to the true coordinates without any interference and at three different jammer-to-signal ratios with interference mitigation. Each measurement spans 4 min.

V. Conclusions

Analog interference mitigation, as opposed to plain digital solutions, becomes necessary when the interference starts to limit the receiver's sensitivity due to the receiver's limited dynamic range. This is an outstanding issue in full-duplex (FD) radios but can also cause problems in co-located radios, especially when considering the typically weak global navigation satellite system (GNSS) transmissions as signals-of-interest. In this work, we analyzed how a digitally-assisted analog interference mitigation scheme affects GPS L1 and Galileo E1 reception in the presence of frequency-modulated interference, whereas the interference parameters are unknown to the receiver. We characterized the impact of interference and its mitigation on the radio-frequency (RF) front-end, acquisition, tracking, and positioning stages of GNSS receivers using a commercial off-the-shelf receiver and a separate open-source sofware-defined receiver.

The experimental results demonstrate considerable improvements in terms of preventing saturation in the RF front-end, cleaning up the acquisition search space, improving tracking accuracy and carrier-to-noise ratio estimates, and enhancing positioning accuracy for both GPS L1 and Galileo E1. The measurement results indicate that the operational jammer-to-signal ratio range of the GNSS receivers is extended proportionally to the amount of interference power suppression, for which one of the main limiting factors is the phase noise of the interference source. While the mitigation of periodic interference might have limited usage, extending such interference mitigation to suppress pseudorandom jamming could be desirable for differentiating between authorized and non-authorized receivers, for example, inside a FD radio shield.

References

[1] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] T. Riihonen, D. Korpi, O. Rantula, H. Rantanen, T. Saarelainen, and M. Valkama, "Inband full-duplex radio transceivers: A paradigm shift in tactical communications and electronic warfare?" *IEEE Communications Magazine*, vol. 55, no. 10, pp. 30–36, Oct. 2017.

[3] K. Pärlin, T. Riihonen, R. Wichman, and D. Korpi, "Transferring the full-duplex radio technology from wireless networking to defense and security," in *Proc. 52nd Asilomar Conference on Signals, Systems and Computers*, Oct. 2018, pp. 2196–2201.

[4] P. Ödling, O. P. Börjesson, T. Magesacher, and T. Nordström, "An approach to analog mitigation of RFI," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 5, pp. 974–986, Jun. 2002.

[5] K. Pärlin and T. Riihonen, "Digitally assisted analog mitigation of narrowband periodic interference," in *Proc. International Symposium on Wireless Communication Systems*, Aug. 2019, pp. 682–686.

[6] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, Jan. 2003.

[7] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "Signal characteristics of civil GPS jammers," in *Proc. Radionavigation Laboratory Conference*, Sep. 2011, pp. 1907–1919.

[8] R. H. Mitch, M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "Signal acquisition and tracking of chirp-style GPS jammers," in *Proc. 26th International Technical Meeting of the Satellite Division of The Institute of Navigation*, Sep. 2013, pp. 2893–2909.

[9] K. D. Rao and M. Swamy, "New approach for suppression of FM jamming in GPS receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 42, no. 4, pp. 1464–1474, Oct. 2006.

[10] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[11] S. M. Kuo and D. R. Morgan, "Active noise control: A tutorial review," *Proceedings of the IEEE*, vol. 87, no. 6, pp. 943–973, Jun. 1999.

[12] C. Fernández–Prades, J. Arribas, P. Closas, C. Avilés, and L. Esteve, "GNSS-SDR: An open source tool for researchers and developers," in *Proc. 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Sep. 2001, pp. 780–794.

[13] D. M. Akos and M. Pini, "Effect of sampling frequency on GNSS receiver performance," *Journal of The Institute of Navigation*, vol. 53, no. 2, pp. 85–95, Aug. 2006.

[14] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, "Automatic gain control (AGC) as an interference assessment tool," in *Proc. 16th International Technical Meeting of the Satellite Division of The Institute of Navigation*, Sep. 2003, pp. 2042–2053.

[15] D. Akopian, "Fast FFT based GPS satellite acquisition methods," *IEE Proceedings—Radar, Sonar and Navigation*, vol. 152, no. 4, pp. 277–286, 2005.

[16] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[17] M. S. Sharawi, D. M. Akos, and D. N. Aloi, "GPS C/N_0 estimation in the presence of interference and limited quantization levels," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, no. 1, pp. 227–238, Jan. 2007.

[18] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, and D. M. Akos, "Jamming detection in GNSS receivers: Performance evaluation of field trials," *Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 73–82, Mar. 2015.

[19] F. Dovis, *GNSS Interference Threats and Countermeasures*. Artech House, 2015.

[20] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187, Apr. 2009.

PUBLICATION 3

Jamming and Classification of Drones Using Full-Duplex Radios and Deep Learning

K. Pärlin, T. Riihonen, G. Karm and M. Turunen

In *Proc. Int. Symposium on Personal, Indoor and Mobile Radio Communications*, Sept. 2020
DOI: 10.1109/PIMRC48278.2020.9217351

Jamming and Classification of Drones Using Full-Duplex Radios and Deep Learning

Karel Pärlin*, Taneli Riihonen†, Gaspar Karm*, and Matias Turunen†
*Rantelon, Tallinn, Estonia
†Tampere University, Finland
e-mail: karel.parlin@rantelon.ee, taneli.riihonen@tuni.fi,
gaspar.karm@rantelon.ee, matias.turunen@tuni.fi

***Abstract*—The emerging full-duplex (FD) radio concept is set to double the spectral efficiency of commercial wireless networks, but it also has potential applications in the defense and security domains. In the form of multifunction military full-duplex radios (MFDRs), the FD capability could enable armed forces to conduct simultaneous electronic attacks, electronic support measures, and tactical communications. This paper demonstrates the feasibility of simultaneous jamming and reconnaissance of drones' remote control (RC) systems using a prototype MFDR. Alongside, we apply deep learning in the form of a convolutional neural network (CNN) for classifying the RC signals and analyze the effect of FD operation on the classification performance.**

I. Introduction

Recent advances in full-duplex (FD) radio research have enabled concurrently receiving and transmitting on the exact same frequencies. Such operation, as compared to the conventional half-duplex (HD) mode, improves the spectral efficiency of wireless communications and consequently enhances the network throughput in commercial systems [1]. In addition, FD radios can also reform the cyber battlefield by facilitating simultaneous combinations of electronic attacks, electronic support, and tactical communication [2], [3]. Several practical works have already demonstrated the feasibility of such concepts in laboratories [4]–[6]. We consider herein the application of the FD radio technology for countering the emerging threats caused by remotely operated aerial vehicles [7]–[9].

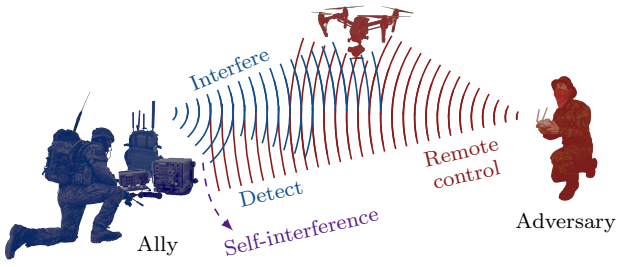


Fig. 1. Military full-duplex radios could be used to simultaneously detect and jam adversary drones' remote control systems, therefore benefiting from improved situational awareness and enhanced jamming techniques.

This research work was supported in part by the Academy of Finland under the grant 315858, in part by the Finnish Scientific Advisory Board for Defence (MATINE), and in part by the Estonian Ministry of Defence.

The objectives of this work are to study the practical feasibility of simultaneously receiving and jamming the remote control (RC) signals of unmanned aerial vehicles/systems (UAV/Ss)—referred to as 'drones' herein—using FD radio technology and then to classify the intercepted signals using machine learning. The challenge is illustrated in Fig. 1. The RC signals received and classified during simultaneous jamming could be used to, e.g., locate the adversary or tailor the jamming waveform against the specific UAS. We propose the application of deep learning in the form of convolutional neural networks (CNNs) for the accurate classification of different RC protocols. Through measured and simulated results, we demonstrate the CNN model's feasibility to identify commercial drone RC signals in HD and FD modes.

II. Signal Detection and Classification

Deep learning has recently enjoyed significant success in various research areas that focus on feature extraction from raw input data [10], [11] and these advances have not gone unnoticed in the wireless communications research. Methods based on CNNs have been proposed for modulation recognition [12], wireless signals' classification [13], transmitter fingerprinting [14], radar classification [15] and, also, drone classification from radar micro-Doppler signatures [16], to name but a few. However, to the best of our knowledge, studies into drone RC signal classification have not been reported.

A. Architecture

Several radio-frequency (RF) signal representation and preprocessing methods have been proposed for deep learning-based signal classification purposes. These include simply using the complex-sampled time series of the signal without any preprocessing [17], the amplitude and phase difference representation [18], and the spectrogram-based method [18]. When considering the time-series representation, the wide bandwidth of the 2.4 GHz unlicensed radio band, in which many commercial drones operate, renders high computational complexity and can also degrade the overall classification accuracy [19]. In addition, time-series signal representation in deep learning methods for signal classification has been shown to have negative impacts on the overall classification accuracy for signals with frequency offsets, which could complicate the classification of the frequency-hopping signals at hand [19].

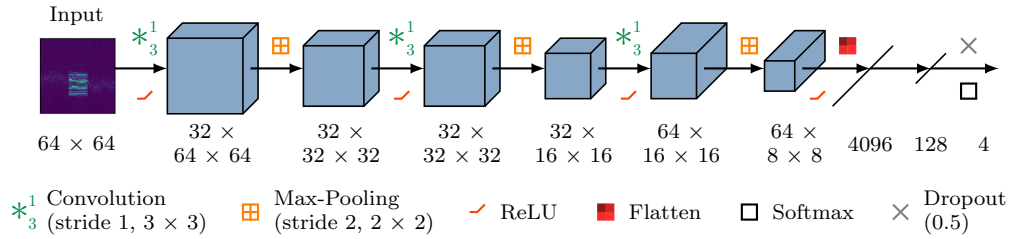


Fig. 2. The architecture of the convolutional neural network (CNN) used in this work for the spectrogram-based detection and classification of unmanned aerial vehicle (UAV) or 'drone' remote control (RC) signals after suppressing the self-interference (SI) caused by simultaneous same-band jamming.

The characteristics of typical drone RC systems, i.e., frequency hopping over a wide bandwidth, different channel frequencies, bandwidths and transmission times across different protocols, suit the spectrogram-based representation, as it is not sensitive to frequency offsets and phase shifts. In this work, we therefore rely on the spectrogram-based representation. In particular, the time-frequency evolution of the 80 MHz input signal is split into smaller spectrograms of size 64 × 64 pixels that are input to the CNN. Thus, the time and frequency coverage of the spectrograms is chosen to be 6.5 ms and 5 MHz, respectively, in order for each of the different drone remote control signals analyzed in this paper to fit inside the spectrograms. The input is also normalized, as this enhances spectrogram-based classification accuracy [20].

The architecture of the proposed CNN model is outlined in Fig. 2. Similarly to efficient object recognition models [11], the spectrogram is passed through a stack of convolutional layers that have filters with very small receptive fields. To classify which of the categories (background interference and noise or one of the RC signals) the 64 × 64 spectrogram contains, it is passed through three consecutive convolutional layers, followed by two fully connected layers. In each of the convolutional layers, the convolution stride is 1 pixel and the receptive field is 3 × 3 pixels. The spatial padding of convolutional-layer inputs is such that the spatial resolution is preserved after the convolution. All convolutional layers are equipped with the rectified linear unit (ReLU) activation function that has been shown to speed up training in comparison to other activation functions [10]. Each convolutional layer is followed by a max-pooling layer for spatial pooling.

The two fully connected layers are followed by a softmax classifier that computes the probability of each class label over all classes. In order to prevent overfitting, dropout is used with a coefficient of 0.5 that has been shown to be close to optimal for a wide range of applications [21]. The model is implemented using open source TensorFlow machine learning framework [22] and Keras deep learning library [23].

B. Training

The CNN model was trained to classify between four categories: *'Noise'*, *'Taranis'*, *'Lightbridge'*, or *'Phantom 2'*. The data for training the model was recorded by connecting the RCs to a digital receiver one-by-one. The samples were recorded with different attenuation levels between the RC transmitter and the receiver in order to diversify the training dataset. During data collection, FD jamming and self-interference (SI) cancellation were not used. The noise class, unlike the three RC classes, was trained with an antenna at the 2.4 GHz band in order to capture authentic background transmissions. The noise samples were recorded in an urban environment iteratively through reinforced learning to minimize the false positive classification of the RCs.

Figure 3 gives examples of the time–frequency representations belonging to the classes that were used for training the CNN. The training dataset consists of 63,600 spectrograms, wherein 57,000 spectrograms represent the noise class and each remote controller is characterized by 2,200 spectrograms. The model was trained with a batch size of 128 using the Adam optimization algorithm, which updates the weights of the network adaptively to minimize classification errors [24].

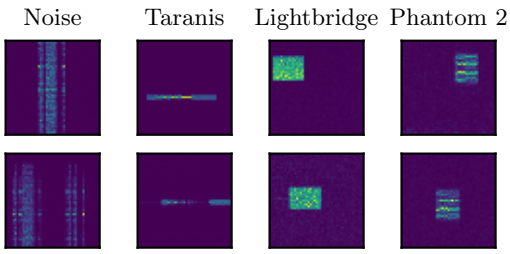


Fig. 3. Each spectrogram is 64 by 64 pixels, has a time duration of 6.5 ms, and covers a frequency bandwidth of 5 MHz. The 'Noise' class includes also co-channel interference, e.g., from WiFi/Bluetooth, and partial RC waveforms.

III. Experimental Setup

In order to verify the feasibility of simultaneous FD jamming and classification, we carried out experiments in a laboratory environment. The measurement setup simulates a scenario where an unauthorized drone is being remotely controlled and a prototype military full-duplex radio (MFDR) is used to simultaneously jam and intercept the RC link as shown in Fig. 4. All of the devices involved in the measurements are connected through coaxial cables instead of using antennas. This provides a controlled environment in which all sources of interference, besides the devices under test, are eliminated. Also, this ensures precise control and measurement of the power levels during the experiments and that the jammer does not cause any unlawful collateral interference to its vicinity.

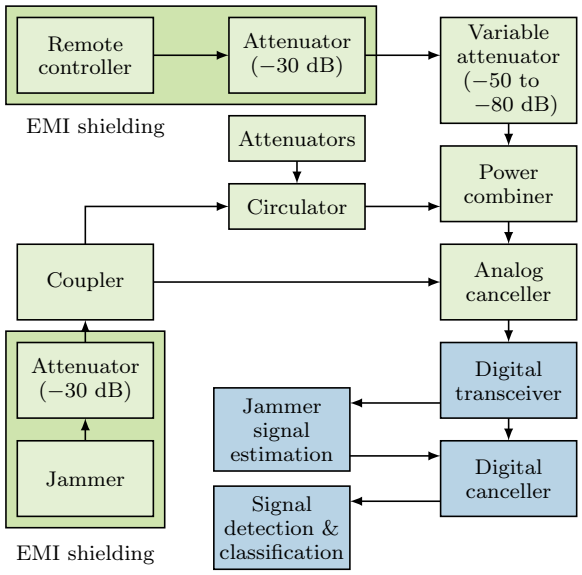


Fig. 4. The measurement setup, where both transmitters were enclosed in electromagnetic interference (EMI) shielding boxes to prevent wireless leakage from reaching the analog canceller and the digital transceiver.

A. Experimental Full-Duplex Transceiver

The MFDR prototype is built on top of a high-quality vector signal transceiver (PXIe-1073) that receives and records signals in a 80 MHz bandwidth (120 MHz sampling rate) with duration of 50 ms. A separate jammer with output power of 43 dBm is used to generate and transmit a 80 MHz wide linear chirp jamming signal that acts as SI for signal surveillance at the receiver. In order to suppress the jamming signal, SI cancellation is implemented in three stages. At the first stage, a circulator is used together with 30 dB of attenuation immediately after the jammer to imitate transmit–receive antenna isolation of approximately 60 dB. Typically drone jammers, and in fact the jammer used in these measurements, use highly directional antennas. Therefore, taking into account the recent research in transmit–receive antenna isolation [25], it is plausible that such separation could be achieved. Passive isolation is followed by an active analog SI canceller [26] and, finally, the residual SI is suppressed digitally [27].

B. Remote Control Systems

Three different drone RC systems were used separately to provide the signals-of-interest in the measurements. The RCs were *FrSky Taranis X9D Plus*, *DJI Phantom 2*, and *DJI Phantom 3 Advanced*. Each of these RC systems makes full use of the 2.4 GHz industrial, scientific, and medical (ISM) band through frequency hopping. The remote controllers' output powers adhere to the 20 dBm limit of the ISM band. In order to emulate different remote controller signal strengths (or link distances), a variable attenuator was used between the remote controller and the receiving front-end. The remote controller signal was attenuated in the range of −80 dB to −110 dB with 5 dB steps.

The RC systems exhibited the following characteristics during our experiments. *FrSky Taranis X9D Plus* hops among 47 frequency channels with 1.5 MHz spacing between the center frequencies of adjacent channels and has a dwell time of 9 ms, which is the time interval between each transmitted packet. The packet transmission time itself is actually lesser, 4.75 ms. *DJI Phantom 2* hops among 36 frequency channels with dwell time of 7 ms, packet transmission duration of 1.6 ms, and has a spacing of 2 MHz between adjacent channels' center frequencies. *DJI Phantom 3 Advanced* uses *DJI Lightbridge* protocol with 34 different channels, spacing of approximately 2 MHz, dwell time of 14 ms, and transmission duration of 2.15 ms. In principle, the differences in these parameters and modulation bandwidths is what enables the CNN model to classify between the protocols based on the spectrograms.

IV. Experimental Results

In this paper, we focus mainly on the classification results, acknowledging that both analog and digital SI cancellation stages contribute 40 dB to 45 dB of SI suppression [27]. The classification of *'Phantom 2'* RC signals is illustrated in Fig. 5. Without any SI, the packets are easily detected by the model, unlike when relying only on passive isolation as then the model is completely blinded. After analog cancellation, the model is already able to detect signals of interest in certain frequency ranges because of the canceller's frequency selectivity. After digital cancellation, the RC signals are accurately detected regardless of the used channel and the results resemble the situation without SI.

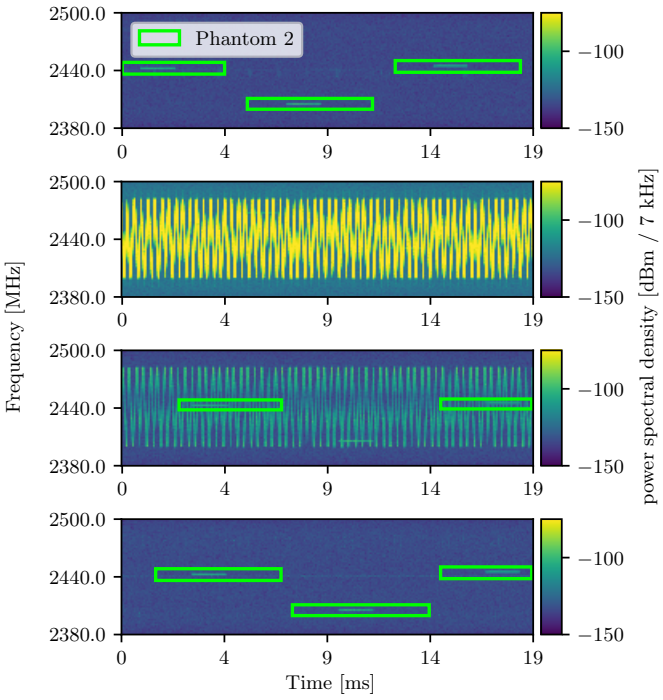
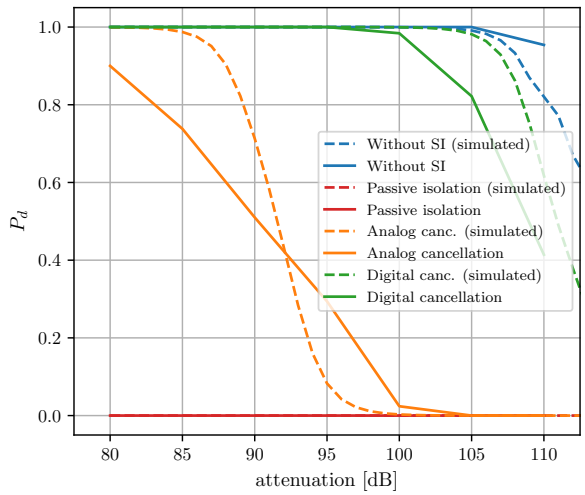
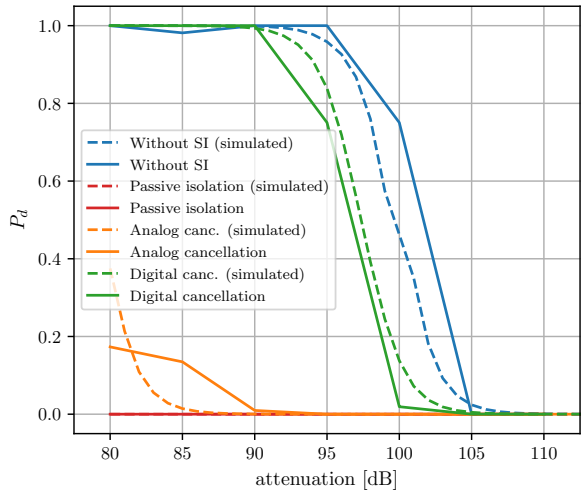


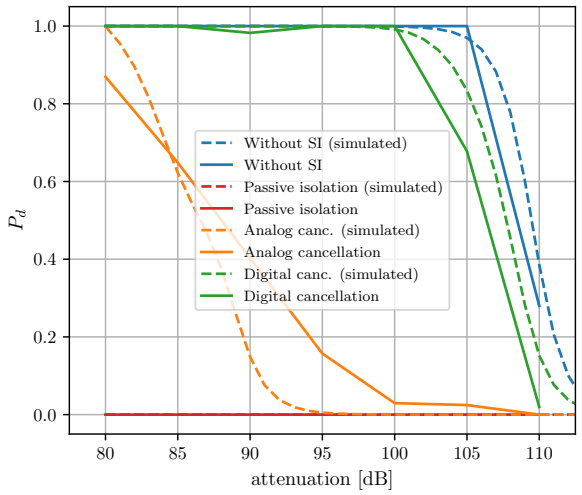
Fig. 5. Top–down: Example signal classification (a) without SI, (b) with SI and only passive isolation, (c) after analog SI cancellation, and (d) after digital SI cancellation. The bounding boxes indicate classification.



(a) Taranis



(b) Lightbridge



(c) Phantom 2

Fig. 6. Remote controller signal detection probability without SI, with SI and only passive isolation, after analog cancellation, and after digital cancellation.

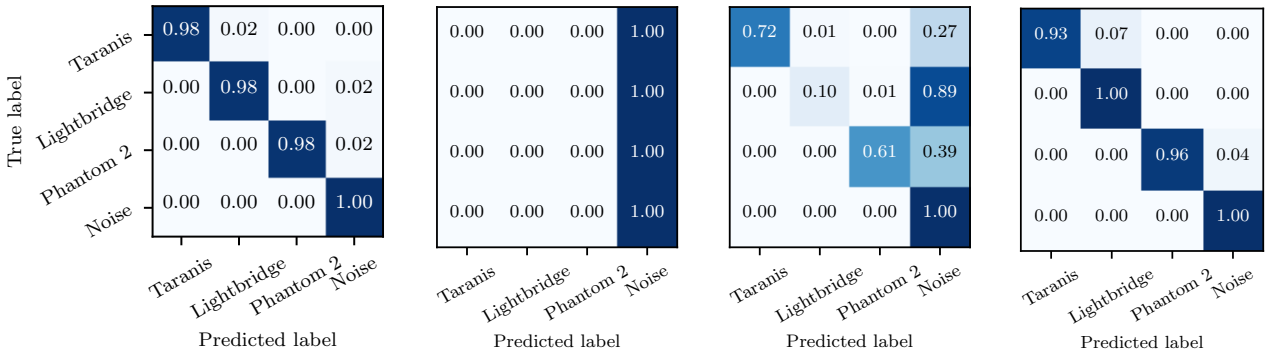
Figure 6 illustrates the measured and reference simulated signal detection probabilities P_d after each of the SI cancellation stages. The model is incapable of detecting any of the RC signals without active SI cancellation. Depending on the remote controller, the CNN is more or less successful in classifying the RC signals after analog cancellation at good signal-to-noise ratios (SNRs). However, digital interference cancellation substantially improves the detection probability and allows to detect the RC signals already at poor SNRs. Nevertheless, when compared to the results without SI from FD jamming, the probability of detection is slightly (2–5 dB) hampered by FD operation.

In general, the simulated and measured results are fairly similar, except for the analog cancellation stage. The simulations were carried out using a frequency-swept signal so that its power was constant and matched to the average measured power of the SI at the respective stage. However, because the analog canceller exhibits considerable frequency selectivity, the residual SI after the analog cancellation stage does not have constant power over the whole frequency band. Thus, in frequency ranges with more effective SI cancellation, the empirical probability of detection is better than in simulations and vice versa. This results in the more gentle slope of detection probability over the measured attenuation range.

The classification accuracy of the CNN model is tabulated in Fig. 7. The confusion matrices are calculated using the combined measurements that were carried out with attenuation values of 80 dB to 90 dB in order to emphasize the effect of residual SI rather than poor SNR. Similarly to the results presented in Figs. 5 and 6, the cases without SI limit the accuracy that can be achieved by using the FD operation mode. However, the results in Fig. 7 also illustrate the robustness of the CNN-based classification model. Regardless of the SI level, the false alarm or incorrect classification rate remains low. This is partly because the measurements were done in a laboratory environment without the presence of other signals, in addition to the residual SI, that could trigger false alarms.

V. Conclusion

In this work, we have demonstrated the feasibility of combining simultaneous jamming and reconnaissance of drone remote control (RC) signals using full-duplex (FD) radio technology and deep learning. We have proposed a convolutional neural network (CNN) based signal classification method that utilizes time–frequency domain data to classify drone RC signals that typically hop in frequency over a wide bandwidth. We have analyzed the impact of residual self-interference (SI) at different stages of the FD radio on the performance of the CNN model through measurements and simulations. Both measured and simulated results indicate that residual SI degrades the classification accuracy and probability of detection to some extent. Nevertheless, given that the classification in the FD operation mode comes at almost no cost to the jamming efficiency, the FD mode can be highly advantageous compared to conventional half-duplex (HD) operation, where jamming needs to be ceased during reconnaissance.



(a) Without self-interference (b) Only passive isolation (c) After analog cancellation (d) After digital cancellation

Fig. 7. The measured classification accuracy of the convolutional neural network model under good signal-to-noise ratio conditions (combined measurements made with attenuation values 80 dB to 90 dB). The model is capable of discerning with high accuracy between frequency-swept interference (or residual thereof) and the different drone remote control signals. The combination of analog and digital self-interference cancellation enables the model to achieve classification accuracy similar to that without any interference.

REFERENCES

[1] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] T. Riihonen, D. Korpi, O. Rantula, H. Rantanen, T. Saarelainen, and M. Valkama, "Inband full-duplex radio transceivers: A paradigm shift in tactical communications and electronic warfare?" *IEEE Communications Magazine*, vol. 55, no. 10, pp. 30–36, Oct. 2017.

[3] K. Pärlin and T. Riihonen, "Full-duplex transceivers for defense and security applications," in *Full-Duplex Communications for Future Wireless Networks*. Springer, Apr. 2020, pp. 249–274.

[4] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, and R. Wichman, "Tactical communication link under joint jamming and interception by same-frequency simultaneous transmit and receive radio," in *Proc. IEEE Military Communications Conference*, Oct. 2018.

[5] T. Riihonen, D. Korpi, M. Turunen, and M. Valkama, "Full-duplex radio technology for simultaneously detecting and preventing improvised explosive device activation," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[6] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, and R. Wichman, "Military full-duplex radio shield for protection against adversary receivers," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[7] S. Basak and B. Scheers, "Passive radio system for real-time drone detection and DoA estimation," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[8] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[9] D. Rauschen, D. Gläsel, H. P. Such, P. Zimmermann, and M. Antweiler, "Commercial of the shelf counter UAV," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

[10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, 2012, pp. 1097–1105.

[11] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[12] T. J. O'Shea, T. Roy, and T. C. Clancy, "Over-the-air deep learning based radio signal classification," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 168–179, Feb. 2018.

[13] M. Kulin, T. Kazaz, I. Moerman, and E. De Poorter, "End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications," *IEEE Access*, vol. 6, pp. 18 484–18 501, Mar. 2018.

[14] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, Feb. 2018.

[15] C. Wang, J. Wang, and X. Zhang, "Automatic radar waveform recognition based on time-frequency analysis and convolutional neural network," in *Proc. International Conference on Acoustics, Speech and Signal Processing*, Mar. 2017, pp. 2437–2441.

[16] B. K. Kim, H.-S. Kang, and S.-O. Park, "Drone classification using convolutional neural networks with merged Doppler images," *IEEE Geoscience and Remote Sensing Letters*, vol. 14, no. 1, pp. 38–42, Jan. 2016.

[17] T. J. O'Shea, J. Corgan, and T. C. Clancy, "Convolutional radio modulation recognition networks," in *Proc. International Conference on Engineering Applications of Neural Networks*, Sep. 2016, pp. 213–226.

[18] A. Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, and L. A. DaSilva, "Spectrum monitoring for radar bands using deep convolutional neural networks," in *Proc. IEEE Global Communications Conference*, Dec. 2017.

[19] S. C. Hauser, W. C. Headley, and A. J. Michaels, "Signal detection effects on deep neural networks utilizing raw IQ for modulation classification," in *Proc. IEEE Military Communications Conference*, Oct. 2017, pp. 121–127.

[20] N. Bitar, S. Muhammad, and H. H. Refai, "Wireless technology identification using deep convolutional neural networks," in *Proc. 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, Oct. 2017.

[21] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting," *The Journal of Machine Learning Research*, vol. 15, pp. 1929–1958, Jun. 2014.

[22] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard *et al.*, "Tensorflow: A system for large-scale machine learning." in *OSDI*, vol. 16, 2016, pp. 265–283.

[23] F. Chollet *et al.*, "Keras: The Python deep learning library," *Astrophysics Source Code Library*, 2018.

[24] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[25] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[26] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y.-S. Choi, L. Anttila, S. Talwar, and M. Valkama, "Full-duplex mobile device: Pushing the limits," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 80–87, Sep. 2016.

[27] K. Pärlin, T. Riihonen, and M. Turunen, "Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.

PUBLICATION 4

Full-Duplex Tactical Information and Electronic Warfare Systems

K. Pärlin, T. Riihonen, V. Le Nir, M. Bowyer, T. Ranström, E. Axell, B. Asp, R. Ulman, M. Tschauner and M. Adrat

IEEE Communications Magazine 59.8, Aug. 2021, 73–79
DOI: 10.1109/MCOM.001.2001139

Full-Duplex Tactical Information and Electronic Warfare Systems

Karel Pärlin, Taneli Riihonen, Vincent Le Nir, Mark Bowyer, Thomas Ranström, Erik Axell, Börje Asp, Robert Ulman, Matthias Tschauner, and Marc Adrat

***Abstract*—Electromagnetic spectrum is a scarce resource becoming increasingly congested as information technologies advance. This is particularly concerning in the military domain, where frequencies are contested for by both CIS and EW systems. The success of NATO activities necessitate mission-critical communications with increasing throughput, hidden from enemy signals intelligence, robust against electronic attacks, and compatible with host EW tasks. In response, the NATO STO IST-175 research task group is working on the disruptive concept of FD radio technology to address those challenges. Military FD radios promise to increase the spectral efficiency and robustness of CIS and improve the performance of EW tasks through simultaneous operation and multifunctionality.**

INTRODUCTION

Tactical communication and information systems (CIS) utilize electromagnetic (EM) spectrum for sharing voice and data between battle units. At the same time, electronic warfare (EW) systems aim at achieving superiority in use of the same EM spectrum. Inevitably, CIS and EW affect each other, and consequently, both disciplines of military operation can benefit from coordinated use. This is especially evident as bandwidth requirements for CIS grow hand in hand with other battlefield technological advancements and congestion of EM spectrum becomes increasingly problematic.

Consequently, military radios must use spectrum efficiently to fulfill the communication needs without compromising reliability requirements [1]. Thus, the outcome of future military operations will depend on information services being provided with increased data throughput, strict timing requirements, robustness against adversarial EW, and compatibility with host EW systems. However, in practice compatibility between CIS and EW systems is often difficult to achieve because both may require to operate on the same frequency bands. This is, for instance, almost always true when considering compatibility between interrelated EW tasks such as signals intelligence and jamming.

Karel Pärlin is with Rantelon; Taneli Riihonen is with Tampere University; Vincent Le Nir is with the Belgian Royal Military Academy; Mark Bowyer is with Airbus Defence & Space; Thomas Ranström, Erik Axell, and Börje Asp are with the Swedish Defence Research Agency (FOI); Robert Ulman is with the US Army Research Office; Matthias Tschauner and Marc Adrat are with Fraunhofer FKIE.

Similarly to most radio technology, CIS and EW technology have evolved into their current state with the assumption that same-frequency simultaneous transmit and receive (SF-STAR) operation, also referred to as in-band full-duplex (FD) operation, is intractable. This technological limitation is a significant contributor to spectral congestion problems and ineffectiveness to carry out simultaneous CIS and EW tasks. However, recent research is forcing a paradigm shift as this assumption is being overturned by FD radios [2].

In the civilian domain, many challenges related to FD radios have already been solved and the technology is seriously being considered for inclusion in next generation wireless communication standards [3]. However, current solutions cannot be directly adopted for the military domain because of significantly different operational conditions like lower carrier frequencies, higher transmit powers, and narrower bandwidths. Overcoming these challenges and taking advantage of this paradigm shift in the military domain can result in technological superiority in the battlefield over conventional half-duplex (HD) radio technology as illustrated in Fig. 1.

As testament to that, the NATO Science and Technology Organization (STO) IST-175 research task group (RTG), which succeeds IST-ET-101 exploratory team [4], is working on introducing FD radio technology into the military domain, in order to enhance both CIS and EW applications. The RTG's aim is to first outline the specific applications and use cases for FD technology in the electronic battlefield and subsequently to solve some of the military-specific challenges related to implementing FD radios for those applications. In this article, we describe the scenarios focused on and capabilities developed within the RTG.

FULL-DUPLEX RADIO TECHNOLOGY

To date, most radio technology (civilian and military) is of HD type, meaning that simultaneous transmission and reception on the same frequency is impossible. This is because when a radio is transmitting a signal, it inevitably reaches the same radio's receiver, as illustrated in Fig. 2, causing self-interference (SI) that drowns out any signals-of-interest transmitted by other distant radios. Until recently, this limitation was considered too ambitious to overcome, and has therefore been circumvented and hidden from the user by employing either frequency-division duplex (FDD) or time-

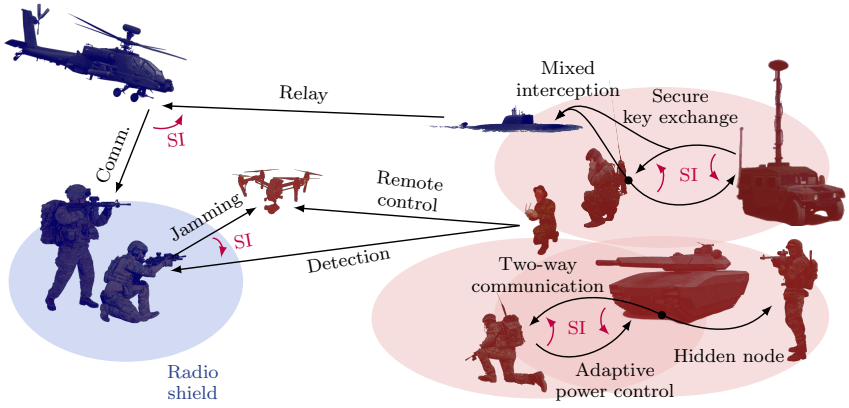


Figure 1. Conceptual use of military FD radios in the battlefield for enhanced CIS and EW.

division duplex (TDD) operation in almost every wireless application. Thus, different frequencies or time slots are used for transmission and reception.

The principal difference in FD radios compared to HD radios is addition of SI cancellation methods, shown in Fig. 2, to suppress different types of SI that inevitably leak into the receiver path. Ideally, SI would be cancelled digitally, however, because of the dynamic range limitations in analog-to-digital conversion, digital cancellation needs to be accompanied by analog methods [3]. The analog canceller typically needs to be designed for a specific carrier frequency and it delays and filters a copy of the transmitted signal so that the copy is in opposite phase to the SI, thus suppressing the SI. The digital canceller is frequency agnostic and works under similar principles as the analog canceller, additionally modelling nonlinearities that affect the SI. Altogether, both stages prevent powerful SI from overpowering the typically weak received signal-of-interest. Current state-of-the-art FD radio prototypes, including those that have been developed by RTG members, achieve SI cancellation in excess of 100 dB [4] and provide reasonable communication conditions in non-military wireless applications [3]. The most obvious advantage of FD radios is to **double the capacity in a point-to-point communication** — which alone is a significant advantage over FDD and TDD operating modes.

For large wireless networks, such as tactical mobile ad hoc networks (MANETs) [5], the advantages of FD operation can be equally influential. Although FD operation inherently increases interference within a network as the number of simultaneous transmissions increases, the overall **throughput of an FD network is improved** compared to an HD network, so long as sufficient SI cancellation is provided and a medium access control protocol designed for FD operation is used [6].

Throughput is not the only aspect improved by FD operation in wireless networks. Tactical MANETs are expected to provide completely self-forming, self-healing, and decentralized platforms for tactical units to join and leave swiftly; particularly in highly time-varying topologies, typical where battlefield infrastructure is lacking or inaccessible due to rapid deployment [1]. Such MANETs face numerous challenges, including cognitive spectrum usage, relaying, and hidden nodes, which all can be addressed with FD operation.

When considering EW aspects, consequences of FD radio technology can result in an equivalent of a wireless superpower, especially as FDD and TDD have severe limitations for many EW tasks, such as detection and neutralisation [7]. The former, FDD, is almost never considered for combined detection and neutralisation, because that would mean detecting and neutralising on different frequencies. When signals of interest fall into either frequency range, only one of two outcomes can arise — detection without neutralisation or neutralisation without detection, neither of which is desirable.

Therefore, TDD is typically used, forcing a trade-off between situational awareness and neutralisation efficiency. By dividing detection and neutralisation operations in time, situational awareness and neutralisation efficiency depend

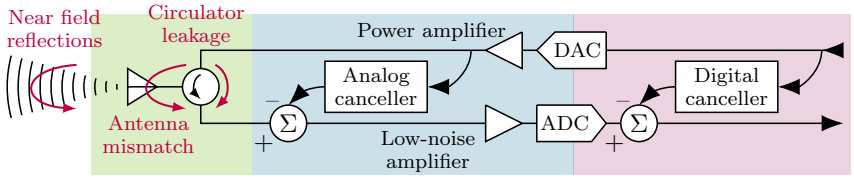


Figure 2. General architecture of FD radios, with passive, analog, and digital cancellation of SI. Digital-to-analog converter is abbreviated as DAC and analog-to-digital converter as ADC.

on the portion of time spent in either state. This is where the FD radio technology excels — it removes that trade-off and opens the way for combining different EW tasks on the same frequency simultaneously. Furthermore, EW tasks can be combined with CIS, introducing EW capabilities to devices that are classically used only for communications. Thus, FD radio technology is a **key enabling technology to develop multifunction military radios** combining CIS and EW functions, which has long been coveted by defence forces [8].

One such case is jamming and signals intelligence, where by using HD radio technology, it is impossible to simultaneously achieve continuous jamming efficiency and situational awareness. Thus, neutralising hostile wireless communications is often approached in an all or nothing way, through jamming the entire enemy frequency band. This is a robust approach given the limitations of modern HD radio technology. However, it requires a lot of power to cover large frequency bands and is also likely to damage friendly communications within the covered frequency bands.

Alternatively, with FD radios, jamming energy can be directed on demand to target only the radio frequency (RF) communications used by the enemy, hence making sure that **collateral damage is minimized**. This is possible because FD technology allows simultaneous jamming, analysis of jamming effectiveness, and to sense if the jammed signal changes its operation mode. Consequently, jamming can be adapted to be more effective and focus only on the malicious RF systems. Not only do FD radios give an advantage to defensive technologies, they also benefit attack-minded applications, which itself is motivation not to forgo this radio superpower.

Enhanced Communication and Information Systems

Within the first of its two demonstrator groups, the RTG is working towards applying the FD radio technology for augmenting CIS. When enhancing tactical CIS, the aim is similar to civilian FD applications. In both cases the objective is, ideally, to double spectral efficiency. This is a significant advantage over conventional HD radio technology, especially when considering how congested and limited military spectrum allocations are.

The main differences between the military and civilian domains arise in frequency bands used and battlefield operating conditions. Many military communication systems operate at either high frequency (HF), very high frequency (VHF), or low ultra high frequency (UHF) band, with higher powers and narrower bandwidths than typical in high UHF band, where the FD radio technology has so far mostly been demonstrated to be feasible with lower powers and comparatively wider bandwidths.

While 100 dB of SI cancellation is considered sufficient for many civilian applications, a military FD radio needs to provide additional 50 dB or more of SI cancellation. Due to the lower carrier frequency, the analog canceller circuit needs delay lines in the order of meters of electrical wavelength leading to challenges in compact design. Furthermore, with respect to typical tactical communication scenarios, fast analog canceller tuning is needed. However, due to the narrow signal bandwidth, the SI estimation can only be provided at very low rates, which subsequently leads to degraded SI cancellation.

Aside from these challenges, the improvement in wireless network throughput resulting from FD operation may fall short of ideal due to the typically asymmetrical data flow, imperfect SI cancellation, and increased inter-node interference. Nevertheless, as discussed next, FD radio technology has potential to improve several other aspects of CIS networks, which in turn can enhance situational awareness and network security.

Cognitive Radio Networks

One of the most promising technologies considered for coping with the limited nature of RF spectrum is dynamic spectrum sharing through cognitive radio (CR). The fundamental idea behind CR is to opportunistically share RF spectrum as opposed to operating within predetermined frequency and time spaces. This allows better use of spectral resources based on operational needs. However, CR relies first and foremost on having an overview of the spectrum usage before deciding to use any spectrum areas. It is also beneficial to retain that overview during transmissions, in order to continue learning from the environment and keep adapting to it, e.g., to detect multi-access collisions or adversarial intervention.

It has been shown that FD-enhanced CR offers higher throughput, higher probability of detection and reduced sensing time, all of which empowers CIS [6], [9]. In tactical scenarios, CR expands beyond just dynamic spectrum sharing as CRs can work around adversarial electronic attacks, especially when enhanced with FD capabilities. For example, FD enables swift and adaptive power control to lower the probability of detection, or enables to detect a jamming attack from an adversary, while simultaneously transmitting tactical communications to an ally on the same frequency channel [10]. Successful detection of electronic attacks enables the radio to take appropriate countermeasures against the attacks, e.g., switching the channel frequency. A combination of cognitive and FD capabilities enables truly multifunctional military radios capable of efficient fusion between CIS and EW based on operational needs.

Moreover, cognition is often envisioned to become a capability of the network, not just being limited to the individual radio. As such, a CR network can build local knowledge about environment (spectral and topological) to reach overall network goals. In military applications, cognitive networking capabilities are especially of interest as a mechanism for intelligently adapting to the dynamics of the theater of war and coping with the temporal nature of tactical

networks [11]. Through cross-layer management and information exchange between all layers of the OSI protocol stack, the spectrum information gathered by an FD-enhanced CR could be propagated throughout the adaptive tactical network to improve resilience, lower probability of detection, and increase throughput of tactical end-to-end communications.

RELAYING

Information flow from data sources to consumers in the modern battlefield is crucial to the success of military operations. However, in the hostile environments where military networks typically operate, provision of robust and dependable connections is a significant challenge. The entirety of CIS systems is often complex, consisting of scattered networks across the battlefield from tactical edge networks (TENs) to the theater of war. In order to tackle those issues, self-organizing and information-centric networking paradigms have been recently proposed [12]. Further, integral to self-organizing and information-centric networking is the use of relays, sometimes referred to as gateways, between the different scattered networks. Traditionally, using conventional HD radios, relaying is achieved by TDD or FDD, where the relay has receive and transmit time slots or frequency channels.

Compared to HD relays, FD operation promises to increase relaying channel capacity, as a single frequency channel is used simultaneously for receiving and forwarding [6]. Additionally, FD radio technology enables relays to seamlessly combine legacy CIS networks and systems that are not designed to work with relays specifically. That is because FD is a more transparent option than HD, in the sense that FD relaying does not introduce timing nor frequency constraints imposed by the use of TDD or FDD. As such, FD relays, including airborne relays for beyond line-of-sight coverage [13], could be used to extend the operational range of CIS networks as illustrated in Fig. 3. However, as with most FD applications, residual SI becomes the performance limiting factor and the full extent of the advantages of using FD over HD in relaying depend on the SI cancellation performance.

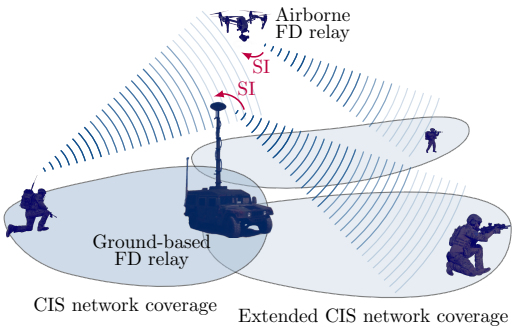


Figure 3. Tactical FD relays can seamlessly extend the coverage of CIS networks.

In hostile environments, FD relays can play an important role in delivering robustness and physical security. Instead of simultaneous reception and transmission, tactical relays with FD capabilities can monitor for adversarial interference while at the same time transmitting information to allies or receive information from allies while simultaneously interfering with its reception by adversarial intelligence. In the first case, interference awareness can aid self-organization within tactical networks. In the second case, simultaneous reception and jamming can create an FD radio shield over the TEN and prevent adversaries from intercepting the host forces' communications or locating units within the TEN. Should the operational scenario require, FD relays can effortlessly become amplify-and-forward eavesdropping relays for carrying out signals intelligence on approaching adversaries.

OUT-OF-BAND INTERFERENCE

As with in-band SI, radio systems that use closely located frequencies may also, due to out-of-band (OOB) emission, suffer from strong interference when transmission and reception occur simultaneously. This problem is particularly prevalent when radios are co-located on the same platform and subject to limited physical separation [8]. The lack of space due to co-siting may equate to poor EM isolation between radios, which results in appreciable interference even when OOB emission requirements are met. This issue is especially prominent in military applications, where it can have a significant negative effect on robustness to interference, communication range, as well as frequency allocation.

When co-located radios are treated like an FD transceiver, the transmitted signal can be forwarded to receiving radios on the platform. Each radio can then perform interference cancellation in their respective spectrum, reducing OOB interference. Though additional hardware is necessary, implementation of such OOB interference cancellation can be done without introducing complex scheduling, or requiring additional time or frequency resources [14]. Consequently, removing OOB interference can significantly boost both robustness of radios on the same platform as well as enable functional communications in situations where this was previously not possible. Furthermore, cancellation of OOB interference can enable integrating multiple RF tasks simultaneously onto a single platform, which is of significant interest in the military domain and has been pursued through programs such as the Advanced Multifunction Radio Frequency Concept and Integrated Topside [8]. For example, radar, EW operations, and communications could be integrated into a multifunction radio with shared aperture.

NATO NARROWBAND WAVEFORM

In general, FD radio technology is waveform agnostic, meaning that the type of waveform used does not affect the capability to transmit

and receive simultaneously on the same frequency. Yet, some properties of a waveform (e.g., bandwidth, crest factor, and frequency hopping) do have an impact on the complexity and performance of an FD radio. Furthermore, in order to take advantage of FD radios in multi-hop configuration, networking protocols need to take FD capabilities into account [3]. As such, the NATO Narrowband Waveform (NBWF) is a prominent candidate to benefit from FD radio technology. It is a modern combat-net radio standard that includes both the waveform and networking capabilities, with the aim to enhance interoperability among NATO forces in multinational missions.

The standardization of NBWF covers the three lowest layers of the OSI networking model: physical, data link, and network layers. On physical layer, the NBWF employs continuous phase modulation (CPM) for spectral efficiency, where the constant envelope property allows transmitter power amplifiers (PAs) to operate near saturation, improving energy efficiency. The same properties that make CPM spectral and energy efficient are also expected to result in efficient SI cancellation. On data and network link layers, NBWF is designed for limited link capacity and harsh interference environments, employing crosslayer link metrics to manage interference and link quality issues. Those characteristics and capabilities are essential to managing residual SI and inter-node interference in FD-capable radio networks.

The NBWF is essentially a single-channel MANET, offering several transmission modes, supporting occupied bandwidths of 25 kHz and 50 kHz, and providing data throughput from 20 kpbs up to 82 kbps. The design allows radios to adapt waveform and power parameters to achieve the desired quality-of-service without wasting resources. Similarly to a general MANET, a multi-hop NBWF network suffers from the hidden node problem, degrading a NBWF network's throughput. Fortunately FD operation is a promising candidate to solve the hidden node challenge [3]. The RTG members have been studying, implementing, and demonstrating FD radio technology using the NBWF as an example tactical waveform. The results of RTG's multinational demonstrator provide a proof of concept for increasing spectral efficiency of the NBWF through FD radio technology [4].

Enhanced Electronic Warfare

In parallel with CIS enhancement efforts, the RTG is working towards applying FD radio technology for EW tasks. Specifically for counter-drone purposes as drones pose an increasingly large threat and RF-based counter-drone methods are prominent [15]. In FD operation mode, a counter-drone node can simultaneously interfere with various RF systems used by a drone and itself receive those signals uninterrupted. The interference creates an invisible EM dome, a so called FD radio shield, around the FD node as illustrated in Fig. 4. Interfering could, in this case, mean either jamming or spoofing, and the concept of FD radio shield has already been shown feasible in a laboratory environment by the RTG for, e.g., disabling drone remote control (RC) links by jamming while simultaneously detecting the same [10].

Ground-Based Radio Shield

A ground-based FD radio shield (either mobile or stationary) can be used to prevent:

- drones from communicating within the swarm while at the same time monitoring the swarms' attempts to communicate within itself — this allows simultaneously preventing the swarm (even an autonomous swarm) from operating as a coherent unit (as communications within the swarm are essential for the functioning thereof) and to track drones by their RF fingerprints (classify and locate individual drones).
- ground station from directing the drone swarm while at the same time intercepting command and control signals — this means that within the radio shield, the swarm is completely cut off from its operator, but the FD node can still observe (classify and locate) the ground control station.
- drones inside the swarm from determining their geographical position using global navigation satellite systems (GNSSs) while at the same time retaining the FD node's own access to GNSS — the swarm can not determine its position using GNSS but the FD node can, which is essential in case of a mobile FD node.
- drones from positioning each other inside the swarm using RF-based methods (two-way ranging or radar-based positioning) while at the same time detecting those efforts — the ability to position each other within the swarm is essential for the operation of a swarm and without this, the swarm becomes paralyzed, yet with FD capabilities those positioning attempts can still be detected.

On the other hand, a ground-based FD radio shield also facilitates:

- locating drones while simultaneously jamming their RC links and other RF systems by using joint radar and jamming waveforms — FD radio technology can become

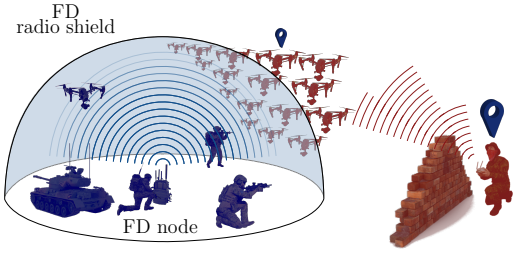


Figure 4. Defensive FD radio shield — simultaneously restricting unauthorized drones access to the defended airspace and monitoring the RF spectrum (detection, classification, and locating of drones and their control stations).

a key enabler for multifunction military radios and RF convergence that have for long been coveted by armed forces [8].
- controlling an allied drone (or drone swarm) from the ground station while at the same time simultaneously sensing for enemy drone's RC signals and electronic attacks within the same frequency band that is used for allied drone RC.

Aerial Radio Shield

Another, more proactive, option is to use FD radios for countering drones as illustrated in Fig. 5. Instead of using a ground-based FD radio shield, a drone itself could be equipped with FD capabilities, allowing to

- interfere with the entire RF spectrum (ground control, inter-drone communications, two-way-ranging, radar) used by a malicious swarm, while itself retaining the ability to communicate with its control station — when the host drone operates on the same frequency as the adversarial drones, FD technology is needed so that the host drone can transmit interference and receive commands at the same time.
- transmit spoofed GNSS signals while itself receiving the actual ones — this could be used to direct the malicious swarm away from its target, although successful GNSS spoofing itself can be expected to be a highly complicated task.
- jam from air, which can be much more energy efficient than jamming from ground, especially if the drone can get close to the swarm — this is a considerable advantage of FD radio technology as this would simultaneously paralyze the swarm but also complicate localization of allied forces on the ground by the enemy (that is typically a high priority).
- use the drone for scouting (e.g., transmitting aerial video feed) while at the same time detecting for frequency usage on the same frequencies by adversarial drones.

Full-Duplex Adversaries

It is also relevant to consider, how FD capabilities in the hands of adversaries affect the electronic battlefield. When facing two adversarial HD nodes that utilize FDD for communication, as is quite typical for drones, a jammer needs to target both the uplink and the downlink frequency channels to completely cut the communication link. In the case of two adversarial FD nodes, only one common frequency channel needs to be targeted. On the other hand, if the enemy is using FD link between two nodes, e.g., for operating a drone, then radiolocating the nodes or eavesdropping on the communication link can be complicated due to the mixed reception of the two signals. As a result, adversarial FD communications can become an easier target compared to HD communications when intentionally interfering but a tougher target when monitoring.

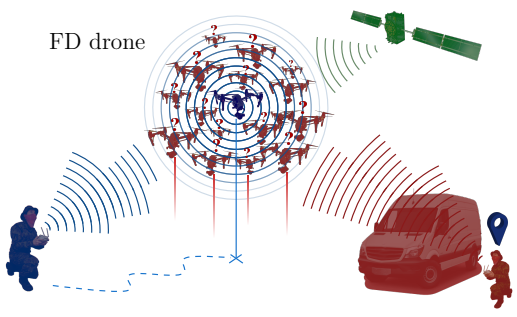


Figure 5. Disruptive FD drone — simultaneously operating on and jamming the same frequencies that are used by the adversarial drones.

But of course the adversary is not limited to applying FD only for communications. The adversary can combine its communications with EW operations or simply combine different EW operations as proposed throughout this article so far. In this case, when the host is limited to HD capabilities, the FD benefits will simply work for adversary's advantage. When both teams use FD capabilities, the playing field becomes increasingly complex. For example, when the adversary is using FD radios to enhance physical layer security and prevent the host from eavesdropping, the host could counter-strike with simultaneous jamming and eavesdropping to pressure the adversary into increasing communication transmission powers.

Cognitive and Multifunctional Electronic Warfare Systems

The aspects considered in this section are made possible by FD radios or FD radio technology significantly improves on the performance that can be achieved when compared to conventional HD radio technology. This is one of the next steps in radio evolution that will enable the growing list of requirements that modern EW faces in congested spectrum environments. However, the advantages to EW applications extend beyond the counter-drone context, which is the main focus of the RTG's second demonstrator group and was described in detail above.

Much more widely, the importance of EW as a whole is on the rise as EM spectrum is recognised as a key operational environment. Classically, all EW tasks have been separated from CIS functions to large extent, so that EW operations do not interfere with the host's CIS [8]. Similarly to the simultaneous combination of different counter-drone aspects, the advent of FD radios enables that paradigm to shift. As a result, and in the future, many of the CIS tasks can be combined with EW tasks to enhance both aspects. Broadly, these combinations mean either simultaneous communication and jamming, interception and communication, or interception and jamming [7]. Such combinations enhance CIS and EW with an added layer of physical security or perception of spectral environment.

CONCLUSIONS

Research into FD radio technology has progressed in strides over the recent decade with mostly civilian/commercial applications in mind. However, the technology is yet to make its way into standardized networks and it is evident that in order to take advantage of the FD concept in CIS and EW systems, much work still lays ahead. Specifically operating frequency ranges and SI cancellation levels must be extended to satisfy the wide requirements set by military radio equipment.

The NATO STO IST-175 RTG is working on overcoming these challenges to take advantage of the FD concept and enhance both CIS and EW systems. In this article, we have discussed the military specific challenges of FD radios and outlined the most promising applications for FD enhancement in the defence domain. As a result of FD operation, the spectral congestion issue within CIS can be alleviated, compatibility with EW equipment improved, and robustness against EW attacks enhanced. Moreover, FD enables truly multifunctional military radios that can simultaneously carry out both CIS and EW functions.

ACKNOWLEDGMENT

The research work leading to this article was supported in part by the Estonian Ministry of Defence, in part by the Academy of Finland, in part by the Finnish Scientific Advisory Board for Defence, as well as in part by the EDA Defence Innovation Prize.

REFERENCES

[1] N. Suri *et al.*, "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *IEEE Commun. Mag.*, vol. 48, no. 10, pp. 60–69, Oct. 2010.

[2] T. Riihonen *et al.*, "Inband full-duplex radio transceivers: A paradigm shift in tactical communications and electronic warfare?" *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 30–36, Oct. 2017.

[3] Z. Zhang *et al.*, "Full-duplex wireless communications: Challenges, solutions and future research directions," *Proc. IEEE*, vol. 104, no. 7, pp. 1369–1409, Jul. 2016.

[4] M. Adrat *et al.*, "Full duplex radio technology – Increasing the spectral efficiency for military applications," NATO, Tech. Rep., Jan. 2020.

[5] J. L. Burbank *et al.*, "Key challenges of military tactical networking and the elusive promise of MANET technology," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 39–45, Nov. 2006.

[6] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2017–2046, Nov. 2015.

[7] K. Pärlin and T. Riihonen, "Full-duplex transceivers for defense and security applications," in *Full-Duplex Communications for Future Wireless Networks*, H. Alves, T. Riihonen, and H. A. Suraweera, Eds. Springer, Apr. 2020, ch. 9, pp. 249–274.

[8] G. C. Tavik *et al.*, "The advanced multifunction RF concept," *IEEE Trans. Microw. Theory Tech.*, vol. 53, no. 3, pp. 1009–1020, Mar. 2005.

[9] K. Mourougayane and S. Srikanth, "A tri-band full-duplex cognitive radio transceiver for tactical communications," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 61–65, Feb. 2020.

[10] T. Riihonen, "Military applications," in *In-Band Full-Duplex Wireless Systems Handbook*, K. E. Kolodziej, Ed. Artech House, Mar. 2021, ch. 17, in press.

[11] H. Tang and S. Watson, "Cognitive radio networks for tactical wireless communications," Defence Research and Development Canada - Ottawa Research Centre, Tech. Rep., Dec. 2014.

[12] G. M. Leal *et al.*, "Empowering command and control through a combination of information-centric networking and software defined networking," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 48–55, Aug. 2019.

[13] M. A. Rupar *et al.*, "Airborne beyond line-of-sight communication networks," *IEEE Commun. Mag.*, vol. 58, no. 8, pp. 34–39, Aug. 2020.

[14] T. Ranström and E. Axell, "Full duplex based digital out-of-band interference cancellation for collocated radios," in *Proc. Wireless Commun. Netw. Conf.*, May 2020.

[15] I. Guvenc *et al.*, "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

BIOGRAPHIES

KAREL PÄRLIN (karel.parlin@rantelon.ee) received his M.Sc. degree in electrical engineering from Tallinn University of Technology, Estonia, in 2017. He is an engineer at Rantelon in Tallinn, Estonia.

TANELI RIIHONEN [S'06, M'14] (taneli.riihonen@tuni.fi) received his D.Sc. degree in electrical engineering from Aalto University, Finland, in 2014. He is a tenure-track assistant professor at Tampere University, Finland.

VINCENT LE NIR (vincent.lenir@rma.ac.be) received his Ph.D. degree in electronics from the National Institute of Applied Sciences, France, in 2004. He is a senior researcher at the Royal Military Academy in Brussels, Belgium.

MARK BOWYER (mark.bowyer@airbus.com) received his Ph.D. in solid state electronics from the University of Kent, United Kingdom, in 1993. He is a senior expert in secure communications at Airbus Defence & Space in Portsmouth, United Kingdom.

THOMAS RANSTRÖM (jranstrom@usf.edu) received his M.Sc. degree in electrical engineering from Linköping University, Sweden, in 2018. He is a research engineer at the Swedish Defence Research Agency (FOI) in Linköping, Sweden and a Ph.D. student at the University of South Florida in Tampa, United States.

ERIK AXELL (erik.axell@foi.se) received his Ph.D. degree in communication systems from Linköping University, Sweden, in 2012. He is a senior scientist at the Swedish Defence Research Agency (FOI) in Linköping, Sweden.

BÖRJE ASP (borje.asp@foi.se) is a research director at the Swedish Defence Research Agency (FOI) in Linköping, Sweden.

ROBERT ULMAN (robert.j.ulman.civ@mail.mil) received his Ph.D. degree in electrical engineering from the University of Maryland, United States, in 1997. He is a program manager at the US Army Research Office in Triangle Park, North Carolina, United States.

MATTHIAS TSCHAUNER (matthias.tschauner@fkie.fraunhofer.de) received his Dipl.-Ing. degree in electrical engineering from RWTH Aachen University, Germany, in 2011. He is a research assistant at Fraunhofer FKIE in Wachtberg, Germany.

MARC ADRAT (marc.adrat@fkie.fraunhofer.de) received his Dr.-Ing. degree in electrical engineering from RWTH Aachen University, Germany, in 2003. He is the head of the SDR research group at Fraunhofer FKIE in Wachtberg, Germany.

PUBLICATION 5

Estimating and Tracking Wireless Channels under Carrier and Sampling Frequency Offsets

K. Pärlin, T. Riihonen, V. Le Nir and M. Adrat

IEEE Transactions on Signal Processing 71.Mar. 2023, 1053–1066
DOI: 10.1109/TSP.2023.3259140

Estimating and Tracking Wireless Channels Under Carrier and Sampling Frequency Offsets

Karel Pärlin, Taneli Riihonen, *Senior Member, IEEE*, Vincent Le Nir, and Marc Adrat

***Abstract*—This article addresses the challenge of estimating and tracking wireless channels under carrier and sampling frequency offsets, which also incorporate phase noise and sampling time jitter. We propose a novel adaptive filter that explicitly estimates the channel impulse response, carrier frequency offset, and sampling frequency offset by minimizing the mean-square error (MSE) and, when the estimated parameters are time-varying, inherently performs tracking. The proposed filter does not have any requirements for the structure of the waveform, but the digital transmitted waveform must be known to the receiver in advance. To aid practical implementation, we derive upper bounds for the filter's step sizes. We also derive expressions for the filter's steady-state MSE performance, by extending the well-known energy conservation relation method to account for the self-induced nonstationarity and coupling of update equations that are inherent in the proposed filter. Theoretical findings are verified by comparison to simulated results. Proof-of-concept measurement results are also provided, which demonstrate that the proposed filter is able to estimate and track a practical wireless channel under carrier and sampling frequency offsets.**

***Index Terms*—Adaptive filtering, frequency offset, mean-square error, steady-state analysis.**

I. Introduction

OSCILLATOR inaccuracies cause two common impairments in wireless systems — mismatches between transmitter and receiver carrier generators result in a carrier frequency offset, while mismatches between sampling clocks result in a sampling frequency offset. Both of those impairments are further aggravated by the random fluctuations of oscillators and the wireless propagation. The former causes the frequency offsets to vary with time and the latter can have equivalent negative consequences due to Doppler shift. In many cases, time-varying frequency offsets can be damaging or destructive to the performance of wireless systems [1], [2].

Manuscript received 4 January 2022; revised 29 August 2022 and 1 February 2023; accepted 13 March 2023. Date of publication 20 March 2023; date of current version 6 April 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Behtash Babadi. This work was supported in part by the Academy of Finland under Grants #315858, #341489, and #346622 and in part by the Finnish Scientific Advisory Board for Defence. *(Corresponding author: Karel Pärlin.)*

Karel Pärlin and Taneli Riihonen are with the Faculty of Information Technology and Communication Sciences, Tampere University, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi; taneli.riihonen@tuni.fi).

Vincent Le Nir is with the Signal and Image Center, Royal Military Academy, B-1000 Brussels, Belgium (e-mail: vincent.lenir@mil.be).

Marc Adrat is with the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), 53343 Wachtberg, Germany (e-mail: marc.adrat@fkie.fraunhofer.de).

Digital Object Identifier 10.1109/TSP.2023.3259140

As such, estimating and compensating frequency offsets in those cases is essential. Although not the main focus of this work, a popular example are orthogonal frequency division multiplexing (OFDM) systems, where synchronization of the carrier frequency at the receiver must be performed accurately in order to avoid loss of orthogonality between the subcarriers. Those systems can only tolerate carrier offsets that are a fraction of the spacing between the subcarriers without large degradation in performance [3], [4], [5]. The performance of OFDM systems can also degrade due to sampling frequency offsets [4], [6], although this is often less significant. Various methods for joint carrier and sampling frequency offset estimation and compensation in OFDM systems exist [7], [8], [9], [10], [11], [12], [13], [14], not to mention abundant works on only either of the offsets. However, those methods largely rely on the properties that are strictly characteristic to OFDM and are not directly applicable to other applications.

Carrier and sampling frequency offsets also pose a major challenge in known-interference cancellation. The capability to cancel known interference is a fundamental prerequisite of physical layer security schemes that envision preventing eavesdropping by superposing the signal of interest with some interference that is known only to the legitimate receiver. Perfect known-interference cancellation has been for long assumed feasible in theoretical physical layer security works without practical basis [15], [16]. However, lack of proper frequency synchronization actually has a considerable negative effect on the cancellation performance [16], [17]. This is leading to the development of interference cancellation methods with built-in frequency synchronization [18], [19].

Frequency synchronization, as well as time synchronization, is also a key issue in interference alignment and distributed beamforming. Interference alignment and distributed beamforming envision concurrent transmissions that result in a substantial increase in wireless network's total capacity [20] or an increase in range and energy efficiency [21]. In addition, since distributed beamforming entails directing more power in the desired direction, less is scattered in the undesired directions, possibly increasing security [21]. However, again the challenges in realizing the benefits of interference alignment and distributed beamforming include coordinating the transmitters for distributed information sharing plus carrier and sampling synchronization, so that the transmissions combine as necessary at the destination [22].

Bistatic radars are promising supplements to classical monostatic systems, and they too face the challenge of synchronization.

Unlike a monostatic radar, a bistatic radar has a transmitter and receiver on separate platforms which results in various operational advantages like, e.g., additional information about the scene, as the scattering characteristics of objects depend strongly on the line-of-sight vectors to the transmitter and receiver. Another advantage is the potential of cost reduction by using one transmitter, or even illuminators of opportunity, and several passive receivers [23]. However, separation of the transmit and receive platforms necessitates time and frequency synchronization for coherent signal processing and range measurement [24], [25].

Similar challenges arise in the acoustic domain. For example, in underwater acoustic communications the use of wideband modulation and low velocity of acoustic waves mean that Doppler shifts have a significantly larger impact than in the electromagnetic domain and these shifts need to be compensated for [2]. In acoustic echo control, the sampling frequency offsets between separate devices, if not compensated for, can cause poor echo cancellation performance [26], [27].

It is often so that adaptive filters are used in such nonstationary environments and consequently frequency offsets compromise the conventional filters' performance [28]. To that end, various extended adaptive filters have been proposed that are able to track certain nonstationarities or nonlinear impairments. For example, least mean squares (LMS)-type gradient descent has been used for explicit time-delay estimation [29] as well as power amplifier distortion [30] and IQ imbalance compensation [31]. An LMS-type adaptive algorithm has been proposed for joint channel estimation and explicit sampling rate correction in acoustic echo control applications [27]. The adaptive notch filter proposed in [32] is a simple algorithm capable of extracting a nonstationary narrowband signal buried in noise, being essentially a carrier frequency offset tracker. However, a single general algorithm for tracking a channel under both carrier and sampling frequency offsets, without specific requirements on the waveform, is still missing.

The purpose of this article is to present an efficient adaptive algorithm for estimating and tracking a channel under time-varying carrier and sampling frequency offsets when the receiver knows the signal that is to be transmitted, or at least a considerable part of it, in advance. The presented algorithm aims to be waveform-agnostic and not strictly rely on the characteristics of the underlying system. Hence, it is potentially applicable to the aforementioned concepts and beyond. We provide a thorough analysis on the optimal selection of the algorithm parameters (viz. three step sizes) to facilitate rapid convergence, and we carry out theoretical steady-state analysis for the proposed algorithm by extending the well-known energy conservation relation [33]. The extended relation introduces nonstationary a priori errors for each update equation and decouples the errors of separate update equations to account for the algorithm's self-induced nonstationarity. Several supporting simulations are provided, which verify the theoretical results and demonstrate that the algorithm is able to track time-varying frequency offsets. Furthermore, proof-of-concept measurement results are presented, which illustrate that the algorithm is capable of explicitly estimating and tracking a wireless channel and

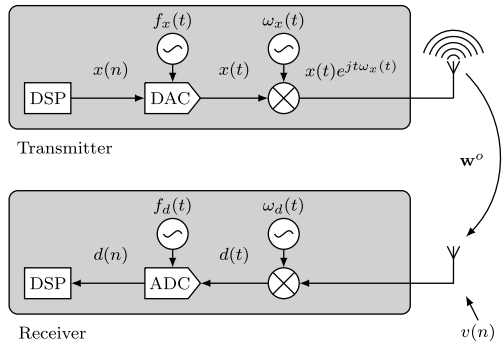


Fig. 1. General system model considered in this work, focusing on the carrier and sampling frequency offsets together with the channel impulse response between a transmitter and a receiver. In this work we assume that the digital transmitted signal $x(n)$ is known to the receiver.

frequency offsets between two radios. The proposed algorithm is positioned with regards to the existing works and comparisons are made throughout.

The rest of this article is organized as follows. Section II introduces a general system model and in Section III the novel adaptive algorithm is presented for estimating and tracking the parameters of the system model. Also, in Section III bounds for the algorithm's step sizes are derived. In Section IV, expressions are derived for the steady-state mean-square error (MSE) of the proposed algorithm, by introducing an energy conservation relation that accounts for the algorithm's self-induced nonstationarity. Section V provides a comparison of the theoretical MSE results to simulations, proof-of-concept experimental results, and a brief comparison. Finally, conclusions of the study are given in Section VI.

Notation: Small boldface letters are used to denote vectors, and capital boldface letters are used to denote matrices, e.g., $\mathbf{w}$ and $\mathbf{R}$. Furthermore, the symbol * denotes Hermitian conjugation for vectors and complex conjugation for scalars. The identity matrix is denoted by $\mathbf{I}$ and a zero vector is denoted by the boldface letter $\mathbf{0}$, both with dimensions compatible to each context. The iteration index is placed as a subscript for vectors and between parentheses for scalars, e.g., $\mathbf{w}_n$ and $v(n)$. All vectors are column vectors, except for two vectors, namely, the input data vector denoted by $\mathbf{x}_n$ and its resampled counterpart $\mathbf{y}_n$, which are taken to be row vectors for convenience of notation. Lastly, $E[\cdot]$ is the statistical expectation operator.

II. System Model

The system model considered in this work focuses on the time-varying sampling and carrier frequency offsets between a transmitter and a receiver along with the channel that separates the two as illustrated in Fig. 1. The relative sampling frequency offset between the two devices is denoted as $\eta^o + \beta(n)$, where $\eta^o = \Delta T/T_x$ represents the fundamental time-invariant offset with $\Delta T = 1/f_d - 1/f_x$ being the difference between the sampling periods at the receiver and transmitter, f_d is the sampling frequency at the receiver, f_x is the sampling frequency

at the transmitter, and $\beta(n)$ is the time-varying offset, including sampling jitter. The carrier frequency offset is denoted as $\epsilon^o + \phi(n)$, where ϵ^o denotes the fundamental time-invariant offset $\epsilon^o = \omega_d - \omega_x$ between the receiver and transmitter carrier frequencies, ω_d is the carrier frequency at the receiver, ω_x is the carrier frequency at the transmitter, and $\phi(n)$ is the time-varying offset, including phase noise. Lastly, we denote the finite impulse response of the complex-valued channel with order M as $\mathbf{w}^o$.

The transmitter broadcasts a complex signal $x(n)$ that, in its discrete-time form, is known to the receiver. However, due to noise, channel, and mismatches in carrier and sampling frequencies at the transmitter and the receiver, the discrete-time signal at the receiver becomes

$$d(n) = \mathbf{y}_n^o \mathbf{w}^o e^{j\sum_{i=1}^{n}\epsilon^o + \phi(i)} + v(n), \tag{1}$$

where $v(n)$ is the measurement noise, $\mathbf{y}_n^o$ accounts for sampling $x(t)$ with sampling frequency offset $\eta^o + \beta(n)$ so that

$$\mathbf{y}_n^o = \left[x\left(\sum_{i=1}^{n-M+1}(1+\eta^o+\beta(i))\right), \ldots, x\left(\sum_{i=1}^{n}(1+\eta^o+\beta(i))\right)\right] \tag{2}$$

and the multiplicative term $e^{j\sum_{i=1}^{n}\epsilon^o+\phi(i)}$ accounts for the carrier frequency offset.

This is a general system model that is relevant, e.g., for the following scenarios. Firstly, it holds in cases when known training data is used to estimate the channel impulse response and frequency offsets to improve subsequent information demodulation. Secondly, this general system model rather directly applies to the bistatic or multistatic radar scenario, in which case the receiver is familiar with the transmitted signal, but is interested in tracking the channel and frequency offsets to estimate range/velocity. Thirdly, in case of the known-interference cancellation scenarios, the received noise $v(n)$ can be considered to contain an unknown signal of interest, which is uncorrelated to the known signal $x(n)$ that is suppressed to facilitate processing the signal of interest.

III. Adaptive Estimation and Tracking

In order to derive an algorithm for estimating and tracking the parameters described in the system model, we first define the instantaneous error of the estimation process as

$$e(n) = d(n) - \mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{3}$$

where $\mathbf{w}_{n-1}$, $\epsilon(n-1)$, and $\eta(n-1)$ are respectively the estimates of the channel's impulse response $\mathbf{w}^o$, carrier frequency offset ϵ^o, and sampling frequency offset η^o at iteration n, and $\mathbf{y}_n$ is the result of resampling $x(n)$ with $\eta(n-1)$, so that

$$\mathbf{y}_n = \left[x\left(\sum_{i=1}^{n-M+1}(1+\eta(i-1))\right), \ldots, x\left(\sum_{i=1}^{n}(1+\eta(i-1))\right)\right]. \tag{4}$$

The instantaneous error $e(n)$ will contain $v(n)$ and excess noise from the algorithm's operation. In case of known-interference cancellation, the instantaneous error $e(n)$ would additionally contain some unknown signal of interest.

The aim of the adaptive filter is to update iteratively the system model parameter estimates $\mathbf{w}_n$, $\epsilon(n)$, and $\eta(n)$ so that a nonnegative cost function $J(n)$ is reduced successively

$$J(n+1) \leq J(n). \tag{5}$$

This will generally ensure that after every iteration, the adaptive filter improves its estimation of the parameters that we are trying to model.

A. Mean-Square Error

We define the cost function as the mean-square value of the estimation error, i.e., the MSE:

$$J(n) = E\left[|e(n)|^2\right] = E\left[e(n)e^*(n)\right]. \tag{6}$$

We opted for the MSE over other potential error measures, e.g., weighted least squares, because of the simplicity of the resulting algorithm. Note that in practical applications of adaptive filtering, the use of ensemble averaging is not feasible as we are adapting the filter in an on-line manner, based on a single realization of the estimation error, $e(n)$, as it evolves across iteration index n. Therefore, during the derivation of the proposed algorithm, we proceed by ignoring the expectation operation in the cost function (6) as is typical to the stochastic gradient descent method [34].

We apply the method of stochastic gradient descent for a sequential computation of the model parameters, using gradients of the performance surface in seeking its minimum. Even though only one of the estimated parameters, namely the channel impulse response $\mathbf{w}_n$, is complex-valued, then in the following derivation we also consider $\epsilon(n)$ and $\eta(n)$ to be complex-valued, as this will lay a clear consistent foundation for later carrying out the steady-state analysis of the adaptive filter. In order to accommodate for complex-valued $\epsilon(n)$ and $\eta(n)$, we use the real and imaginary part operators, $\Re\{z\}$ and $\Im\{z\}$, where appropriate.

We obtain the gradient vector at any point on the performance surface by differentiating the cost function (6) with respect to the model parameter estimates, resulting in

$$\nabla J(n) = \left[\frac{\partial J(n)}{\partial \mathbf{w}_{n-1}}, \frac{\partial J(n)}{\partial \epsilon(n-1)}, \frac{\partial J(n)}{\partial \eta(n-1)}\right], \tag{7}$$

where

$$\frac{\partial J(n)}{\partial \mathbf{w}_{n-1}} = -\left[\mathbf{y}_n e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}}\right]^* e(n), \tag{8a}$$

$$\frac{\partial J(n)}{\partial \epsilon(n-1)} = -\left[\mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}} j\right]^* e(n), \tag{8b}$$

$$\frac{\partial J(n)}{\partial \eta(n-1)} = -\left[\mathbf{y}'_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}}\right]^* e(n), \tag{8c}$$

and $\mathbf{y}'_n$ is the derivative of $\mathbf{y}_n$.

When using (8b) and (8c) in practice, we are only interested in the partial derivative of a complex function $e(n)$ with respect to the real part of the parameters $\epsilon(n)$ and $\eta(n)$. Therefore, we can simplify the partial derivatives relying on the Cauchy–Riemann equations [35] and consider only the real parts of the partial derivatives so that

$$\frac{\partial J(n)}{\partial \epsilon(n-1)} = -\Im\Big\{\Big[\mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}\Big]^* e(n)\Big\}, \quad (9b)$$

$$\frac{\partial J(n)}{\partial \eta(n-1)} = -\Re\Big\{\Big[\mathbf{y}'_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}\Big]^* e(n)\Big\}. \quad (9c)$$

B. Algorithm

We formulate the updating rules of the algorithm using the stochastic gradient in (7) by moving in the opposite direction of the gradient vector so that

$$\mathbf{w}_n = \mathbf{w}_{n-1} - \mu_w \frac{\partial J(n)}{\partial \mathbf{w}_{n-1}}, \quad (10a)$$

$$\epsilon(n) = \epsilon(n-1) - \mu_\epsilon \frac{\partial J(n)}{\partial \epsilon(n-1)}, \quad (10b)$$

$$\eta(n) = \eta(n-1) - \mu_\eta \frac{\partial J(n)}{\partial \eta(n-1)}, \quad (10c)$$

where $\mathbf{w}_0$, $\epsilon(0)$, and $\eta(0)$ are initial guesses and μ_w, μ_ϵ, and μ_η are fixed positive step size parameters that allow to control the convergence speed and steady-state performance of the algorithm. For computing the gradient vector at every iteration of the algorithm, (9b) and (9c) are to be used in (10b) and (10c). However, for carrying out the steady-state analysis, we will rely on the full complex-valued gradient and use (8b) and (8c) in (10b) and (10c); while (8a) is always used in (10a).

We also acknowledge that the partial derivative (9c) with regards to the sampling rate offset estimate $\eta(n-1)$ includes a time derivative of the resampled signal vector. If the third derivative of $\mathbf{y}_n$ exists, then it is beneficial to use the centered first-order divided difference, which has an approximation error of order two [36, p. 172], so that

$$\mathbf{y}'_n \mathbf{w}_{n-1} \approx \frac{(\mathbf{y}_{n+1} - \mathbf{y}_{n-1})\,\mathbf{w}_{n-1}}{2(1+\eta(n))}. \quad (11)$$

This is equivalent to considering $\mathbf{w}_{n-1}$ to be time-invariant and taking the centered first-order difference of $(\mathbf{y}_n \mathbf{w}_{n-1})'$. Alternatively, the first-order backward divided difference

$$\mathbf{y}'_n \mathbf{w}_{n-1} \approx \frac{(\mathbf{y}_n - \mathbf{y}_{n-1})\,\mathbf{w}_{n-1}}{1+\eta(n)} \quad (12)$$

can be used, which does not require computation of $\mathbf{y}_{n+1}$ nor the existence of the third derivative, but has an approximation error of order one.

To produce $\mathbf{y}_n$, the sampling rate of the know signal $\mathbf{x}_n$ needs to be converted. Various methods exist for arbitrary sampling rate conversion (SRC) [37], such as, e.g., the Lagrange interpolator [38], but the used SRC method can be selected independently of the proposed algorithm. If prior knowledge of the estimation parameters is available, then this knowledge may be used to speed up the start-up process of the algorithm. Otherwise, $\mathbf{w}_0$, $\epsilon(0)$, and $\eta(0)$ can be initialized to zero. Conclusively, the adaptive algorithm for iteratively estimating and tracking a wireless channel under carrier and sampling frequency offsets is listed as Algorithm 1 and illustrated in Fig. 2. It should be noted that in order for the algorithm to be able to handle sampling frequency offsets, several filter taps should be allocated, i.e., $M > 1$, even if the channel itself can be modeled by a single complex coefficient. Furthermore, in general there are several equivalent formulations for complex-valued adaptive filters [39, p. 69] and corresponding equivalent formulations exist also for the proposed algorithm. An open-source implementation of the algorithm is available as part of an adaptive filters toolkit.[1]

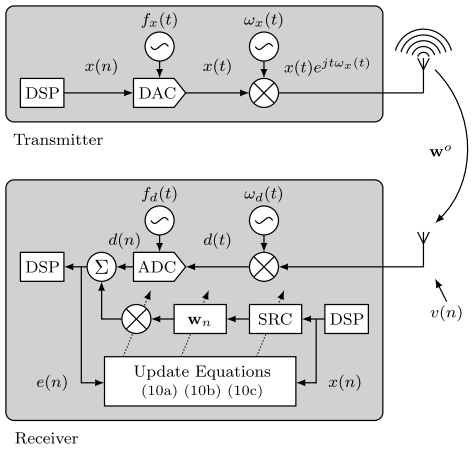


Fig. 2. System model with the proposed adaptive filter.

Algorithm 1: LMS-Type Frequency Offsets Tracking.

Procedure FO-LMS($x, d, \mu_w, \mu_\varepsilon, \mu_\eta, M$)
  $\mathbf{w}_0 \leftarrow \mathbf{0}_{1,M}$
  $\epsilon(0) \leftarrow 0, \eta(0) \leftarrow 0$
  $\phi(1) \leftarrow 0, t(1) \leftarrow 0$
  for $n \leftarrow 1$ to N **do**
    $\mathbf{y}_n \leftarrow [x(t(n)), x(t(n) - (1+\eta(n-1))), \ldots, x(t(n) - (M+1)(1+\eta(n-1)))]$
    $e(n) \leftarrow d(n) - \mathbf{y}_n \mathbf{w}_{n-1} e^{j\phi(n)}$
    $\mathbf{w}_n \leftarrow \mathbf{w}_{n-1} + \mu_w [\mathbf{y}_n e^{j\phi(n)}]^* e(n)$
    $\epsilon(n) \leftarrow \epsilon(n-1) + \mu_\epsilon \Im\{[\mathbf{y}_n \mathbf{w}_{n-1} e^{j\phi(n)}]^* e(n)\}$
    $\eta(n) \leftarrow \eta(n-1) + \mu_\eta \Re\{[\mathbf{y}'_n \mathbf{w}_{n-1} e^{j\phi(n)}]^* e(n)\}$
    $\phi(n+1) \leftarrow \phi(n) + \epsilon(n)$
    $t(n+1) \leftarrow t(n) + (1+\eta(n))$
  end for
end procedure

C. Computational Cost

A useful property of the proposed algorithm, mainly due to the chosen cost function, is its computational simplicity —

[1] https://github.com/karel/gr-adapt

each iteration of the algorithm requires only a limited number of straightforward calculations. Evaluation of the proposed algorithm requires $12\,M + 26$ real-valued multiplications and $14\,M + 13$ real-valued additions at each iteration. There can be various ways to perform specific calculations, but the resulting overall filter complexity will be of the same order of magnitude. However, these numbers do not include the arbitrary SRC, which can be implemented in several ways with varying complexity and accuracy. For example, Lagrange interpolation can be implemented with computational complexity growing linearly with the interpolation order [40].

D. Convergence Properties

For a given system with a fixed set of parameters, the choice of step sizes μ_w, μ_ϵ, and μ_η is effectively the only way to affect the performance of the algorithm. For example, in order to speed up the initial adaptation process, it might be desirable to use large step sizes, which minimize the instantaneous error at every iteration as much as possible, yet do not cause the algorithm to diverge. An approximate way of finding the upper bounds for the step sizes of an adaptive filter is by expanding the instantaneous output error by a Taylor series expansion [41], [39, p. 86], which in this case gives

$$e(n+1) = e(n) + \frac{\partial e(n)}{\partial \mathbf{w}_{n-1}}\Delta\mathbf{w}_{n-1} + \frac{\partial e(n)}{\partial \epsilon(n-1)}\Delta\epsilon(n-1) + \frac{\partial e(n)}{\partial \eta(n-1)}\Delta\eta(n-1) + h.o.t., \tag{13}$$

where $\Delta\mathbf{w}_{n-1}$, $\Delta\epsilon(n-1)$, and $\Delta\eta(n-1)$ are the estimate updates and $h.o.t.$ denotes the truncated higher-order terms of the expansion. From (10a), (10b), and (10c), by considering the full complex-valued gradient vector, we get

$$\Delta\mathbf{w}_{n-1} = \mu_w e(n)\left[\mathbf{y}_n e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}}\right]^*, \tag{14a}$$

$$\Delta\epsilon(n-1) = \mu_\epsilon e(n)\left[\mathbf{y}_n\mathbf{w}_{n-1}e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}}j\right]^*, \tag{14b}$$

$$\Delta\eta(n-1) = \mu_\eta e(n)\left[\mathbf{y}'_n\mathbf{w}_{n-1}e^{j\sum_{i=1}^{n}\Re\{\epsilon(i-1)\}}\right]^*, \tag{14c}$$

respectively. For sufficiently small $\Delta\mathbf{w}_n$, $\Delta\epsilon(n)$, and $\Delta\eta(n)$, the values of the higher-order terms in (13) can be neglected and, therefore, in the following analysis we approximate the expansion without them. Thus, evaluating the partial derivatives in (13) and substituting in (14a), (14b), and (14c) yields after direct simplification

$$e(n+1) \approx e(n)\cdot\left(1 - \mu_w\|\mathbf{y}_n\|^2 - \mu_\epsilon|\mathbf{y}_n\mathbf{w}_{n-1}|^2 - \mu_\eta|\mathbf{y}'_n\mathbf{w}_{n-1}|^2\right). \tag{15}$$

In order to ensure convergence, it is essential that the norm of the left hand side is not greater than that of the right hand side so that

$$|e(n+1)| \le |e(n)|\cdot\left|1 - \mu_w\|\mathbf{y}_n\|^2 - \mu_\epsilon|\mathbf{y}_n\mathbf{w}_{n-1}|^2 - \mu_\eta|\mathbf{y}'_n\mathbf{w}_{n-1}|^2\right|. \tag{16}$$

The goal in (16) is reached if the following relation holds:

$$|1 - \mu_w\|\mathbf{y}_n\|^2 - \mu_\epsilon|\mathbf{y}_n\mathbf{w}_{n-1}|^2 - \mu_\eta|\mathbf{y}'_n\mathbf{w}_{n-1}|^2| \le 1, \tag{17}$$

which in turn implies the following bounds on the choice of the step sizes μ_w, μ_ϵ, and μ_η:

$$0 < \mu_w \le \frac{2 - \mu_\epsilon|\mathbf{y}_n\mathbf{w}_{n-1}|^2 - \mu_\eta|\mathbf{y}'_n\mathbf{w}_{n-1}|^2}{\|\mathbf{y}_n\|^2}, \tag{18a}$$

$$0 < \mu_\epsilon \le \frac{2 - \mu_w\|\mathbf{y}_n\|^2 - \mu_\eta|\mathbf{y}'_n\mathbf{w}_{n-1}|^2}{|\mathbf{y}_n\mathbf{w}_{n-1}|^2}, \tag{18b}$$

$$0 < \mu_\eta \le \frac{2 - \mu_w\|\mathbf{y}_n\|^2 - \mu_\epsilon|\mathbf{y}_n\mathbf{w}_{n-1}|^2}{|\mathbf{y}'_n\mathbf{w}_{n-1}|^2}. \tag{18c}$$

However, the expressions above are merely necessary conditions for the stability of the proposed algorithm. The actual values of the step sizes to achieve stability are slightly smaller than the derived bounds due to the used approximation, i.e., discarding the higher-order terms in the error expansion.

We see that all quantities in (18) are positive, so the convergence properties depend on the slope but not on the sign of the gradient vector, and that the upper bounds are coupled, so the step sizes are to be selected collectively. That is, upper bound for each step size depends on the other two step sizes and convergence can be reached only if the relation in (17) is satisfied. The preceding analysis on the Taylor series expansion of the instantaneous error provides two results. Firstly, the step size bounds that are necessary but not sufficient conditions for the algorithm to converge and, secondly, these bounds can potentially be used to derive a normalized variant of the algorithm. As is, the adaptive filter assumes fixed step sizes, but an approach could also be developed that varies the step sizes to optimize convergence speed and subsequent steady-state performance.

E. Comparison

The application-specific methods for estimating a wireless channel and frequency offsets typically require the waveform to have a certain structure. The most general of those techniques aims to suppress known interference so as to provide physical layer security and relies on the waveform being cyclic with some period L [19]. Evaluation of that method for one cyclic block with length L requires $25\,L + 9$ real-valued multiplications, $18\,L - 1$ real-valued additions, $L + 1$ real-valued divisions, evaluating atan2() $L + 1$ times, and calculating the L-point discrete Fourier transform at least once. This puts the referenced and proposed methods roughly on par in terms of computational complexity for a single data point. However, due to its block-based nature, the reference method can take advantage of parallel processing. Also, methods that rely on features built into the waveform generally require fewer samples than the proposed algorithm to provide accurate parameter estimates. Then again, the repetitive waveform structure required by the reference method could be a vulnerability in physical layer security applications.

IV. Steady-State Analysis

An important performance measure of an adaptive filter, which is typically used in the literature, is its steady-state excess mean-square error (EMSE) [35]. In this section, we will carry out the derivation to express the total EMSE in terms of three EMSEs, each related to an update equation in (10). The analysis developed in this section relies on energy conservation arguments [33] and on decoupling the errors of separate update equations by solving a system of linear equations [42]. In order to accommodate the errors accumulated by the frequency offset update equations, we extend the existing methodology to account for what we will refer to as the self-induced nonstationarity. Furthermore, to make the analysis tractable, we omit the time-varying terms $\phi(n)$ and $\beta(n)$ of the system model here. That is, the focus is on steady-state analysis rather than tracking analysis, considering a quasi-static channel.

A. Self-Induced Nonstationarity

In practice, the frequency offset estimates $\epsilon(n)$ and $\eta(n)$ are bound to differ from the actual parameters ϵ^o and η^o, resulting in estimation errors $\tilde{\epsilon}(n) = \epsilon^o - \epsilon(n)$ and $\tilde{\eta}(n) = \eta^o - \eta(n)$. This is especially so during the start-up phase of the algorithm but also during the steady state, as gradient noise affects the estimates at each iteration. Therefore, the accumulating estimation errors $\sum_{i=1}^{n} \tilde{\epsilon}(i-1)$ and $\sum_{i=1}^{n} \tilde{\eta}(i-1)$ inevitably cause a phase shift and fractional time delay, or self-induced nonstationarity, which the channel estimate $\mathbf{w}_n$ will then try to compensate for. In order to proceed with the steady-state analysis, we first need a way to express how those accumulated estimation errors affect the channel update equation (10a).

Based on (3), we define the total a priori error as

$$e_a(n) = \mathbf{y}_n^o \mathbf{w}^o e^{j\sum_{i=1}^{n}\epsilon^o} - \mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{19}$$

which is simply the error between the received signal and the estimated signal but discarding the noise term $v(n)$. By shifting both sides of the a priori error equation in phase by $-\sum_{i=1}^{n}\epsilon(i-1)$ and in time by $-\sum_{i=1}^{n}\eta(i-1)$, we get

$$e_a^s(n) = \mathbf{x}_n \mathbf{T}_n \mathbf{w}^o e^{j\sum_{i=1}^{n}\tilde{\epsilon}(i-1)} - \mathbf{x}_n \mathbf{w}_{n-1}, \tag{20}$$

where, for notational simplicity, we have denoted the phase and time shifted a priori error as

$$e_a^s(n) \triangleq e_a\left(n - \sum_{i=1}^{n}\eta(i-1)\right) e^{-j\sum_{i=1}^{n}\epsilon(i-1)} \tag{21}$$

and $\mathbf{T}_n$ is an arbitrary time-shift matrix of size $M \times M$ that, when multiplying with $\mathbf{x}_n$, delays the signal $\mathbf{x}_n$ by $\sum_{i=1}^{n}\tilde{\eta}(i-1)$. From (20), we can define $\mathbf{w}_n^o$ as

$$\mathbf{w}_n^o \triangleq \mathbf{T}_n \mathbf{w}^o e^{j\sum_{i=1}^{n}\tilde{\epsilon}(i-1)}. \tag{22}$$

In order to proceed, we call on the following assumption.

A.1: At the steady state, as $n \to \infty$, the instantaneous estimation errors $\tilde{\epsilon}(n)$ and $\tilde{\eta}(n)$ satisfy the conditions

$$\tilde{\epsilon}(n) \ll 1 \qquad \text{and} \qquad \tilde{\eta}(n) \ll \frac{1}{f_{max}},$$

where f_{max} is the maximum frequency component of $\mathbf{x}_n$.

This is a reasonable assumption because in steady state we expect the estimation errors to vary around zero. Relying on A.1, we can use linear approximation [43] to write (20) as

$$\begin{aligned} e_a^s(n) \approx{}& \left[\mathbf{x}_n \mathbf{T}_{n-1} + (\mathbf{x}_n' \mathbf{T}_{n-1}) \circ \tilde{\boldsymbol{\eta}}_{n-1}\right] \mathbf{w}^o \\ &\cdot \left[e^{j\sum_{i=1}^{n-1}\tilde{\epsilon}(i-1)} + e^{j\sum_{i=1}^{n-1}\tilde{\epsilon}(i-1)} j\tilde{\epsilon}(n-1)\right] - \mathbf{x}_n \mathbf{w}_{n-1}, \end{aligned} \tag{23}$$

where $\circ$ denotes the Hadamard product, i.e., element-wise multiplication, and $\tilde{\boldsymbol{\eta}}_n$ is the row vector

$$\tilde{\boldsymbol{\eta}}_n = [\tilde{\eta}(n-M+1), \ldots, \tilde{\eta}(n-1)].$$

By expanding (23), and ignoring the cross-terms that include both $\tilde{\epsilon}(n-1)$ and $\tilde{\eta}(n-1)$, as they are very small under A.1, (23) can be rewritten as

$$\begin{aligned} e_a^s(n) \approx{}& \mathbf{x}_n \mathbf{T}_{n-1} \mathbf{w}^o e^{j\sum_{i=1}^{n-1}\tilde{\epsilon}(i-1)} \\ &+ \mathbf{x}_n \mathbf{T}_{n-1} \mathbf{w}^o e^{j\sum_{i=1}^{n-1}\tilde{\epsilon}(i-1)} j\tilde{\epsilon}(n-1) \\ &+ \mathbf{x}_n' \mathbf{T}_{n-1} \mathbf{w}^o e^{j\sum_{i=1}^{n-1}\tilde{\epsilon}(i-1)} \tilde{\eta}(n-1) - \mathbf{x}_n \mathbf{w}_{n-1}, \end{aligned} \tag{24}$$

which, by substituting in (22) for index $n-1$, is simply

$$\begin{aligned} e_a^s(n) \approx{}& \mathbf{x}_n \mathbf{w}_{n-1}^o + \mathbf{x}_n \mathbf{w}_{n-1}^o j\tilde{\epsilon}(n-1) \\ &+ \mathbf{x}_n' \mathbf{w}_{n-1}^o \tilde{\eta}(n-1) - \mathbf{x}_n \mathbf{w}_{n-1}. \end{aligned} \tag{25}$$

Finally, taking $\tilde{\mathbf{w}}_n = \mathbf{w}_n^o - \mathbf{w}_n$ to be the estimation error of the channel and reversing the phase and time shift introduced in (20), the a priori error can be expressed as

$$\begin{aligned} e_a^n(n) \approx{}& \mathbf{y}_n \tilde{\mathbf{w}}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)} \\ &+ \mathbf{y}_n \mathbf{w}_{n-1}^o j\tilde{\epsilon}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)} \\ &+ \mathbf{y}_n' \mathbf{w}_{n-1}^o \tilde{\eta}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)} \end{aligned} \tag{26}$$

and we denote the three terms on the right-hand side as the a priori errors of the three update equations so that

$$e_{w,a}^n(n) = \mathbf{y}_n \tilde{\mathbf{w}}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{27a}$$

$$e_{\epsilon,a}^n(n) = \mathbf{y}_n \mathbf{w}_{n-1}^o j\tilde{\epsilon}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{27b}$$

$$e_{\eta,a}^n(n) = \mathbf{y}_n' \mathbf{w}_{n-1}^o \tilde{\eta}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{27c}$$

where the superscript ^{n} denotes this first set of definitions for the a priori errors.

B. Mean-Square Performance

Following the well-known energy conservation relation method [28], we also define the following second set of a priori errors

$$e_{w,a}(n) = \mathbf{y}_n (\mathbf{w}_n^o - \mathbf{w}_{n-1}) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{28a}$$

$$e_{\epsilon,a}(n) = \mathbf{y}_n \mathbf{w}_{n-1} \tilde{\epsilon}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{28b}$$

$$e_{\eta,a}(n) = \mathbf{y}_n' \mathbf{w}_{n-1} \tilde{\eta}(n-1) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{28c}$$

so that the total error $e(n)$ is the sum of the a priori errors and the measurement noise

$$e(n) = e_{w,a}(n) + e_{\epsilon,a}(n) + e_{\eta,a}(n) + v(n). \tag{29}$$

Similarly, we define the a posteriori errors

$$e_{w,p}(n) = \mathbf{y}_n \tilde{\mathbf{w}}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{30a}$$

$$e_{\epsilon,p}(n) = \mathbf{y}_n \mathbf{w}_n \tilde{\epsilon}(n) e^{j\sum_{i=1}^{n}\epsilon(i-1)}, \tag{30b}$$

$$e_{\eta,p}(n) = \mathbf{y}'_n \mathbf{w}_n \tilde{\eta}(n) e^{j\sum_{i=1}^{n}\epsilon(i-1)}. \tag{30c}$$

A.2: The noise sequence $v(n)$ is stationary, with variance σ_v^2, and statistically independent of the a priori errors $e_{w,a}(n)$, $e_{\epsilon,a}(n)$, and $e_{\eta,a}(n)$.

Under the above justifiable assumption, we find that the MSE is equivalently given by

$$MSE = \zeta + \sigma_v^2 = \zeta^w + \zeta^\epsilon + \zeta^\eta + \sigma_v^2, \tag{31}$$

where

$$\zeta^w = \lim_{n\to\infty} E\left[|e_{w,a}(n)|^2\right], \tag{32a}$$

$$\zeta^\epsilon = \lim_{n\to\infty} E\left[|e_{\epsilon,a}(n)|^2\right], \tag{32b}$$

$$\zeta^\eta = \lim_{n\to\infty} E\left[|e_{\eta,a}(n)|^2\right]. \tag{32c}$$

Employing the energy conservation relation method and relying on the two sets of a priori errors, it is shown in the Appendix that the following equations hold:

$$\begin{aligned}&\mu_w E\left[\|\mathbf{y}_n\|^2|e_{w,a}(n)|^2\right] + \mu_w E\left[\|\mathbf{y}_n\|^2|e_{\epsilon,a}(n)|^2\right]\\ &\quad + \mu_w E\left[\|\mathbf{y}_n\|^2|e_{\eta,a}(n)|^2\right] + \mu_w E\left[\|\mathbf{y}_n\|^2|v(n)|^2\right]\\ &\quad + E\left[\frac{M}{\mu_w\|\mathbf{y}_n\|^2}|e^n_{\epsilon,a}(n)|^2\right] + E\left[\frac{M}{\mu_w\|\mathbf{y}_n\|^2}|e^n_{\eta,a}(n)|^2\right]\\ &= 2E\left[|e_{w,a}(n)|^2\right],\end{aligned} \tag{33a}$$

$$\begin{aligned}&\mu_\epsilon E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2|e_{w,a}(n)|^2\right] + \mu_\epsilon E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2|e_{\epsilon,a}(n)|^2\right]\\ &\quad + \mu_\epsilon E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2|e_{\eta,a}(n)|^2\right] + \mu_\epsilon E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2|v(n)|^2\right]\\ &= 2E\left[|e_{\epsilon,a}(n)|^2\right],\end{aligned} \tag{33b}$$

$$\begin{aligned}&\mu_\eta E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2|e_{w,a}(n)|^2\right] + \mu_\eta E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2|e_{\epsilon,a}(n)|^2\right]\\ &\quad + \mu_\eta E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2|e_{\eta,a}(n)|^2\right] + \mu_\eta E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2|v(n)|^2\right]\\ &= 2E\left[|e_{\eta,a}(n)|^2\right].\end{aligned} \tag{33c}$$

This system of equations can now be solved for the EMSEs ζ^w, ζ^ϵ, and ζ^η. To do so, we consider the following two cases.

1) Using Separation Principle: One way to solve the equations in (33) is by imposing the following assumption.

A.3: In steady state, $\|\mathbf{y}_n\|^2$, $|\mathbf{y}_n\mathbf{w}_{n-1}|^2$, and $|\mathbf{y}'_n\mathbf{w}_{n-1}|^2$ are statistically independent of $|e_{w,a}|^2$, $|e_{\epsilon,a}(n)|^2$, and $|e_{\eta,a}(n)|^2$.

This assumption is reasonable at the steady state since the behavior of the a priori errors is less likely to be sensitive to the input data. It is similar to the separation principle assumption made in, e.g., [33], [42], and allows us to write

$$E\left[\|\mathbf{y}_n\|^2|e_{w,a}(n)|^2\right] = E\left[\|\mathbf{y}_n\|^2\right] E\left[|e_{w,a}(n)|^2\right],$$

$$E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2|e_{\epsilon,a}(n)|^2\right] = E\left[|\mathbf{y}_n\mathbf{w}_{n-1}|^2\right] E\left[|e_{\epsilon,a}(n)|^2\right],$$

$$E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2|e_{\eta,a}(n)|^2\right] = E\left[|\mathbf{y}'_n\mathbf{w}_{n-1}|^2\right] E\left[|e_{\eta,a}(n)|^2\right].$$

Furthermore, we make the following assumptions.

A.4: In steady state for a static channel, as $n\to\infty$, the channel estimate is close to the actual channel $\mathbf{w}_{n-1}\to\mathbf{w}^o$.

A.5: In steady state, for sufficiently small η^o, the following equalities hold: $\|\mathbf{y}_n\|^2 = \|\mathbf{x}_n\|^2$, $|\mathbf{y}_n\mathbf{w}_{n-1}|^2 = |\mathbf{x}_n\mathbf{w}^o|^2$ and $|\mathbf{y}'_n\mathbf{w}_{n-1}|^2 = |\mathbf{x}'_n\mathbf{w}^o|^2$.

A.6: In steady state, the two sets of a priori errors are equivalent, i.e., $E|e^n_{w,a}(n)|^2 = E|e_{w,a}(n)|^2$, $E|e^n_{\epsilon,a}(n)|^2 = E|e_{\epsilon,a}(n)|^2$, $E|e^n_{\eta,a}(n)|^2 = E|e_{\eta,a}(n)|^2$.

Using the assumptions A.3 through A.6, and solving (33) for ζ^w, ζ^ϵ, and ζ^η, we obtain the following expressions for the EMSEs of the proposed algorithm:

$$\boxed{\begin{aligned}\zeta^w &= \frac{2\mu_w \operatorname{Tr}(\mathbf{R})\sigma_v^2}{\gamma}\\ &\quad + \frac{M\frac{\mu_\epsilon \operatorname{Tr}(\mathbf{RQ})}{\mu_w \operatorname{Tr}(\mathbf{R})}\sigma_v^2 + M\frac{\mu_\eta \operatorname{Tr}(\mathbf{PQ})}{\mu_w \operatorname{Tr}(\mathbf{R})}\sigma_v^2}{\gamma},\\ \zeta^\epsilon &= \frac{2\mu_\epsilon \operatorname{Tr}(\mathbf{RQ})\sigma_v^2}{\gamma},\\ \zeta^\eta &= \frac{2\mu_\eta \operatorname{Tr}(\mathbf{PQ})\sigma_v^2}{\gamma},\end{aligned}} \tag{35a, 35b, 35c}$$

where the denominator γ is

$$\begin{aligned}\gamma &= 4 - 2\mu_w \operatorname{Tr}(\mathbf{R}) - 2\mu_\epsilon \operatorname{Tr}(\mathbf{RQ}) - 2\mu_\eta \operatorname{Tr}(\mathbf{PQ})\\ &\quad - M\frac{\mu_\epsilon \operatorname{Tr}(\mathbf{RQ})}{\mu_w \operatorname{Tr}(\mathbf{R})} - M\frac{\mu_\eta \operatorname{Tr}(\mathbf{PQ})}{\mu_w \operatorname{Tr}(\mathbf{R})}\end{aligned} \tag{36}$$

and $\mathbf{R}$ is the covariance matrix $\mathbf{R} = E[\mathbf{x}_n^*\mathbf{x}_n]$, $\mathbf{P}$ is the covariance matrix $\mathbf{P} = E[(\mathbf{x}'_n)^*\mathbf{x}'_n]$, and $\mathbf{Q} = \mathbf{w}^o(\mathbf{w}^o)^*$.

Note that, in order for the algorithm to remain stable, the denominator of the EMSEs needs to be positive. If we consider an approximation of the denominator without the self-induced nonstationarity terms, i.e., the last two terms in (36), then this result has an equivalent implication to that of the simple approximation (18), which we derived using the Taylor series expansion of the instantaneous error.

2) Assuming Gaussian White Input Signals: For Gaussian white input signals (with $\mathbf{R} = \sigma_x^2\mathbf{I}$), relying on A.4 and A.5, (33) can be more accurately solved by resorting to the following independence assumption.

A.7: At steady state, the estimation errors $\tilde{\mathbf{w}}_n$, $\tilde{\epsilon}(n)$, and $\tilde{\eta}(n)$ are all statistically independent of $\mathbf{x}_n$, $\mathbf{x}_n\mathbf{w}^o$, and $\mathbf{x}'_n\mathbf{w}^o$.

This is an extension of the assumption, which is widely used for analysing the performance of adaptive filters [33]. Relying on the independence assumption A.7 and following the same reasoning that is used for analysing the steady-state performance of the LMS adaptive filter [35, p. 296], it can be verified that

$$E\left[\|\mathbf{x}_n\|^2|e_{k,a}(n)|^2\right] = (M+1)\sigma_x^2\zeta^k, \tag{37a}$$

$$E\left[|\mathbf{x}_n\mathbf{w}^o|^2|e_{k,a}(n)|^2\right] = \left(1+\frac{1}{M}\right)\sigma_x^2\|\mathbf{w}^o\|^2\zeta^k, \tag{37b}$$

$$E\left[|\mathbf{x}'_n\mathbf{w}^o|^2|e_{k,a}(n)|^2\right] \approx \left(2+\frac{2}{M}\right)\sigma_x^2\|\mathbf{w}^o\|^2\zeta^k, \tag{37c}$$

where k is either w, ϵ, or η, and we have used that

$$\sigma_{x'}^2 = \frac{\sigma_{x(n)}^2 + \sigma_{x(n-1)}^2}{(\Delta n)^2} = 2\sigma_x^2,$$

where we are first relying on the independence of successive samples of $x(n)$ and consequently on the samples being identically distributed as well. The last equation in (37) does not hold precisely but is an approximation, because the derivative itself is not identically and independently distributed. Still, for a channel $\mathbf{w}^o$ with a relatively flat frequency response, this approximation can be practical, as will be seen in the results section. Using A.4, A.5, A.7, and solving (33) for ζ^w, ζ^ϵ, and ζ^η, we obtain

$$\zeta^w = \frac{2\mu_w M\sigma_x^2\sigma_v^2}{\gamma} + \frac{\frac{\mu_\epsilon}{\mu_w M}\|\mathbf{w}^o\|^2\sigma_v^2 + \frac{\mu_\eta}{\mu_w M}2\|\mathbf{w}^o\|^2\sigma_v^2}{\gamma}, \tag{38a}$$

$$\zeta^\epsilon = \frac{2\mu_\epsilon\sigma_x^2\|\mathbf{w}^o\|^2\sigma_v^2}{\gamma}, \tag{38b}$$

$$\zeta^\eta = \frac{4\mu_\eta\sigma_x^2\|\mathbf{w}^o\|^2\sigma_v^2}{\gamma}, \tag{38c}$$

where the denominator γ is the same for all equations:

$$\begin{aligned}\gamma = 4 &- 2\mu_w(M+1)\sigma_x^2 \\ &- 2\mu_\epsilon\left(1+\frac{1}{M}\right)\sigma_x^2\|\mathbf{w}^o\|^2 - \frac{\mu_\epsilon}{\mu_w}\left(1+\frac{1}{M}\right)\|\mathbf{w}^o\|^2 \\ &- 4\mu_\eta\left(1+\frac{1}{M}\right)\sigma_x^2\|\mathbf{w}^o\|^2 - 2\frac{\mu_\eta}{\mu_w}\left(1+\frac{1}{M}\right)\|\mathbf{w}^o\|^2.\end{aligned} \tag{39}$$

V. Numerical Results

In order to verify the theoretical steady-state MSE expressions and evaluate the performance of the proposed algorithm, the theoretical results are herein first compared to steady-state simulations, where the channel and frequency offsets are assumed to be known to the algorithm and time-varying terms are omitted, and then time-varying simulations together with proof-of-concept RF measurements are presented.

A. Steady-State Results

In Fig. 3, the steady-state theoretical MSEs obtained from expressions (35) and (38) are compared with the MSE observed in simulations. The simulations are run with different channel weight vectors $\mathbf{w}^o$, each of length $M = 3$ with a rather flat frequency response. The input signal $\mathbf{x}_n$ is Gaussian of unit variance and the noise $v(n)$ is Gaussian with variance $\sigma_v^2 = 10^{-3}$. From here on out, in order to make the results relatable, we refer to the sampling frequency offset as $\Delta f = f_d - f_x$ instead of η^o. The simulated frequency offsets are $\epsilon^o = 6\,\mathrm{kHz}$ and $\Delta f = 5\,\mathrm{Hz}$, which, considering a carrier frequency of $2.4\,\mathrm{GHz}$ and sampling frequency of $2\,\mathrm{MHz}$, is equivalent to a $2.5\,\mathrm{ppm}$ oscillator inaccuracy. Note that the MSE expressions do not depend on the frequency offset values, since the offsets themselves inherently do not affect the energy conservation relation. This is in alignment with our extensive simulation results for practical ranges of ϵ^o and Δf (that are not shown herein), as steady-state MSE is indifferent w.r.t. the offset values. Thus, the simulated results are only plotted for these two example frequency offsets.

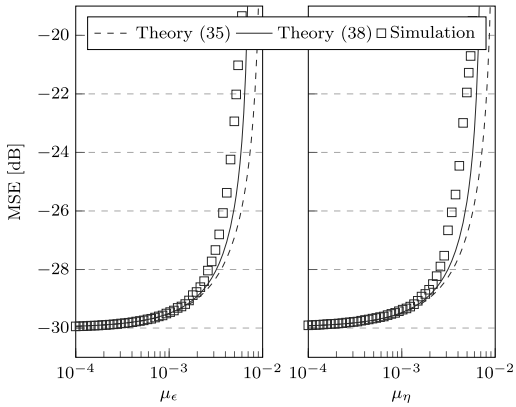


Fig. 3. Simulated and theoretical MSE curves relying on the separation principle and Gaussian input versus μ_ϵ for $\mu_w = 0.0025$ and $\mu_\eta = 0$ on the left and versus μ_η for $\mu_w = 0.005$ and $\mu_\epsilon = 0$ on the right.

Each simulation result is the steady-state statistical average of 1024 runs, with 5000 iterations in each run. The average of the last 2500 entries of the ensemble-average curve is then used as the simulated MSE value. Oversampling is used to prevent interpolation errors from skewing the simulation results. In Fig. 3, the analysis focuses separately on either frequency offset estimation combined with the channel estimation. The comparison shows that both expressions are in good match with simulation results at small values of μ_ϵ and μ_η. However, (38) gives a better match with the simulation results for larger μ_ϵ and μ_η values, which supports the use of A.7.

Figs. 4 and 5 compare the theoretical MSE obtained from (38) with the simulated MSE for various μ_w over a range of μ_ϵ or μ_η. Again, the results show a good match between theoretical and simulated results, especially at smaller step size values, when the steady-state assumptions are better justified. However, in general the sampling frequency offset update equation is not well suited for operating with disproportionally selected step sizes — carrier frequency offset can usually be recovered, but if the signals become unaligned in time because of persisting large estimation errors in sampling frequency offset, then this can be difficult to recover from.

Furthermore, Figs. 4 and 5 also illustrate the relevance of the the step sizes' upper bound (18). For visual clarity, only a single upper bound is calculated and plotted by taking the two step sizes, which are varied, to be equal in (18). As the step sizes approach the upper bound, performance of the filter deteriorates, and, since the filter leaves the steady state, the match between theoretical and simulated MSE results also declines. Finally, Fig. 6 presents a comparison of the theoretical and

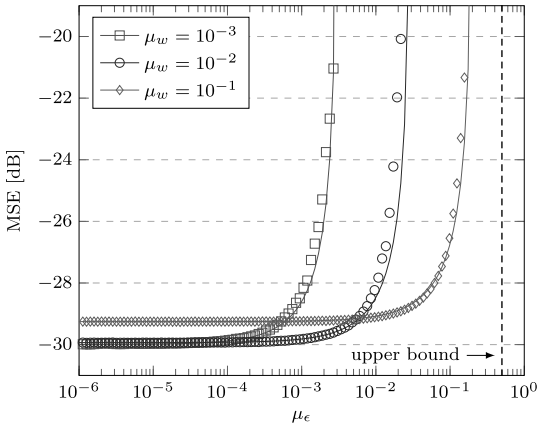


Fig. 4. Simulated (only markers) and theoretical (solid lines) MSE curves at various μ_w versus μ_ϵ for $\mu_\eta = 0$. The dashed vertical line indicates the upper bound for the two step sizes when $\mu_w = \mu_\epsilon$.

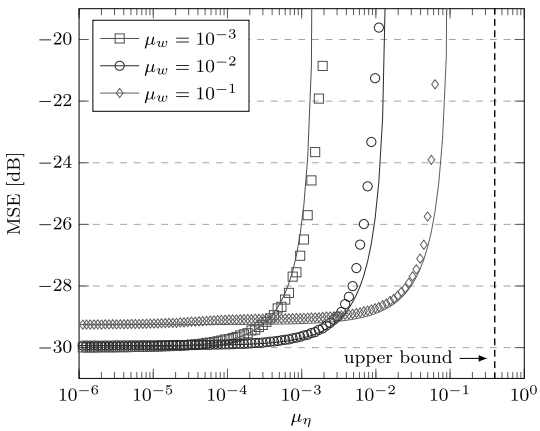


Fig. 5. Simulated (only markers) and theoretical (solid lines) MSE curves at various μ_w versus μ_η for $\mu_\epsilon = 0$. The dashed vertical line indicates the upper bound for the two step sizes when $\mu_w = \mu_\eta$.

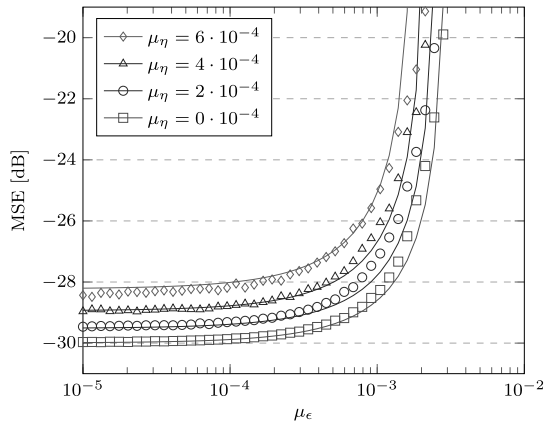


Fig. 6. Simulated (only markers) and theoretical (solid lines) MSE curves at various μ_ϵ versus μ_η for $\mu_w = 10^{-3}$.

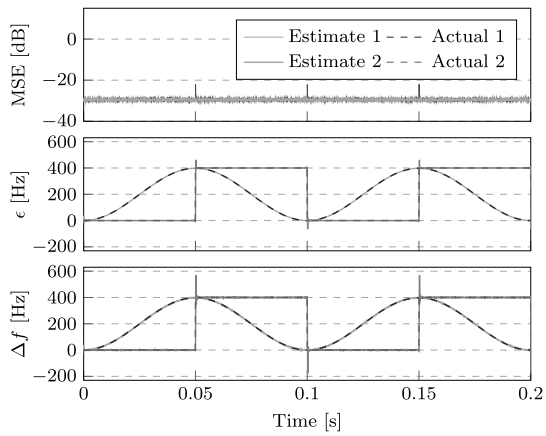


Fig. 7. Simulated results illustrating the filter's ability to track time-varying frequency offsets at step sizes $\mu_w = 10^{-3}$, $\mu_\epsilon = 10^{-6}$, and $\mu_\eta = 10^{-6}$.

simulated MSEs of the proposed algorithm when all of the system parameters are simultaneously estimated. As shown by all the foregoing numerical results in Figs. 3–6, the theoretical results match very well with the simulations.

B. Time-Varying Results

In this subsection, using simulations, we analyze the performance of the proposed filter when the frequency offsets are time-varying, i.e., we focus on the effect of $\phi(n)$ and $\beta(n)$ on the algorithm's performance. Fig. 7 illustrates the filter's ability to track long-term changes in the time-varying terms. The simulations are started with perfect knowledge about the initial state of the channel and with zero frequency offsets. Then both frequency offsets are varied over time either gradually or abruptly as shown in Fig. 7 with the dashed lines. Other simulation parameters are kept the same as previously, including the ensemble averaging. The simulation results indicate that the adaptive filter is able to track those changes, regardless of whether the parameters change gradually or abruptly. As a result, the MSE is stable over time, except for a brief readjustment period during the abrupt frequency offset changes, which is expected.

In contrast, Fig. 8 demonstrates the filter's tracking performance under short-term changes, i.e., phase noise and sampling time jitter. Both are modelled as first-order autoregressive processes with the process parameters α_ϕ and α_β close to one and the variances being σ_ϕ^2 and σ_β^2 (the exact values of which are given in Fig. 8). The algorithm is run for 10^6 iterations and, again, the simulations are started with perfect knowledge of the initial state of the channel, yet without knowledge about

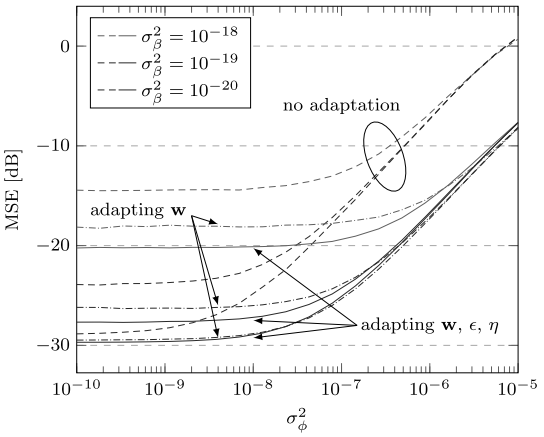


Fig. 8. Simulated performance for various sampling jitter and phase noise variances when $\epsilon^o = 0$ and $\eta^o = 0$ at step sizes $\mu_w = 0$, $\mu_\epsilon = 0$, and $\mu_\eta = 0$ (dashed lines), $\mu_w = 10^{-3}$, $\mu_\epsilon = 0$, and $\mu_\eta = 0$ (dash dotted lines), and $\mu_w = 10^{-3}$, $\mu_\epsilon = 10^{-5}$, and $\mu_\eta = 10^{-5}$ (solid lines).

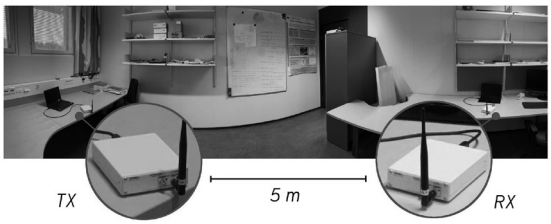


Fig. 9. Experiment setup in an office room with two USRP-2900s.

the noise processes. The simulations illustrate three cases: no adaptation at all, adaptation of only the channel estimate $\mathbf{w}_n$, and adaptation of all the parameters. The case without adaptation serves as a baseline for the MSE performance in the given noisy circumstances, while the other cases illustrate the benefits of adapting the channel and frequency offset estimates. The results show that, even though excessive phase noise and sampling jitter can degrade the algorithm's performance, adapting all the parameters still has a clear benefit compared to limited or no adaptation.

C. Experimental Results

The experiment is carried out indoors using two USRP-2900 software-defined radios with dipole antennas. The radios have internal temperature-compensated crystal oscillators with frequency accuracy of couple parts per million, presenting a fair scenario for analyzing the algorithm. The radios are positioned in the opposite corners of an office room with about five meters line-of-sight distance between them as shown in Fig. 9. As such, the experimental setup is static, with only the inherent oscillator drifts contributing a slowly time-varying component. The measurements are done in a relatively quiet section of the $2.4\,\mathrm{GHz}$ ISM frequency band, so that signals from other wireless devices

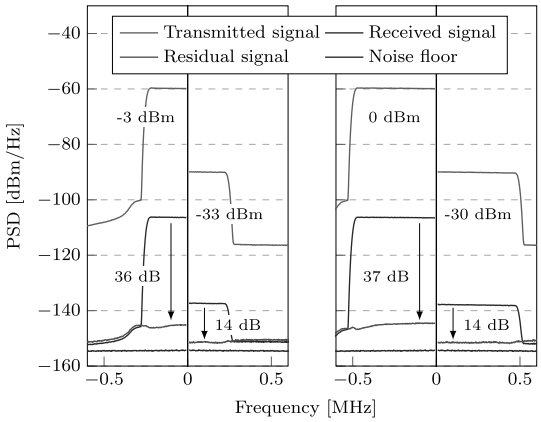


Fig. 10. Power spectral densities of the transmitted, received, and residual signals along with the noise floor at the receiver in steady state, i.e., discarding the start-up phase of the algorithm.

do not affect the measurements, and using a sampling rate of $2\,\mathrm{MHz}$. The transmitter broadcasts a bandlimited Gaussian noise signal, which is known to the receiver entirely. As such, the experiment illustrates the known-interference cancellation scenario, where the residual error signal could contain a signal of interest. Two signals bandwidths, $1\,\mathrm{MHz}$ and $0.5\,\mathrm{MHz}$, are used with transmit powers -60 dBm/Hz or -90 dBm/Hz. The receiving node receives the bandlimited noise signal over the air and records it. The algorithm is then run offline on the recordings.

Length of the estimated channel vector $\mathbf{w}_n$ is taken to be $M = 9$, which is more than sufficient for this scenario, and all of the estimated parameters are initialized to zero. For the algorithm to converge, it is required that the known and received signal streams be coarsely aligned in time (i.e., the difference in the two streams' starts may not exceed $M - 1$ samples). That coarse alignment is provided by onset detection — comparing the received signal's energy to a threshold. Fig. 10 shows the measured signal spectra at different stages of the system model. It can be observed that suppression of the known interference is not significantly affected by its bandwidth. Furthermore, when the received known interference is substantially above the noise floor then the MSE, i.e., the residual signal, is much higher than the measurement noise floor. This is caused by the nonlinearities induced in the USRP-2900 RF front-ends, which the algorithm does not account for. When the received known interference is not so powerful, those nonlinearities do not affect cancellation. Based on measurements at other received known-interference power levels that are omitted for brevity, in this scenario the algorithm requires that the signal be at least $4\,\mathrm{dB}$ above the noise floor in order to provide stable parameter estimates.

Finally, Fig. 11 demonstrates the algorithm's performance for the purpose of known-interference cancellation while estimating and tracking the channel together with the frequency offsets (Residual 2 and 3) as opposed to estimating and tracking the channel without compensating for the frequency offsets (Residual 1). It is evident that explicit adaptation of frequency

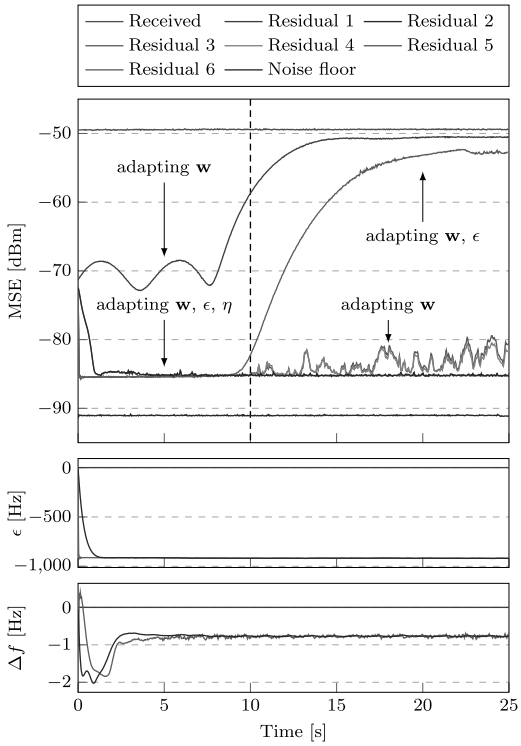


Fig. 11. Proposed algorithm's MSE progression in time for the 0.5 MHz −60 dBm/Hz signal. Residual 1 is without frequency offset compensation ($\mu_\epsilon = 0$ and $\mu_\eta = 0$); Residual 2 uses larger step sizes for frequency offset updates ($\mu_\epsilon = 5 \cdot 10^{-5}$ & $\mu_\eta = 5 \cdot 10^{-5}$) and Residual 3 uses smaller step sizes ($\mu_\epsilon = 2 \cdot 10^{-6}$ & $\mu_\eta = 2 \cdot 10^{-6}$); Residual 4 and 5 supplement cases 2 and 3, as the frequency offset estimations are stopped after 10 s. Residual 6 illustrates the situation without sampling frequency offset compensation.

offsets gives better short-term and long-term performance. The results also show how continuous frequency offsets tracking is necessary in practice (Residual 4, 5 and 6), due to their time-varying nature. Again, it is clear that the experimental MSE does not reach the noise floor, as excessive phase noise, sampling time jitter, and nonlinear distortions degrade the performance of the algorithm. Nevertheless, the experimental results demonstrate the efficiency of the proposed algorithm in estimating and compensating for time-varying carrier and sampling frequency offsets of an unknown channel.

We compared the proposed algorithm to the method in [19] using a separate set of measurements with a cyclic bandlimited Gaussian noise waveform having period L. The two algorithms achieved a similar level of MSE eventually as long as the period L was chosen so that the carrier frequency offset remained within the reference algorithm's estimation range. As such, only the proposed algorithm's results are presented in the figures for brevity. The reference algorithm does have an advantage over the proposed algorithm in that it provides estimates of the channel and frequency offsets quicker. However, this advantage of the reference method relies on the assumptions that the used waveform is cyclic with period L and the combination of period L and sampling rate is appropriate for the frequency offsets. The latter of which significantly limits the acceptable range of L. The proposed algorithm, however, is not limited to cyclic waveforms and, as such, is also free from the related estimation range and accuracy limitations.

VI. Conclusion

This article proposed an adaptive filter for jointly and explicitly estimating the channel impulse response, carrier frequency offset, and sampling frequency offset between a transmitter and receiver pair. The proposed algorithm relies on the stochastic gradient descent method minimizing the mean-square error and is therefore computationally simple, yet effective. Compared to existing methods, the proposed adaptive filter facilitates estimating the channel and frequency offsets without requirements on the used waveform. Stability and convergence of the algorithm depend on the proper selection of step sizes in relation to the other system parameters. Hence, upper bounds for the step sizes were derived and presented. Furthermore, this article also provides a theoretical steady-state analysis of the proposed adaptive filter. Novel expressions for the excess mean-square error were derived by extending the energy conservation relation to account for the self-induced nonstationarity inherent in the proposed adaptive filter. Validity of the theoretical expressions was corroborated through comparison to simulations. Also, simulation results were presented for time-varying and noisy frequency offsets. Finally, the algorithm was validated on measurement data.

Appendix

The following analysis extends the energy conservation relation [33], which is established by expressing the update equations in (10) in terms of the estimation errors $\tilde{\mathbf{w}}_n$, $\tilde{\epsilon}(n)$, and $\tilde{\eta}(n)$. Subtracting both sides of (10a) from $\mathbf{w}_n^o$, both sides of (10b) from ϵ^o, and both sides of (10c) from η^o, we get

$$\tilde{\mathbf{w}}_n = \mathbf{w}_n^o - \mathbf{w}_{n-1} - \mu_w \left[\mathbf{y}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)}\right]^* e(n), \quad (40a)$$

$$\tilde{\epsilon}(n) = \tilde{\epsilon}(n-1) - \mu_\epsilon \left[\mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)} j\right]^* e(n), \quad (40b)$$

$$\tilde{\eta}(n) = \tilde{\eta}(n-1) - \mu_\eta \left[\mathbf{y}'_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}\right]^* e(n). \quad (40c)$$

Furthermore, by multiplying both sides of equation (40a) with $\mathbf{y}_n e^{j\sum_{i=1}^{n}\epsilon(i-1)}$ from the left, (40b) with $\mathbf{y}_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}$, and (40c) with $\mathbf{y}'_n \mathbf{w}_{n-1} e^{j\sum_{i=1}^{n}\epsilon(i-1)}$, we see that the a priori (28) and a posteriori (30) estimation errors are related via

$$e_{w,p}(n) = e_{w,a}(n) - \mu_w \|\mathbf{y}_n\|^2 e(n), \quad (41a)$$

$$e_{\epsilon,p}(n) = e_{\epsilon,a}(n) - \mu_\epsilon |\mathbf{y}_n \mathbf{w}_{n-1}|^2 j^* e(n), \quad (41b)$$

$$e_{\eta,p}(n) = e_{\eta,a}(n) - \mu_\eta |\mathbf{y}'_n \mathbf{w}_{n-1}|^2 e(n). \quad (41c)$$

Equations (40) and (41) provide an alternative representation of the adaptive filter in terms of the error quantities. This is useful, as it will allow relating the steady-state behavior of these errors. So, rearranging (41a), (41b), and (41c) allows us to express the total error $e(n)$ separately in terms of the three sets of a priori and a posteriori errors:

$$e(n) = \frac{1}{\mu_w \|\mathbf{y}_n\|^2} \left[e_{w,a}(n) - e_{w,p}(n) \right], \tag{42a}$$

$$e(n) = \frac{1}{\mu_\epsilon |\mathbf{y}_n \mathbf{w}_{n-1}|^2} \left[e_{\epsilon,a}(n) - e_{\epsilon,p}(n) \right], \tag{42b}$$

$$e(n) = \frac{1}{\mu_\eta |\mathbf{y}_n' \mathbf{w}_{n-1}|^2} \left[e_{\eta,a}(n) - e_{\eta,p}(n) \right]. \tag{42c}$$

Substituting the right-hand sides of the above into (40a), (40b), and (40c), gives respectively

$$\tilde{\mathbf{w}}_n = \mathbf{w}_n^o - \mathbf{w}_{n-1} - \frac{\mathbf{y}_n^*}{\|\mathbf{y}_n\|^2} \left[e_{w,a}(n) - e_{w,p}(n) \right], \tag{43a}$$

$$\tilde{\epsilon}(n) = \tilde{\epsilon}(n-1) - \frac{(\mathbf{y}_n \mathbf{w}_{n-1})^*}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2} \left[e_{\epsilon,a}(n) - e_{\epsilon,p}(n) \right], \tag{43b}$$

$$\tilde{\eta}(n) = \tilde{\eta}(n-1) - \frac{(\mathbf{y}_n' \mathbf{w}_{n-1})^*}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2} \left[e_{\eta,a}(n) - e_{\eta,p}(n) \right], \tag{43c}$$

where on each side those identities, we have a combination of a priori and a posteriori errors, while the step sizes cancel out. By evaluating the energies of both sides, we find that the following energy equalities hold:

$$\|\tilde{\mathbf{w}}_n\|^2 + \frac{|e_{w,a}(n)|^2}{\|\mathbf{y}_n\|^2} = \|\mathbf{w}_n^o - \mathbf{w}_{n-1}\|^2 + \frac{|e_{w,p}(n)|^2}{\|\mathbf{y}_n\|^2}, \tag{44a}$$

$$|\tilde{\epsilon}(n)|^2 + \frac{|e_{\epsilon,a}(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2} = |\tilde{\epsilon}(n-1)|^2 + \frac{|e_{\epsilon,p}(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2}, \tag{44b}$$

$$|\tilde{\eta}(n)|^2 + \frac{|e_{\eta,a}(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2} = |\tilde{\eta}(n-1)|^2 + \frac{|e_{\eta,p}(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2}. \tag{44c}$$

Comparing (44a) with (44b) and (44c), we see that the main difference concerns the interpretation of the terms $\mathbf{w}_n^o - \mathbf{w}_n$ and $\mathbf{w}_n^o - \mathbf{w}_{n-1}$. While the term on the left-hand side of (44a) can be recognized as $\tilde{\mathbf{w}}_n$, just like the terms on the left-hand sides of (44b) and (44c), the second difference is not $\tilde{\mathbf{w}}_{n-1}$ since, due to the self-induced nonstationarity, $\tilde{\mathbf{w}}_{n-1}$ is defined as $\tilde{\mathbf{w}}_{n-1} = \mathbf{w}_{n-1}^o - \mathbf{w}_{n-1}$ in terms of $\mathbf{w}_{n-1}^o$ and not $\mathbf{w}_n^o$.

In order to explain the relevance of the energy relation equations to the steady-state analysis of the adaptive filter, we first need to relate $\|\mathbf{w}_n^o - \mathbf{w}_{n-1}\|^2$ to $\|\tilde{\mathbf{w}}_{n-1}\|^2$. To do so, we can write

$$\|\mathbf{w}_n^o - \mathbf{w}_{n-1}\|^2 = \left\| \mathbf{w}_{n-1}^o + \mathbf{w}_{n-1}^o j\tilde{\epsilon}(n-1) + \frac{\mathbf{y}_n^*}{\|\mathbf{y}_n\|^2} \mathbf{y}_n' \mathbf{w}_{n-1}^o \tilde{\eta}(n-1) - \mathbf{w}_{n-1} \right\|^2. \tag{45}$$

Recall that the first three terms on the right-hand side within the squared norm constitute $\mathbf{w}_n^o$ by means of linear approximation as in the derivation of (26). Based on (45), we get

$$\|\mathbf{w}_n^o - \mathbf{w}_{n-1}\|^2 = \|\tilde{\mathbf{w}}_{n-1}\|^2 + \left\|\mathbf{w}_{n-1}^o j\tilde{\epsilon}(n-1)\right\|^2 + \left\| \frac{\mathbf{y}_n^*}{\|\mathbf{y}_n\|^2} \mathbf{y}_n' \mathbf{w}_{n-1}^o \tilde{\eta}(n-1) \right\|^2. \tag{46}$$

The last two terms on the right-hand side of which can be related to $|e_{\epsilon,a}^n(n)|^2$ and $|e_{\eta,a}^n(n)|^2$ by writing

$$\|\mathbf{w}_n^o - \mathbf{w}_{n-1}\|^2 = \|\tilde{\mathbf{w}}_{n-1}\|^2 + \frac{M|e_{\epsilon,a}^n(n)|^2}{\|\mathbf{y}_n\|^2} + \frac{M|e_{\eta,a}^n(n)|^2}{\|\mathbf{y}_n\|^2}. \tag{47}$$

Substituting (47) into (44a), taking the expectation of both sides of (44a), (44b), and (44c), using that $E\|\tilde{\mathbf{w}}_n\|^2 = E\|\tilde{\mathbf{w}}_{n-1}\|^2$, $E|\tilde{\epsilon}(n)|^2 = E|\tilde{\epsilon}(n-1)|^2$, and $E|\tilde{\eta}(n)|^2 = E|\tilde{\eta}(n-1)|^2$ in steady state as $n \to \infty$, gives the following fundamental variance relations:

$$E\left[\frac{|e_{w,a}(n)|^2}{\|\mathbf{y}_n\|^2}\right] = E\left[\frac{M|e_{\epsilon,a}^n(n)|^2}{\|\mathbf{y}_n\|^2}\right] + E\left[\frac{M|e_{\eta,a}^n(n)|^2}{\|\mathbf{y}_n\|^2}\right] + E\left[\frac{|e_{w,p}(n)|^2}{\|\mathbf{y}_n\|^2}\right], \tag{48a}$$

$$E\left[\frac{|e_{\epsilon,a}(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2}\right] = E\left[\frac{|e_{\epsilon,p}(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2}\right], \tag{48b}$$

$$E\left[\frac{|e_{\eta,a}(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2}\right] = E\left[\frac{|e_{\eta,p}(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2}\right]. \tag{48c}$$

These equalities are given in terms of the a priori and a posteriori errors. However, we know from (41) how those errors are related. Therefore, using (41) the above collapse to the following error variance relations in terms of the a priori errors and noise only:

$$E\left[\frac{|e_{w,a}(n)|^2}{\|\mathbf{y}_n\|^2}\right] = E\left[\frac{M|e_{\epsilon,a}^n(n)|^2}{\|\mathbf{y}_n\|^2}\right] + E\left[\frac{M|e_{\eta,a}^n(n)|^2}{\|\mathbf{y}_n\|^2}\right] + E\left[\frac{1}{\|\mathbf{y}_n\|^2}|e_{w,a}(n) - \mu_w\|\mathbf{y}_n\|^2 e(n)|^2\right], \tag{49a}$$

$$E\left[\frac{|e_{\epsilon,a}(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2}\right] = E\left[\frac{|e_{\epsilon,a}(n) - \mu_\epsilon |\mathbf{y}_n \mathbf{w}_{n-1}|^2 j^* e(n)|^2}{|\mathbf{y}_n \mathbf{w}_{n-1}|^2}\right], \tag{49b}$$

$$E\left[\frac{|e_{\eta,a}(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2}\right] = E\left[\frac{|e_{\eta,a}(n) - \mu_\eta |\mathbf{y}_n' \mathbf{w}_{n-1}|^2 e(n)|^2}{|\mathbf{y}_n' \mathbf{w}_{n-1}|^2}\right]. \tag{49c}$$

Expanding the above, rearranging, and dividing by μ_w, μ_ϵ, and μ_η respectively, we get

$$\mu_w E\left[\|\mathbf{y}_n\|^2 |e(n)|^2\right] + E\left[\frac{M|e_{\epsilon,a}^n(n)|^2}{\mu_w \|\mathbf{y}_n\|^2}\right] + E\left[\frac{M|e_{\eta,a}^n(n)|^2}{\mu_w \|\mathbf{y}_n\|^2}\right] = 2\Re\left\{E\left[e_{w,a}^*(n)e(n)\right]\right\}, \tag{50a}$$

$$\mu_\epsilon E\left[|\mathbf{y}_n \mathbf{w}_{n-1}|^2 |e(n)|^2\right] = 2\Re\left\{E\left[e_{\epsilon,a}^*(n)e(n)\right]\right\}, \tag{50b}$$

$$\mu_\eta E\left[|\mathbf{y}_n' \mathbf{w}_{n-1}|^2 |e(n)|^2\right] = 2\Re\left\{E\left[e_{\eta,a}^*(n)e(n)\right]\right\}. \tag{50c}$$

Finally, substituting (29) into the equations in (50) while also relying on A.2, we arrive at the equations in (33).

REFERENCES

[1] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[2] B. S. Sharif, J. Neasham, O. R. Hinton, and A. E. Adams, "A computationally efficient Doppler compensation system for underwater acoustic communications," *IEEE J. Ocean. Eng.*, vol. 25, no. 1, pp. 52–61, Jan. 2000.

[3] T. Pollet, M. V. Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and Wiener phase noise," *IEEE Trans. Commun.*, vol. 43, no. 2/3/4, pp. 191–193, Apr. 1995.

[4] B. Stantchev and G. Fettweis, "Time-variant distortions in OFDM," *IEEE Commun. Lett.*, vol. 4, no. 10, pp. 312–314, Oct. 2000.

[5] L. Weng et al., "Effect of carrier frequency offset on channel estimation for SISO/MIMO-OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1854–1863, May 2007.

[6] T. Pollet, P. Spruyt, and M. Moeneclaey, "The BER performance of OFDM systems using non-synchronized sampling," in *Proc. IEEE Glob. Commun. Conf.*, 1994, pp. 253–257.

[7] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994.

[8] M. Sliskovic, "Carrier and sampling frequency offset estimation and correction in multicarrier systems," in *Proc. Glob. Telecommun. Conf.*, 2001, vol. 1, pp. 285–289.

[9] S.-Y. Liu and J.-W. Chong, "A study of joint tracking algorithms of carrier frequency offset and sampling clock offset for OFDM-based WLANs," in *Proc. IEEE Int. Conf. Commun., Circuits Syst.*, 2002, vol. 1, pp. 109–113.

[10] H. Nguyen-Le, T. Le-Ngoc, and C. C. Ko, "RLS-based joint estimation and tracking of channel response, sampling, and carrier frequency offsets for OFDM," *IEEE Trans. Broadcast.*, vol. 55, no. 1, pp. 84–94, Mar. 2009.

[11] K. Shi, E. Serpedin, and P. Ciblat, "Decision-directed fine synchronization in OFDM systems," *IEEE Trans. Commun.*, vol. 53, no. 3, pp. 408–412, Mar. 2005.

[12] M. Morelli and M. Moretti, "Fine carrier and sampling frequency synchronization in OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1514–1524, Apr. 2010.

[13] Y.-H. Kim and J.-H. Lee, "Joint maximum likelihood estimation of carrier and sampling frequency offsets for OFDM systems," *IEEE Trans. Broadcast.*, vol. 57, no. 2, pp. 277–283, Jun. 2011.

[14] X. Wang and B. Hu, "A low-complexity ML estimator for carrier and sampling frequency offsets in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 3, pp. 503–506, Mar. 2014.

[15] H. Viswanathan, S. Venkatesan, and H. Huang, "Downlink capacity evaluation of cellular networks with known-interference cancellation," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 802–811, Jun. 2003.

[16] W. Guo, C. Li, H. Zhao, R. Wen, and Y. Tang, "Comprehensive effects of imperfect synchronization and channel estimation on known interference cancellation," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 457–470, Jan. 2020.

[17] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, "Effect of frequency offset on cooperative jamming cancellation in physical layer security," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–5.

[18] C. Li, Y. Liu, Q. Xu, and Y. Tang, "Self-interference cancellation with frequency offset and nonlinear distortion suppression for cooperative jamming communications," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 2091–2094, Nov. 2019.

[19] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 240–243, Feb. 2020.

[20] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[21] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[22] R. Mudumbai, D. R. B. Iii, U. Madhow, and H. V. Poor, "Distributed transmit beamforming: Challenges and recent progress," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 102–110, Feb. 2009.

[23] I. Walterscheid et al., "Bistatic SAR experiments with PAMIR and TerraSAR-X–setup, processing, and image results," *IEEE Trans. Geosci. Remote Sens.*, vol. 48, no. 8, pp. 3268–3279, Aug. 2010.

[24] M. Weib, "Synchronisation of bistatic radar systems," in *Proc. Int. Geosc. Remote Sens. Symp.*, 2004, vol. 3, pp. 1750–1753.

[25] J. Yi, X. Wan, D. Li, and H. Leung, "Robust clutter rejection in passive radar via generalized subband cancellation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 4, pp. 1931–1946, Aug. 2018.

[26] R. Gitlin and J. Thompson, "A phase adaptive structure for echo cancellation," *IEEE Trans. Commun.*, vol. 26, no. 8, pp. 1211–1220, Aug. 1978.

[27] M. Pawig, G. Enzner, and P. Vary, "Adaptive sampling rate correction for acoustic echo control in voice-over-IP," *IEEE Trans. Signal Process.*, vol. 58, no. 1, pp. 189–199, Jan. 2010.

[28] N. R. Yousef and A. H. Sayed, "Ability of adaptive filters to track carrier offsets and channel nonstationarities," *IEEE Trans. Signal Process.*, vol. 50, no. 7, pp. 1533–1544, Jul. 2002.

[29] H.-C. So, P.-C. Ching, and Y.-T. Chan, "A new algorithm for explicit adaptation of time delay," *IEEE Trans. Signal Process.*, vol. 42, no. 7, pp. 1816–1820, Jul. 1994.

[30] Z. Li, Y. Xia, W. Pei, K. Wang, and D. P. Mandic, "An augmented nonlinear LMS for digital self-interference cancellation in full-duplex direct-conversion transceivers," *IEEE Trans. Signal Process.*, vol. 66, no. 15, pp. 4065–4078, Aug. 2018.

[31] X. Zhang, Y. Xia, C. Li, L. Yang, and D. P. Mandic, "Complex properness inspired blind adaptive frequency-dependent I/Q imbalance compensation for wideband direct-conversion receivers," *IEEE Trans. Wireless Commun.*, vol. 19, no. 9, pp. 5982–5992, Sep. 2020.

[32] M. Meller, "Cheap cancellation of strong echoes for digital passive and noise radars," *IEEE Trans. Signal Process.*, vol. 60, no. 5, pp. 2654–2659, May 2012.

[33] N. R. Yousef and A. H. Sayed, "A unified approach to the steady-state and tracking analyses of adaptive filters," *IEEE Trans. Signal Process.*, vol. 49, no. 2, pp. 314–324, Feb. 2001.

[34] S. S. Haykin, *Adaptive Filter Theory*, 5th ed. London, U.K.: Pearson Education, 2014.

[35] A. H. Sayed, *Fundamentals of Adaptive Filtering*. Hoboken, NJ, USA: Wiley, 2003.

[36] K. Atkinson and W. Han, *Theoretical Numerical Analysis*, vol. 39. New York, NY, USA: Springer, 2005.

[37] T. Ramstad, "Digital methods for conversion between arbitrary sampling frequencies," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 32, no. 3, pp. 577–591, Jun. 1984.

[38] T. I. Laakso, "Splitting the unit delay," *IEEE Signal Process. Mag.*, vol. 13, no. 1, pp. 30–60, Jan. 1996.

[39] D. P. Mandic and V. S. L. Goh, *Complex Valued Nonlinear Adaptive Filters: Noncircularity, Widely Linear and Neural Models*. Hoboken, NJ, USA: Wiley, 2009.

[40] C. Candan, "An efficient filtering structure for Lagrange interpolation," *IEEE Signal Process. Lett.*, vol. 14, no. 1, pp. 17–19, Jan. 2007.

[41] E. Soria-Olivas, J. Calpe-Maravilla, J. F. Guerrero-Martinez, M. Martinez-Sober, and J. Espi-Lopez, "An easy demonstration of the optimum value of the adaptation constant in the LMS algorithm [FIR filter theory]," *IEEE Trans. Educ.*, vol. 41, no. 1, p. 81, Feb. 1998.

[42] N. Zhang, J. Ni, J. Chen, and Z. Li, "Steady-state mean-square error performance analysis of the tensor LMS algorithm," *IEEE Trans. Circuits Syst. II:Exp. Briefs*, vol. 68, no. 3, pp. 1043–1047, Mar. 2021.

[43] N. D. Dalt, M. Harteneck, C. Sandner, and A. Wiesbauer, "On the jitter requirements of the sampling clock for analog-to-digital converters," *IEEE Trans. Circuits Syst. I*, vol. 49, no. 9, pp. 1354–1360, Sep. 2002.

Karel Pärlin received the M.Sc. degree in electrical engineering from the Tallinn University of Technology, Tallinn, Estonia, in 2017. He is currently working toward the D.Sc. degree in communication engineering with Tampere University, Tampere, Finland. His research interests include adaptive signal processing, signal processing for communications, and physical layer security.

Taneli Riihonen (Senior Member, IEEE) received the D.Sc. degree in electrical engineering from Aalto University, Espoo, Finland, in 2014. He is currently a tenure-track Associate Professor with the Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland. His research interests include physical-layer OFDM(A), multiantenna, multihop, and full-duplex wireless techniques with current research interest includes the evolution of beyond 5G systems.

Vincent Le Nir received the Ph.D. degree in electronics from the National Institute of Applied Sciences, France, in 2004. He is currently a Senior Researcher with the Royal Military Academy, Brussels, Belgium. His research interests include digital communications and signal processing in the wireless and wireline domains, MIMO communications, space–time coding, OFDM and multicarrier-code-division multiple-access, turbo-equalization, software defined, and cognitive radio.

Marc Adrat received the Diploma and Dr.-Ing. degrees in electrical engineering from RWTH Aachen University, Aachen, Germany, in 1997 and 2003, respectively. He is currently the Head of the Software Defined Radio (SDR) Research Group, Fraunhofer FKIE, Wachtberg, Germany. His research interests include digital signal processing for mobile tactical radio communications, and emerging technologies like in-band full-duplex communications. Since more than 10 years, he is a Guest Lecturer with RWTH Aachen University for a course on channel coding.

PUBLICATION 6

Physical-Layer Reliability of Drones and Their Counter-Measures: Full vs. Half Duplex

K. Pärlin, T. Riihonen, V. Le Nir and M. Adrat

IEEE Transactions on Wireless Communications 2023. In press
DOI: 10.1109/TWC.2023.3290257

Physical-Layer Reliability of Drones and Their Counter-Measures: Full vs. Half Duplex

Karel Pärlin, Taneli Riihonen, *Senior Member, IEEE*, Vincent Le Nir, and Marc Adrat

***Abstract*—In this article, we study the advantages and disadvantages that full-duplex (FD) radio technology brings to remote-controlled drone and counter-drone systems in comparison to classical half-duplex (HD) radio technology. We consider especially the physical-layer reliability perspective that has not yet been comprehensively studied. For establishing a solid analytical background, we first derive original closed-form expressions to evaluate demodulation and detection performance of frequency-hopped and frequency-shift keyed drone remote control signals under external or self-inflicted interference. The developed analytical tools are verified by comparison to simulated results and then used to study the impact that the operation mode has on the operable area of drones and effectiveness of counter-drone systems in different scenarios, linking the physical layer performance to practical safety. Analysis of the scenarios shows that FD operation compared to HD can improve the effectiveness of a counter-drone system and that in FD mode a drone can detect the attacks from the counter-drone system from a greater distance than in HD mode. However, two-way communication between the remote controller and drone in FD mode compared to HD significantly reduces the drone's operable area when targeted by a smart counter-drone system.**

***Index Terms*—Reliability, drone, UAV, counter-drone, half-duplex, full-duplex, jamming, energy detection.**

I. Introduction

RELIABILITY is a critical issue in wireless communications, since malicious users may, due to the broadcast nature of wireless transmissions, rather easily interfere with the reception of the transmitted signals at the intended receiver. There are some reliability-enhancing methods that can be used on the upper layers of a two-point wireless communications link to mitigate the effect of interference. For example, channel coding can help overcome interference at the cost of redundancy in the communication. However, the physical-layer implementation (i.e., the modulation technique and rate along with the use of spread spectrum techniques) of a wireless system lays the foundation for the communication's overall reliability, similarly to how the physical-layer implementation of an electronic counter-measure system determines its respective performance.

Manuscript received 25 March 2023; revised 17 May 2023 and 9 June 2023; accepted 23 June 2023. The associate editor coordinating the review of this paper and approving it for publication was Prof. J. Choi.

K. Pärlin and T. Riihonen are with Tampere University, Faculty of Information Technology and Communication Sciences, Korkeakoulunkatu 1, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi).

V. Le Nir is with Royal Military Academy, Signal and Image Center, Avenue de la Renaissance 30, B-1000 Brussels, Belgium.

M. Adrat is with Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Fraunhofer Straße 20, 53343 Wachtberg, Germany.

This research work was supported by the Academy of Finland and the Finnish Scientific Advisory Board for Defence.

Digital Object Identifier 10.1109/TWC.2023.3290257

One recent development that has the potential to enhance both wireless communication and electronic counter-measure systems is full-duplex (FD) radio technology. Advances in the self-interference (SI) cancellation research are facilitating FD operation [1] that potentially allows to simultaneously combine wireless communications and electronic warfare functions. This entails, e.g., simultaneous signals reception and jamming, to prevent eavesdropping and increase the security of wireless systems, or simultaneous surveillance and jamming, to increase the efficiency of electronic counter-measure systems [2]. As such, FD radio technology is a promising candidate for improving the reliability and also security of wireless systems. Several practical works demonstrating the feasibility of applying FD technology for such combinations have already been published [3]–[5] in addition to the information theoretic physical-layer secrecy studies [6]–[9]. However, practical gains of such combinations with regards to physical-layer reliability have not yet been comprehensively studied.

Reliability is essential in any wireless application and it is becoming increasingly relevant as the number of connected devices grows. However, in order to relate this work to the safety of practical and timely systems, we focus here on drone and counter-drone systems only. We consider drones as the central theme of this work because the proliferation of consumer drones poses a significant challenge in protecting various airspaces [10] and, as the application of drones in all aspects of life increases, their reliability and security is becoming more and more important for the safety of the applications in which they are used [11], [12]. There is also significant overlap in FD and drone research as FD-enhanced drones have been shown to outperform their terrestrial and strictly half-duplex (HD) counterparts as base stations [13] and relaying systems [14].

Countering malicious drones and improving the reliability and security of remote-controlled drones has received significant interest as the availability of drones has increased. The existing counter-measures have been thoroughly studied and various aspects of counter-drone operations are progressively enhanced [15], [16]. Likewise, robustness and privacy of the wireless communications links of legitimate drone applications have been carefully considered against various threats and improvements are being suggested [17], [18]. Furthermore, it has been recognized that the management of intentional interference in satellite navigation on board of drones is of significant importance [19]. However, all of these works emphasize that, in order to promote safe, secure, and privacy-respecting drone operations, there is still a need for innovative technologies to neutralize malicious drones and improve resilience of legitimate drone applications.

In the context of wireless networks, it has been proposed that jointly optimizing the trajectory and output power [20] or beamforming [21] can be used to improve the physical-layer security of drones. However, these methods rely on the channel state information being available to drones and this is difficult to acquire in practice, especially when dealing with non-cooperative nodes. Another solution, which has been studied under the term covert communications, is hiding wireless transmissions [22]. Interference-generating FD receivers have great potential of hiding wireless transmissions from eavesdroppers [23], but this assumes that the interference-generating node is ever-present at the eavesdroppers location [23] or that the eavesdropper is uncertain about the noise parameters at its receiver [24]. In practice it is difficult to justify these assumptions within the context of counter-drone scenarios.

In this work, we examine how enhancing remote-controlled drones and counter-drone systems with FD capabilities affects their reliability. In order to provide a comprehensive and practically relevant analysis, we consider counter-drone systems with varying levels of sophistication. The goal of this study is to characterize the performance of practical remote-controlled drone and counter-drone systems for all of the relevant configurations of HD and FD capabilities on either side, giving detailed insight into the achievable physical-layer reliability, which translates into the safety of practical environments where drones are used, for good or bad.

Similar reliability analysis has not been carried out before and, therefore, this work complements the existing research from a new, practical perspective. Unlike the drone physical-layer security works [20], [21], this work does not assume known channel states nor optimizes the output power and trajectory, but studies if FD is beneficial over HD at practical output powers and operation-imposed trajectories. Compared to FD physical-layer security works [6], [7], this work does not analyse the information theoretical security of communications, but their physical-layer reliability under interference. Furthermore, this work does not focus on the spectrum efficiency of FD communications [13], [14], but the physical safety, which stems from the remote control link reliability. Unlike existing counter-drone [15], [16] and counter counter-drone works [17], [18] that consider aspects such as machine learning, e.g., this work studies the duplexing modes.

In order to facilitate the analysis, we first derive analytical methods for evaluating the detection and demodulation probabilities of frequency-hopped binary frequency-shift keying (BFSK) signals under interference. We then use that functionality within three scenarios that illustrate the duplexing mode trade-offs in improving the reliability and security of remotely controlled drones as following. Firstly, the analysis shows that operating a counter-drone system in FD mode can be expected to improve its effectiveness compared to that in HD mode. Secondly, operating the drone and remote controller in FD two-way communication mode makes the drone an easier target than in HD mode and, hence, reduces the operable area. Thirdly, a FD-enhanced drone has superior interference detection performance compared to a HD-limited drone, possibly allowing the FD-enhanced drone to avoid areas where it would be rendered inoperable by jamming. All three scenarios also show the performance difference of counter-drone systems with different complexities. Finally, we study the energy efficiencies of the jamming strategies and demonstrate the hard truth that elevating the counter-drone system can be a more significant improvement than any of the strategies or operation modes.

The rest of this article is organized as follows. To begin with, Section II introduces in detail the system model considered in this work. Then, Section III develops the techniques necessary for analysing all the possible configurations of the presented system model. In Section IV, the developed analysis techniques are, firstly, verified by comparison to simulations and, secondly, used in three practical scenarios to study the performance of HD and FD operation mode therein. Finally, conclusions of the study are given in Section V.

II. System Model

In this work we consider a system of three nodes as illustrated in Fig. 1, consisting of a remote controller, a remote-controlled drone, and a counter-drone system. We assume that the remote controller and the drone use a two-way slow frequency-hopped BFSK radio-frequency (RF) remote control link, such as is used in many practical remote-controlled drones [10]. The counter-drone system aims to detect that RF link and neutralize the remote-controlled drone by interfering with that RF link. Each of the nodes operates in either HD or FD mode, with the FD mode enabling simultaneous transmission and reception on the same frequency to combine a selection of wireless communications, signals reconnaissance, and signals interference functions. We assume that the channels between the three nodes are frequency flat, affected only by the path loss, and can be modeled by complex coefficients h_{RD}, h_{RJ}, and h_{DJ} as shown in Fig. 1. We make the same assumptions for the self-interference channels h_{RR}, h_{DD}, and h_{JJ} with the addition that these also potentially include the effect of self-interference cancellation. The specific capabilities and objectives of the three nodes are as follows.

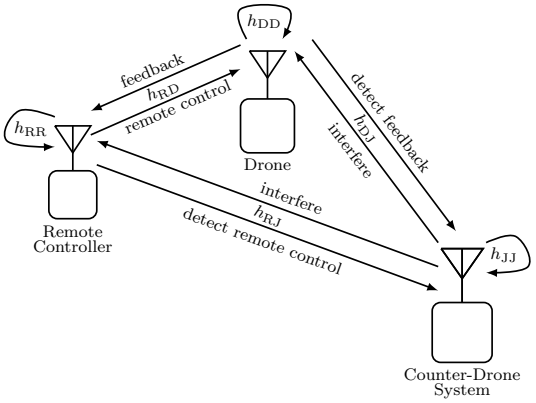


Fig. 1. Three-node system model, consisting of a remote controller, a remote-controlled drone, and a counter-drone system. This system model is a simple, yet realistic representation of counter-drone scenarios.

A. Remote Controller

The main task of the remote controller is to transmit control signals to the drone for directing its movements. The basic elements of the transmitter at the remote controller are shown in Fig. 2. The input binary data has a rate R_b [bits/s] and it is error-correction encoded at a code rate r, so that the encoded data has a rate $R_\mathrm{c} = R_\mathrm{b}/r$ [bits/s]. The encoded data is converted to BFSK symbols, and, since binary modulation is considered, the symbol rate is equal to the encoded data rate $R_\mathrm{s} = R_\mathrm{c}$. Finally, the symbols are mixed with a frequency hopping tone of frequency ω_m that changes with hop rate R_h. As a result, the drone's remote controller transmits a sequence of slow frequency-hopped BFSK signal

$$x^{\mathrm{R}}_{m,l}(t) = \sqrt{P^{\mathrm{R}}_{\mathrm{x}}} \exp\left(i\left(\omega_m + l\omega_\Delta\right)t + i\theta_{\mathrm{x}}\right) \tag{1}$$

with fixed signal power $P^{\mathrm{R}}_{\mathrm{x}}$, frequency-hopped channel center frequency ω_m, channel number m, symbol l either 1 or -1 depending on the encoded data, frequency deviation ω_Δ, and random initial phase θ_x. The superscript R in (1) denotes the remote controller, while the superscript D will be used to denote the drone's signal and output power. The usual definition of slow frequency hopping is that $R_\mathrm{s} > R_\mathrm{h}$, so that several symbols are transmitted during a single hop, which is also the case here. The total bandwidth W is divided into M consecutive frequency hopping channels with bandwidths W/M, as is typical for commercial drones in order to provide a robust control link in noisy radio environments [10].

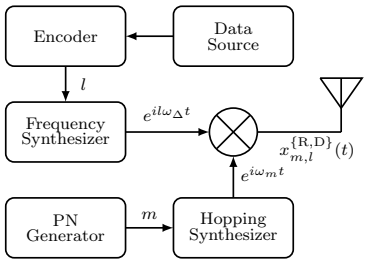


Fig. 2. Block diagram of a slow frequency-hopped binary frequency-shift keying transmitter at the remote controller or drone as indicated with the use of curly brackets in $x^{\{\mathrm{R,D}\}}_{m,l}$.

Additionally, in HD mode the remote controller is capable of receiving signals on any of the channels that it is not simultaneously transmitting on, while in FD mode the remote controller is capable of receiving signals on any of the channels at any time, subject to disturbance from residual SI on the channel that it is simultaneously transmitting on. Residual SI refers to the interference that the transmitting node causes to itself, which due to insufficient cancellation interferes with the desired signal being received by that node [1]. The received signals can be either feedback from the drone, interference from the counter-drone system, or both feedback and interference superposed. The remote controller is assumed to be fitted with a feedback receiver, which corresponds to the noncoherent demodulator described in the next subsection.

B. Remote-Controlled Drone

For the purpose of this system model, the main task of the drone is to receive the remote control signals without errors from the operator. The structure of the receiver at the drone is illustrated in Fig. 3. It is assumed that the remote controller and drone have in advance agreed on a frequency hopping pattern and that the dehopping synthesizer is perfectly aligned with the hopping synthesizer in time and frequency. After dehopping, the received complex baseband signal for channel m at the drone receiver is

$$y^{\mathrm{D}}_m(t) = \left[h_{\mathrm{RD}} x^{\mathrm{R}}_{m,l}(t) + h_{\mathrm{DJ}} j_m(t) + n(t)\right] e^{-i\omega_m t}, \tag{2}$$

where $j_m(t)$ is the interference transmitted by the counter-drone system on frequency channel m, and $n(t)$ denotes complex lowpass additive white Gaussian noise with variance $\mathcal{E}\{n^2(t)\} \triangleq \sigma^2_{\mathrm{n}}$. In order to demodulate the signal, the noncoherent demodulator decides between the two hypotheses

$$H_0 : y^{\mathrm{D}}_m(t) = \left[h_{\mathrm{RD}} x^{\mathrm{R}}_{m,-1}(t) + h_{\mathrm{DJ}} j_m(t) + n(t)\right] e^{-i\omega_m t}, \tag{3}$$

$$H_1 : y^{\mathrm{D}}_m(t) = \left[h_{\mathrm{RD}} x^{\mathrm{R}}_{m,+1}(t) + h_{\mathrm{DJ}} j_m(t) + n(t)\right] e^{-i\omega_m t}, \tag{4}$$

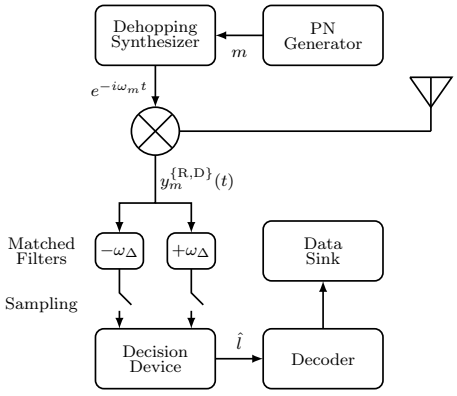
where the signal-of-interest, $x^{\mathrm{R}}_{m,l}(t)$, has been transmitted with either $l = -1$ or $l = +1$ deviation. The noncoherent demodulator passes the dehopped signal through two matched filters, see Fig. 3(b), the output of which are sampled at rate R_c and which result in two test statistics $Y_l = \int_0^{T_\mathrm{c}} v_l(t) y^{\mathrm{D}}_m(t) dt$, where $v_l = \exp\left(il\omega_\Delta t\right)$ is the complex basis function and T_c the coded bit time duration. To decide between the hypotheses, the two values, Y_{-1} and Y_{+1}, are compared and the largest chosen. This provides an estimate $\hat{l}$ of the transmitted symbol.

Finally, decoding aims to correct any errors. We assume that block coding is used, allowing to approximate the information-bit error rate (BER) based on the channel-BER as

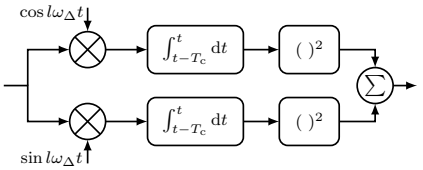
$$P_{\mathrm{ib}} \approx \frac{d}{n} \sum_{i=t+1}^{d} \binom{n}{i} P^i_{\mathrm{e}} \left(1 - P_{\mathrm{e}}\right)^{n-i} + \frac{1}{n} \sum_{i=d+1}^{n} i \binom{n}{i} P^i_{\mathrm{e}} \left(1 - P_{\mathrm{e}}\right)^{n-i}, \tag{5}$$

where P_e is the channel-BER, d is the minimum distance between codewords, $t = \lfloor (d-1)/2 \rfloor$, and n is the length of the codewords [25].

Furthermore, in HD mode the drone is capable of transmitting signals on any of the channels that its not simultaneously receiving on, while in FD mode the drone is capable of transmitting signals on any of the channels at any time, although impacting the receiving performance due to residual SI. The transmitted signals can be either feedback to the remote controller or interference targeting the counter-drone system, if the drone chooses to apply some electronic counter-countermeasures. For transmitting feedback signals, the drone is assumed to be fitted with the same transmitter as described in the previous subsection. We consider that the drone is in its operable area when the channel-BER in both ways is below a certain threshold P_T; that is, $\max\{P^{\mathrm{D}}_e, P^{\mathrm{R}}_e\} < P_\mathrm{T}$.



(a) Receiver



(b) Matched filter

Fig. 3. Block diagram of a slow frequency-hopped binary noncoherent frequency-shift keying receiver at the remote controller (R) or drone (D) as indicated with the use of curly brackets in $y_m^{\{\mathrm{R,D}\}}$.

C. Counter-Drone System

The counter-drone system is composed of detection and jamming subsystems and we analyze the entire system with various levels of sophistication that are typical for electronic counter-measure systems [26]. For detecting the signals, the counter-drone system relies on a channelized energy detector (illustrated in Fig. 4), which gives a single binary detection result together with an index $\hat{m}$ of the channel that decidedly contains the signal. It is assumed that the energy detector has M channels that are perfectly matched with the channel frequencies and bandwidths used by the drone (for analytical purposes). The task of each of the individual energy detector channels is to decide between the two hypotheses

$$H_0 : y_m^{\mathrm{J}}(t) = h_{\mathrm{JJ}} j_m(t) + n(t), \tag{6}$$

$$H_1 : y_m^{\mathrm{J}}(t) = h_{\{\mathrm{RJ,DJ}\}} x_{m,l}^{\{\mathrm{R,D}\}}(t) + h_{\mathrm{JJ}} j_m(t) + n(t), \tag{7}$$

where the signal-of-interest from remote controller or drone (R or D) $x_{m,l}^{\{\mathrm{R,D}\}}$ is absent or present, could even be superposition of both signals (e.g., if the drone and remote controller are operating in FD mode), and the superscript J denotes the counter-drone system. In order to decide, the energy detector filters, squares, and integrates the received signal over a period T_d, which results in a test statistic $z_m = 1/T_\mathrm{d} \int_0^{T_\mathrm{d}} \left| y_m^{\mathrm{J}}(t) \right|^2 dt$ that is compared to an energy threshold V_T to select between the two hypotheses [27]. As it is impractical to assume that the counter-drone system would have information about the channels h_RJ or h_DJ, the counter-drone system chooses numerically the detection threshold V_T based on the detection time T_d and noise variance σ_n^2 to produce some acceptable constant false alarm rate (CFAR).

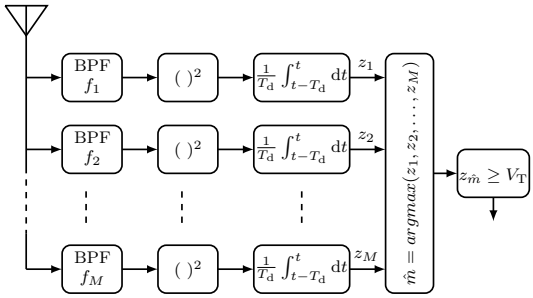


Fig. 4. Block diagram of a channelized energy detector.

We consider that the counter-drone system has the described signal detection capability and then it applies either constant, reactive, or follower jamming principles, which are illustrated in Fig. 5 and altogether cover the bulk of the modern jamming strategies. Conversely to the operable area of a drone, we consider that the effective area of a counter-drone system is the area in which the counter-drone system forces the channel-BER over a certain threshold in either direction of the remote control link; that is, the counter-drone system is effective when $\max\{P_e^{\mathrm{D}}, P_e^{\mathrm{R}}\} \geq P_\mathrm{T}$.

1) Constant: In the simplest case, the counter-drone system completely avoids the chance of it not detecting the remote control signals, the system does not try to conserve energy, nor does it try to hide the jamming signals. As such, it continuously jams the total bandwidth W using either noise with fixed signal power P_j or linearly frequency-swept interference

$$j(t) = \sqrt{P_\mathrm{j}} \exp\left(i\left(ct/2 + \omega_\mathrm{j}\right)t + i\theta_\mathrm{j}\right) \tag{8}$$

with sweep rate c, arbitrary phase offset θ_j, and fixed signal power P_j. As such, the counter-drone system is strictly limited to jamming if it operates in HD mode. However, in FD mode, the counter-drone system still has the possibility to detect the remote control signals, as long as the signal-to-interference-plus-noise ratio (SINR) allows, even though constant jamming itself does not have any use for this kind of signals intelligence. Still, the information can be useful in a broader perspective within an operational scenario. For example, to notify the counter-drone system operator of an advancing threat or perhaps to change the jamming strategy.

2) Reactive: In the more complicated case, the counter-drone system does rely on the channelized radiometer to detect the targeted signal, but does not take into account the detected channel, instead considering the detection result for the whole band using logical-OR combining, i.e., selecting the individual energy detector corresponding to the channel $\hat{m}$ with highest test statistic, so that $z_{\hat{m}} \geq z_m \ \forall \ m$, and comparing that test statistic to the threshold, resulting in

$$\text{detection} = \begin{cases} \text{true}, & \text{if } z_{\hat{m}} \geq V_\mathrm{T} \\ \text{false}, & \text{otherwise.} \end{cases} \tag{9}$$

This may be desirable if the counter-drone system is interested in interfering also with fast frequency-hopped communications where the reaction time might be insufficient, the propagation delays cause problems, or if in reality the counter-drone system does not have the channel information or capability to process the full bandwidth in a channelized manner [28]. Then, to neutralize the connection between the remote controller and drone, the jamming subsystem of the counter-drone system transmits either noise with total bandwidth W and signal power P_{j} or linearly frequency-swept interference as in (8) but for time duration T_{j}. In HD mode, after T_{j}, the counter-drone system stops jamming and returns to detection mode, while in FD mode, the counter-drone system then continues jamming throughout the next detection stage.

3) Follower: In the most sophisticated and potentially most efficient case, the counter-drone system relies on the complete information produced by the channelized radiometer to follow the targeted signal in the frequency domain [29]. As such, the follower jammer transmits noise with bandwidth W/M and signal power P_{j} in a single channel with most received energy above the threshold V_{T}. For the follower jammer, we discard the frequency-swept interference, since the idea behind frequency sweeping is to spread the interference impact across many channels, when the exact channel is unknown. In HD mode, the counter-drone system applying follower jamming is limited to detecting the remote control signals when it is not simultaneously jamming, while in FD mode, the counter-drone system is able to simultaneously jam and detect on all of the channels, subject to SI on the jammed channel. This is a reasonable presumption as we will rely on powerful jammer output powers, for which receiving even on adjacent channels simultaneously to transmitting is challenging in HD mode.

III. Analysis Techniques

In this section, we present methods for evaluating the detection and demodulation probabilities of frequency-hopped BFSK signal under interference, self-inflicted or otherwise. These methods will allow us to analyse how the drone and counter-drone system will perform depending on operation modes and strategies. The methods are presented in terms of

- N_{d} — number of samples per channel,
- P_{r} — received signal power,
- P_{si} — received self-interference power,
- P_{i} — received interference power,
- σ_{n}^2 — noise variance per channel,
- c — sweep rate,
- V_{T} — detection threshold, and
- M — number of channels.

Subscripts C, R and F distinguish probabilities pertaining to constant, reactive and follower jammer, MJ refers to missed jamming opportunity, while MD and FA indicate missed detection and false alarm. In Section IV, the methods will be used for studying the operable area of remote-controlled drones and the effectiveness of counter-drone systems. Note that if the remote controller and drone are communicating in FD mode, then the received signal power P_{r} at the counter-drone system is the power of the superposition of these two signals. Assuming negligible frequency offsets and that on average the phase difference between those two signals is uniformly distributed, the total received signal power can be taken to be the sum of the powers of both received signals.

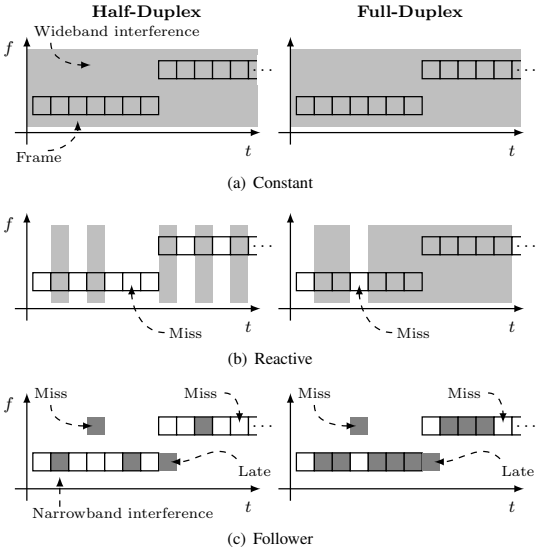


Fig. 5. Conceptual diagram of frequency-hopped communications and different jamming techniques. The wideband interference can be either wideband noise or frequency-swept narrowband signal. For reactive and follower jamming strategies, the FD operation mode allows to affect a larger portion of the targeted signal frame than HD operation mode.

A. Detection

Since we consider a counter-drone system that operates in HD or FD mode and uses any of the specified strategies, we present novel probability expressions for the following separate cases that altogether cover the counter-drone system capabilities described in the system model.

Proposition 1. *The steady-state probability of a half-duplex counter-drone system missing a jamming opportunity (i.e., not deciding to jam due to missed detection or not being able to jam while in detection mode) is*

$$P_{\mathrm{MJ,F}}^{\mathrm{HD}}\left(N_{\mathrm{d}}, P_{\mathrm{r}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right) = 1/\left(2 - P_{\mathrm{MD,F}}\left(N_{\mathrm{d}}, P_{\mathrm{r}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right)\right) \quad (10)$$

where the probability of missed detection for a channelized energy detector without self-interference is

$$P_{\mathrm{MD,F}}\left(N_{\mathrm{d}}, P_{\mathrm{r}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right) = 1 - \frac{1}{2}\int_{V_{\mathrm{T}}}^{\infty}\left(\frac{x}{\lambda}\right)^{\frac{N_{\mathrm{d}}-1}{2}}\left(\frac{\gamma\left(N_{\mathrm{d}}, \frac{x}{2}\right)}{\Gamma\left(N_{\mathrm{d}}\right)}\right)^{M-1} \cdot \exp\left(\frac{-\lambda - x}{2}\right) I_{N_{\mathrm{d}}-1}\left(\sqrt{\lambda x}\right) \mathrm{d}x, \quad (11)$$

where $\lambda = 2N_{\rm d}P_{\rm r}/\sigma_{\rm n}^2$ is the noncentrality parameter, $\gamma(a,x)$ is the lower incomplete gamma function [30, eq. 6.5.2], $\Gamma(z)$ denotes the gamma function [30, eq. 6.1.1], and $I_v(z)$ is the modified Bessel function of the first kind [30, eq. 9.6.3].

Proof. Given z_k, the test statistic for the channel that contains the signals of interest, and that z_m are statistically independent for all m, the probability of the test statistic z_k being larger than any of the other test statistics is

$$\Pr\left(z_m < z_k, \text{ all } m \neq k \mid z_k\right) = \prod_{m=1, m\neq k}^{M} \Pr\left(z_m < z_k \mid z_k\right), \quad (12)$$

where the probability on the right-hand side can be expressed through the cumulative distribution function of a chi-squared distributed random variable so that

$$\Pr\left(z_m < z_k \mid z_k\right) = \frac{\gamma\left(N_{\rm d}, \frac{z_k}{2}\right)}{\Gamma\left(N_{\rm d}\right)}. \quad (13)$$

Since z_k contains the signal-of-interest, it has a noncentral chi-squared probability density function (PDF) given by

$$p_{\chi^2}\left(x; N_{\rm d}, \lambda\right) = \frac{1}{2}\left(\frac{x}{\lambda}\right)^{\frac{N_{\rm d}-1}{2}} \exp\left(\frac{-\lambda - x}{2}\right) I_{N_{\rm d}-1}\left(\sqrt{\lambda x}\right) \quad (14)$$

and the probability of correct detection is (12) averaged over z_k from $V_{\rm T}$ to ∞, where z_k has the PDF given in (14). Therefore, the single-shot probability of missed detection for a channelized energy detector without self-interference results in the integral given in (11). Considering that the HD counter-drone system is always required to go into detection state after jamming or after a missed detection, which can be considered the two distinct states of a two-state Markov chain [31]. The transition probability of going into detection mode after jamming is $\nu = 1$ and the probability of transitioning into jamming mode after detection is $\mu = 1 - P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}, M\right)$. The steady-state probability of a HD counter-drone system missing a jamming opportunity is, therefore, $\frac{\nu}{\nu+\mu}$ that results in (10) and characterises the steady-state probability of such Markov chain. □

Proposition 2. *The steady-state probability of a half-duplex counter-drone system with logical-OR energy detector missing a jamming opportunity (i.e., not deciding to jam due to missed detection or not being able to jam while in detection mode) is*

$$P_{\rm MJ,R}^{\rm HD}\left(N_{\rm d}, P_{\rm r}, \sigma_n^2, V_{\rm T}, M\right) = 1/\left(2 - P_{\rm MD,R}\left(N_{\rm d}, P_{\rm r}, \sigma_n^2, V_{\rm T}, M\right)\right) \quad (15)$$

where the probability of missed detection for a channelized energy detector using logical-OR without self-interference is

$$P_{\rm MD,R}\left(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}, M\right) = P_{\rm MD}(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}) \cdot \left(1 - P_{\rm FA}(N_{\rm d}, \sigma_{\rm n}^2, V_{\rm T})\right)^{M-1}, \quad (16)$$

where

$$P_{\rm FA}(N_{\rm d}, \sigma_{\rm n}^2, V_{\rm T}) = \frac{\Gamma(N_{\rm d}, \frac{V_{\rm T}}{\sigma_{\rm n}^2})}{\Gamma(N_{\rm d})} \quad (17)$$

and

$$P_{\rm MD}(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}) = 1 - Q_{N_{\rm d}}\left(\sqrt{2N_{\rm d}P_{\rm r}/\sigma_{\rm n}^2}, \sqrt{2V_{\rm T}/\sigma_{\rm n}^2}\right), \quad (18)$$

with $Q_v(\alpha,\beta)$ being the generalized Marcum Q-function [32, eq. A.16].

Proof. When relying on logical-OR combining at the output of the channelized energy detector, the overall probability of missed detection can be expressed in terms of the probabilities of false alarm $P_{\rm FA}(N_{\rm d}, \sigma_{\rm n}^2, V_{\rm T})$ and missed detection $P_{\rm MD}(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T})$ for an individual energy detector channel. The probabilities of false alarm and missed detection for an individual energy detector channel without interference are characterized by the noncentral χ^2 distribution as given in (17) and (18) respectively [33]. The probability of missed detection for a channelized energy detector using logical-OR combining is the probability that the detection is missed for the channel that actually contains the signal and that the other channels, which do not contain the signal-of-interest, do not cause a false alarm. The probability of those independent events occurring together can be estimated using the result in (16). And again, the steady-state probability of a HD counter-drone system missing a jamming opportunity is given by (15) by considering jamming and detection to be two distinct states of a two-state Markov chain. □

Propositions 1 and 2 provide the main tools for analyzing the counter-drone system's performance in detecting the remote control signals without SI. With SI, the estimation is further complicated due to the non-uniform noise floor for follower jamming and frequency-swept interference for reactive jamming.

Proposition 3. *The steady-state probability of a full-duplex counter-drone system missing a jamming opportunity (i.e., not deciding to jam due to missed detection) is*

$$P_{\rm MJ,F}^{\rm FD}\left(N_{\rm d}, P_{\rm r}, P_{\rm si}, \sigma_{\rm n}^2, V_{\rm T}, M\right) = P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}\sigma_{\rm n}^2/\left(P_{\rm si}+\sigma_{\rm n}^2\right), \sigma_{\rm n}^2, V_{\rm T}, M\right) / \left(P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}\sigma_{\rm n}^2/\left(P_{\rm si}+\sigma_{\rm n}^2\right), \sigma_{\rm n}^2, V_{\rm T}, M\right) + 1 - P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}, M\right)\right). \quad (19)$$

Proof. We assume that the energy detector knows the residual SI power and normalizes the energy in the affected channel to have the same distribution as the channels without SI. This is equivalent to defining separate detection thresholds for the channels with and without SI based on a desired CFAR. In either case, the detector-jammer then has two states — firstly, the SI is occupying a different channel as the signal-of-interest or there being no SI at all due to previous missed detection and, secondly, the SI is occupying the same channel as the signal-of-interest. In the first case, the probability of missed detection is simply given by (11) as $P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}, \sigma_{\rm n}^2, V_{\rm T}, M\right)$, whereas in the second case the probability of missed detection due to the normalization of the integrated energy is given by (11) as $P_{\rm MD,F}\left(N_{\rm d}, P_{\rm r}\sigma_{\rm n}^2/\left(P_{\rm si}+\sigma_{\rm n}^2\right), \sigma_{\rm n}^2, V_{\rm T}, M\right)$. Again,

these probabilities give us the transition probabilities of a two-state Markov chain as in the proof of Proposition 1 and the steady-state distribution, or the overall probability of a missed jamming opportunity, becomes (19). □

Proposition 4. *The steady-state probability of a full-duplex counter-drone system with logical-OR energy detector missing a jamming opportunity (i.e., not deciding to jam due to missed detection) under wideband noise-like self-interference is*

$$P^{\mathrm{FD}}_{\mathrm{MJ,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right)= P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}}\sigma^2_{\mathrm{n}}/\left(P_{\mathrm{si}}+\sigma^2_{\mathrm{n}}\right),\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right) /\big(P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}}\sigma^2_{\mathrm{n}}/\left(P_{\mathrm{si}}+\sigma^2_{\mathrm{n}}\right),\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right) + 1-P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right)\big). \quad (20)$$

Proof. Similarly to the proof of Proposition 3, we assume that the energy detector knows the residual SI power and normalizes the integrated energy in all of the channels to have the same distribution as the channels would without the SI. This is equivalent to defining a separate detection thresholds for detection with and without SI based on a desired CFAR. In either case, the detector-jammer then has two states — firstly, there is no SI due to previous missed detection or, secondly, the SI is hampering the detection of the signal-of-interest. In the first case, the probability of missed detection is simply given by (16) as $P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right)$, whereas in the second case the probability of missed detection due to the normalization of the integrated energy is given by (16) as $P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{r}}\sigma^2_{\mathrm{n}}/\left(P_{\mathrm{si}}+\sigma^2_{\mathrm{n}}\right),\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right)$. These probabilities give us the transition probabilities of a two-state Markov chain. The steady-state distribution, or the overall missed detection probability, becomes (20). □

From (18), it directly follows that the false alarm probability under deterministic interference for an individual energy detector is

$$P^{\mathrm{SI}}_{\mathrm{FA}}(N_{\mathrm{d}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}}) = Q_{N_{\mathrm{d}}}\left(\sqrt{2N_{\mathrm{d}}P_{\mathrm{si}}/\sigma^2_{\mathrm{n}}},\sqrt{2V_{\mathrm{T}}/\sigma^2_{\mathrm{n}}}\right). \quad (21)$$

In order to calculate the probability of missed detection under deterministic interference for an individual energy detector, the signal-and-interference to noise ratio must be considered instead of the signal-to-noise ratio (SNR). So that (18) becomes

$$P^{\mathrm{SI}}_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},\rho_l) = 1-Q_{N_{\mathrm{d}}}\left(\sqrt{2\gamma},\sqrt{2V_{\mathrm{T}}/\sigma^2_{\mathrm{n}}}\right), \quad (22)$$

and where γ is the signal-and-interference to noise ratio of the superposed signal-of-interest and interference signals as

$$\gamma=\frac{P_{\mathrm{r}}+P_{\mathrm{si}}+\sqrt{P_{\mathrm{r}}P_{\mathrm{si}}}\Re\{\rho_l\}}{\sigma^2_{\mathrm{n}}}, \quad (23)$$

where $\Re\{\}$ denotes the real part of a complex-valued variable and ρ_l is the correlation coefficient between the signal-of-interest $x_{m,l}$ and interference j_m that for frequency-swept interference can be estimated using Proposition 5.

The probability of missed detection using logical-OR without interference is given by the probability of independent events that the signal-of-interest is missed in the channel where it exists and a false alarm does not occur in any other channels as in (16). When a deterministic interference and signal-of-interest are in the same channel this probability becomes

$$P^{\mathrm{SI,1}}_{\mathrm{MD,R}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M,\rho_l) = P^{\mathrm{SI}}_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},\rho_l) \cdot\left(1-P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right)^{M-1}. \quad (24)$$

If both occupy different channels, the probability becomes

$$P^{\mathrm{SI,2}}_{\mathrm{MD,R}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M) = P_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{r}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\cdot\left(1-P^{\mathrm{SI}}_{\mathrm{FA}}(N_{\mathrm{d}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right) \cdot\left(1-P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right)^{M-2}. \quad (25)$$

With uniform frequency hopping, the probability that interference and remote control signal are in the same channel is $1/M$ and the overall probability of missed detection is

$$P^{\mathrm{SI}}_{\mathrm{MD,R}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M,\rho_l) = \frac{1}{M}P^{\mathrm{SI,2}}_{\mathrm{MD,R}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M) + \frac{M-1}{M}P^{\mathrm{SI,1}}_{\mathrm{MD,R}}(N_{\mathrm{d}},P_{\mathrm{r}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M,\rho_l). \quad (26)$$

The probability of a FD counter-drone system with logical-OR energy detector missing a jamming opportunity under wideband frequency-swept interference is therefore given by substituting (26) into (20) in place of the SI-affected terms.

The probability of false alarm when using logical-OR without interference is given by the probabilities that in none of the channels a false alarm occurs [34]

$$P_{\mathrm{FA,R}}\left(N_{\mathrm{d}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right)=1-\left(1-P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right)^M. \quad (27)$$

With interference, which for the integration time stays within a single channel, the probability of false alarm for that channel is given by (21) and the logical-OR result becomes

$$P^{\mathrm{SI}}_{\mathrm{FA,R}}\left(N_{\mathrm{d}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}},M\right) = 1-\left(1-P^{\mathrm{SI}}_{\mathrm{FA}}(N_{\mathrm{d}},P_{\mathrm{si}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right) \cdot\left(1-P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma^2_{\mathrm{n}},V_{\mathrm{T}})\right)^{M-1}. \quad (28)$$

Proposition 5. *Correlation coefficient between a BFSK signal and frequency-swept interference can be estimated from*

$$\rho_l\left(\omega_{\mathrm{j}},\omega_\Delta,\theta,c,T\right)=\exp\left(i\theta-i\frac{\left(\omega_{\mathrm{j}}+l\omega_\Delta\right)^2}{2c}\right) \left(\frac{1+i}{2}\right)\sqrt{\frac{\pi}{c}}\left(\operatorname{erf}\left(\frac{\left(1-i\right)\left(\omega_{\mathrm{j}}+l\omega_\Delta\right)}{2\sqrt{c}}\right)- \operatorname{erf}\left(\frac{\left(1-i\right)\left(cT+\omega_{\mathrm{j}}+l\omega_\Delta\right)}{2\sqrt{c}}\right)\right), \quad (29)$$

where erf *is the complex error function [30, eq. 7.1.1].*

Proof. Correlation of a tone and frequency-swept signal is

$$\rho_l=\int_0^T\exp\left(i\left(ct^2/2+\omega_{\mathrm{j}}t+\theta\right)\right)\exp\left(-il\omega_\Delta t\right)\mathrm{d}t \quad (30)$$

$$=\int_0^T\exp\left(i\left(ct^2/2+\left(\omega_{\mathrm{j}}-l\omega_\Delta\right)t+\theta\right)\right)\mathrm{d}t. \quad (31)$$

Using rule [35, eq. (5.A2)], this simplifies to

$$\rho_l = \exp\left(i\theta - i\frac{(\omega_\mathrm{j}+l\omega_\Delta)^2}{2c}\right)\left(\frac{1+i}{2}\right)\sqrt{\frac{\pi}{c}} \operatorname{erf}\left(\frac{(1-i)\,(ct+\omega_\mathrm{j}+l\omega_\Delta)}{2\sqrt{c}}\right)\Bigg|_0^T \quad (32)$$

that evaluated from 0 to T results in (29). □

Since frequency-swept interference can have any frequency and phase offsets, the overall missed detection probability for an individual radiometer is obtained by averaging the phase θ over interval $(0, 2\pi)$ and frequency ω_j over the relevant interval.

B. Demodulation

In order to evaluate the demodulation BER under interference, the challenge becomes to determine the probability by which one Rician random variable fluctuates above another. It has been previously shown that for uncorrelated Rician random variables, i.e., orthogonal BFSK, this probability can be calculated using

$$P_\mathrm{e}(N_\mathrm{d}, P_\mathrm{r}, \sigma_\mathrm{n}^2, \rho) = \frac{1}{2}\left[1 + Q_1\left(\sqrt{b}, \sqrt{a}\right) - Q_1\left(\sqrt{a}, \sqrt{b}\right)\right], \quad (33)$$

where variables a and b denote the ratios between the deterministic and nondeterministic signal components in either of the BFSK branches such as $a = N_\mathrm{d}P_\mathrm{r}/\sigma_\mathrm{n}^2$ and $b = 0$ for $x_{m,-1}$ transmitted [36]. In case of correlated Rician variables, i.e. nonorthogonal BFSK, the variables must first be decorrelated [36], resulting in

$$a = \frac{N_\mathrm{d}P_\mathrm{r}}{2\sigma_\mathrm{n}^2}\left(1 + \sqrt{1-|\rho|^2}\right) \qquad b = \frac{N_\mathrm{d}P_\mathrm{r}}{2\sigma_\mathrm{n}^2}\left(1 - \sqrt{1-|\rho|^2}\right)$$

where $\rho = |\rho|e^{i\alpha}$ is the correlation coefficient between $x_{m,-1}$ and $x_{m,+1}$.

Proposition 6. *The probability of bit error for noncoherent BFSK demodulator under deterministic interference, a signal with known form and energy, is*

$$P_\mathrm{e}^\mathrm{I}\left(N_\mathrm{d}, P_\mathrm{r}, P_\mathrm{i}, \sigma_\mathrm{n}^2, \rho, \rho_l\right) = \frac{1}{2}\left[1 + Q_1\left(\sqrt{b_l}, \sqrt{a_l}\right) - Q_1\left(\sqrt{a_l}, \sqrt{b_l}\right)\right], \quad (34)$$

where

$$a_l = \frac{P_\mathrm{i}N_\mathrm{d}}{4\sigma_\mathrm{n}^2\left(|\rho|+1\right)}\big(\left(C+\rho_l\right)\left(\beta+1\right)e^{i\alpha} - \left(\beta-1\right)\left(C\rho+\rho_{-l}\right)\big)^2 e^{-2i\alpha}, \quad (35)$$

$$b_l = \frac{P_\mathrm{i}N_\mathrm{d}}{4\sigma_\mathrm{n}^2\left(|\rho|+1\right)}\big(-\left(C+\rho_l\right)\left(\beta-1\right)e^{i\alpha} + \left(\beta+1\right)\left(C\rho+\rho_{-l}\right)\big)^2 e^{-2i\alpha}, \quad (36)$$

$C = \sqrt{P_\mathrm{r}/P_\mathrm{i}}$ *and* $\beta = \sqrt{(1+|\rho|)\,/\,(1-|\rho|)}$.

Proof. The underlying correlated Rician random variables of the test statistics are $Y_{-1} = v_{-1}^* y_m/\sigma_\mathrm{n}^2$ and $Y_{+1} = v_{+1}^* y_m/\sigma_\mathrm{n}^2$. The means of those correlated variables are $\langle y_1\rangle = \sqrt{P_\mathrm{r}}\sigma_\mathrm{n}(1+\frac{\rho_l}{C})$ and $\langle y_2\rangle = \sqrt{P_\mathrm{r}}\sigma_\mathrm{n}(\rho+\frac{\rho_{-l}}{C})$. In [36] the decorrelation transformation is given by

$$\langle x_1\rangle = \langle y_1\rangle\left(1+\beta\right)b + \langle y_2\rangle(1-\beta)be^{-i\alpha}, \quad (37)$$

$$\langle x_2\rangle = \langle y_1\rangle\left(1-\beta\right)b + \langle y_2\rangle(1+\beta)be^{-i\alpha}, \quad (38)$$

where $b = \frac{1}{\sqrt{4\beta}}$. Applying the transformation, we get

$$\langle x_1\rangle = \frac{\sqrt{P_\mathrm{r}}\sigma_\mathrm{n}}{2C\sqrt{\beta}}\big(\left(C+\rho_l\right)\left(\beta+1\right)e^{i\alpha} - \left(\beta-1\right)\left(C\rho+\rho_{-l}\right)\big)e^{-i\alpha}, \quad (39)$$

$$\langle x_2\rangle = \frac{\sqrt{P_\mathrm{r}}\sigma_\mathrm{n}}{2C\sqrt{\beta}}\big(-\left(C+\rho_l\right)\left(\beta-1\right)e^{i\alpha} + \left(\beta+1\right)\left(C\rho+\rho_{-l}\right)\big)e^{-i\alpha}. \quad (40)$$

Resultingly, variance of the newly created uncorrelated complex Gaussian variables is $\sigma_{x_1}^2 = \sigma_{x_2}^2 = 4b^2(1+\rho)$ [37, pp. 226–231] and therefore arguments of the Q-function in (33) are given by $\frac{\langle x_1\rangle^2}{4b^2(1+\rho)}$ and $\frac{\langle x_2\rangle^2}{4b^2(1+\rho)}$ that result in (35) and (36). Thus, the probability of bit error is (34). □

Again, ρ_l can be calculated using (29). The overall probability of bit error is obtained by averaging the phase θ over region $(0, 2\pi)$ and frequency ω_j over the relevant interval. Note that Proposition 6 relies on solving the canonical problem proposed in [36], which itself relies on transforming the received signal to that canonical model. Using a modulation other than BFSK would require that transformation step to be retailored. However, if an appropriate transform was found, then the canonical solution along with its extensions could be used for other modulation schemes in place of the BFSK. Still, the approach used herein does not limit the practicality of this work, since BFSK is widely used in drone systems [38], [39]. Furthermore, while different modulation schemes would affect the absolute values obtained in the following numerical analysis, they are not expected to significantly change the relative performance of the studied operation modes and strategies.

C. Duplex Comparison

Fig. 6 illustrates how the propositions can be used to estimate, depending on the operation mode and strategy of the counter-drone system, the probability that a counter-drone system misses a jamming opportunity and, consequently, what will be the average BER at either the drone or remote controller. Here, we use the propositions to analytically characterise the remote control link reliability in the presence of a follower counter-drone system. The BER of a receiver under attack from HD and FD follower counter-drone systems, as per Fig. 6, are respectively

$$P_\mathrm{e,F}^\mathrm{HD}\left(N_\mathrm{d}, P_\mathrm{r}^\mathrm{J}, P_\mathrm{r}^\mathrm{D}, P_\mathrm{i}^\mathrm{D}, \sigma_\mathrm{n}^2, \rho, V_\mathrm{T}, M\right) = P_\mathrm{e}(N_\mathrm{d}, P_\mathrm{r}^\mathrm{D}, \sigma_\mathrm{n}^2, \rho) \cdot P_\mathrm{MJ,F}^\mathrm{HD}(N_\mathrm{d}, P_\mathrm{r}^\mathrm{J}, \sigma_\mathrm{n}^2, V_\mathrm{T}, M) + P_\mathrm{e}^\mathrm{I}(N_\mathrm{d}, P_\mathrm{r}^\mathrm{D}, 0, P_\mathrm{i}^\mathrm{D}+\sigma_\mathrm{n}^2, \rho, 0) \cdot \left(1 - P_\mathrm{MJ,F}^\mathrm{HD}(N_\mathrm{d}, P_\mathrm{r}^\mathrm{J}, \sigma_\mathrm{n}^2, V_\mathrm{T}, M)\right) \quad (41)$$

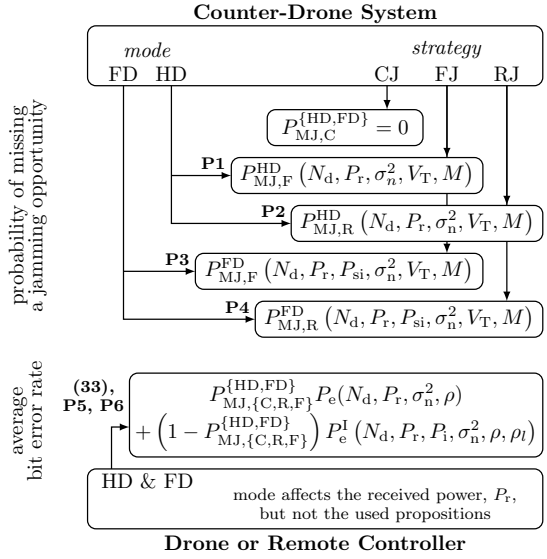


Fig. 6. Calculating the average bit error rate caused by the counter-drone system depending on its mode and strategy. **P1** refers to Proposition 1 etc.

and

$$P^{\mathrm{FD}}_{\mathrm{e,F}}\left(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{J}}_\mathrm{si}, P^{\mathrm{D}}_\mathrm{i}, \sigma^2_\mathrm{n}, \rho, V_\mathrm{T}, M\right) = P_\mathrm{e}(N_\mathrm{d}, P^{\mathrm{D}}_\mathrm{r}, \sigma^2_\mathrm{n}, \rho) \cdot P^{\mathrm{FD}}_{\mathrm{MJ,F}}(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{J}}_\mathrm{si}, \sigma^2_\mathrm{n}, V_\mathrm{T}, M) + P^{\mathrm{I}}_\mathrm{e}(N_\mathrm{d}, P^{\mathrm{D}}_\mathrm{r}, 0, P^{\mathrm{D}}_\mathrm{i} + \sigma^2_\mathrm{n}, \rho, 0) \cdot \left(1 - P^{\mathrm{FD}}_{\mathrm{MJ,F}}(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{J}}_\mathrm{si}, \sigma^2_n, V_\mathrm{T}, M)\right). \quad (42)$$

where the superscripts D and J denote the received power by drone and counter-drone system respectively.

To highlight the differences of HD and FD counter-drone system operation modes in (41) and (42), we can consider the special case where both the counter-drone system and remote-controlled drone have good SNR of the remote control signal so that $P^{\mathrm{J}}_\mathrm{r} \gg \sigma^2_\mathrm{n}$ and $P^{\mathrm{D}}_\mathrm{r} \gg \sigma^2_\mathrm{n}$, while the counter-drone system also has good SINR $P^{\mathrm{J}}_\mathrm{r} \gg P^{\mathrm{J}}_\mathrm{si}$ and a nonzero CFAR. This altogether yields asymptotic BERs

$$P^{\mathrm{HD}}_{\mathrm{e,F}}\left(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{i}, \sigma^2_\mathrm{n}, \rho, V_\mathrm{T}, M\right) \approx \frac{1}{2} P_\mathrm{e}(N_\mathrm{d}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{i} + \sigma^2_\mathrm{n}, \rho) \quad (43)$$

and

$$P^{\mathrm{FD}}_{\mathrm{e,F}}\left(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{J}}_\mathrm{si}, P^{\mathrm{D}}_\mathrm{i}, \sigma^2_\mathrm{n}, \rho, V_\mathrm{T}, M\right) \approx P_\mathrm{e}(N_\mathrm{d}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{i} + \sigma^2_\mathrm{n}, \rho). \quad (44)$$

The asymptotic results in (43) and (44) emphasise the fundamental difference between the two operation modes — a counter-drone system in FD mode can inflict double the BER compared to that in HD mode.

Even if we do not assume that the signal received by the counter-drone system is more powerful than the SI, then still the FD system has an advantage over its HD counterpart due to the FD system's ability to more often react to false alarms. To explain this, assume that the SI at the counter-drone system is much more powerful than the signal-of-interest and the power of SI approaches infinity $P^{\mathrm{J}}_\mathrm{si} \to \infty$, while the other assumptions stay the same. Then the asymptotic BER inflicted by the FD counter-drone system becomes

$$P^{\mathrm{FD}}_{\mathrm{e,F}}\left(N_\mathrm{d}, P^{\mathrm{J}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{J}}_\mathrm{si}, P^{\mathrm{D}}_\mathrm{i}, \sigma^2_\mathrm{n}, \rho, V_\mathrm{T}, M\right) \approx \frac{1}{2 - \frac{1-(1-P_\mathrm{FA}(N_\mathrm{d}, \sigma^2_\mathrm{n}, V_\mathrm{T}))^M}{M}} P_\mathrm{e}(N_\mathrm{d}, P^{\mathrm{D}}_\mathrm{r}, P^{\mathrm{D}}_\mathrm{i} + \sigma^2_\mathrm{n}, \rho), \quad (45)$$

which means that as longs as the system's CFAR is nonzero, the system occasionally uses the FD-provided time slot for jamming the correct channel and, therefore, (45) results in larger BER than (43). This is illustrated in Fig. 7 at different false alarm probabilities and with different number of channels but assuming that $P^{\mathrm{D}}_\mathrm{i} \gg P^{\mathrm{D}}_\mathrm{r}$. The comparisons show that the FD counter-drone system always outperforms its HD counterpart, doubling the BER in favourable conditions.

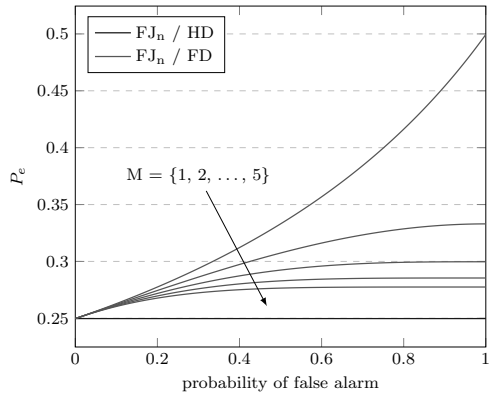


Fig. 7. Asymptotic comparison of follower counter-drone systems.

While we considered the follower counter-drone system, similar comparisons and conclusions can be drawn for the other strategies. However, to truly recognize the differences of the two operation modes, it is important to consider how significant the impact of BER doubling is and when it is achievable. Doing so using analytical comparisons is challenging due to the intricate expressions and large number of parameters. As such, we present the following numerical results for comprehensive insight that includes comparing the performance across different strategies.

IV. Results and Analysis

We compare the advantages and disadvantages of FD and HD in three different scenarios. We consider that the three nodes operate as described in Section II and we use the propositions developed in Section III to evaluate the performance of these nodes in different operation modes and strategies. In the first scenario, we evaluate the counter-drone system's ability to minimize the area into which a remote-controlled drone can intrude (i.e., minimizing the intrusion

area). In the second scenario, we consider the drone's ability to maximize the area in which it can operate in the presence of a malicious counter-drone system (i.e., maximizing the operable area). In the third scenario, we study the drone's ability to detect malicious interference at ineffective levels to prevent entering areas in which the interference would become effective. Table I summarizes operation configurations of the three devices (remote controller (RC), drone (UAV), and counter-drone system (CDS)) in the considered scenarios. The highlighted background in the table's some cells indicates the comparison in question for any given scenario. The table also summarizes the outcomes of the comparisons, which will be covered scenario-by-scenario in detail in Sections IV-B, IV-C, and IV-D, respectively. Finally, we also analyse the energy efficiency of different counter-drone system strategies and the effect of elevation.

TABLE I
SUMMARY OF SCENARIOS

	Transmit	Receive	Interfere	Detect	Device	Outcome of Using FD
1	HD	HD			RC	increased effective area
	HD	HD			UAV	
			HD/FD	HD/FD	CDS	
2	HD/FD	HD/FD			RC	reduced operable area
	HD/FD	HD/FD			UAV	
			HD/FD	HD/FD	CDS	
3	HD	HD			RC	increased detection range
	HD/FD	HD		HD/FD	UAV	
			HD/FD	HD/FD	CDS	

In Scenario 1, the counter-drone system either detects and interferes intermittently (HD) or simultaneously (FD), the latter resulting in an improved effective area for the counter-drone system. In Scenario 2, the drone and remote controller either communicate intermittently (HD) on the same frequency or simultaneously (FD), the latter resulting in a reduced operable area for the drone. In Scenario 3, the drone either transmits in one channel and detects jamming in the other channels (HD) or it also simultaneously detects jamming in the channel it is transmitting in (FD), the latter increasing the drone's capability to detect the intentional interference from the counter-drone system. Conclusively, both Scenarios 1 and 3 benefit from the FD operation mode, whereas Scenario 2 does not.

The following parameters are used in the system model to represent realistic devices and environments. The parameter values do not strictly correspond to specific systems, but are close to what can be found in many remote-controlled drone and counter-drone systems [38], [39]. The total bandwidth used by the remote control link is taken to be $80\,\mathrm{MHz}$ and it is divided into 160 equally spaced channels with bandwidths of $0.5\,\mathrm{MHz}$. The remote controller and drone transmit BFSK signal with frequency deviation of $200\,\mathrm{kHz}$, encoded data rate $25\,\mathrm{kbps}$, and frequency hopping rate of 40 hops per second.

The remote controller and drone both have transmit output powers of $20\,\mathrm{dBm}$ in HD mode, while the counter-drone system has an output power of $40\,\mathrm{dBm}$ regardless of the operation mode. The drone system halves its output power in FD mode to retain the same energy-per-bit ratio as in HD mode, while the counter-drone system uses always the highest possible output power to maximise its impact. For frequency sweep jamming, $2.5\,\mathrm{kHz}$ sweep rate is used, meaning that the interference covers 16 channels during a single bit transmission in HD mode, giving a good chance of high BER even at low jammer-to-signal ratios (JSRs). The noise floor in a $0.5\,\mathrm{MHz}$ channel is taken to be $-90\,\mathrm{dBm}$. Both the signal detection and jamming times are taken to be $1.6\,\mathrm{ms}$, hence the HD counter-drone system uses a 50% duty cycle.

We consider the radio link between the remote controller and drone to be functional as long as the channel-BER in both ways is less than 1% (i.e., $P_{\mathrm{T}} = 0.01$). The area coverable by the drone in which that constraint is satisfied will be referred to as the operable area. Conversely, for a drone and its remote controller at fixed positions, the area in which the counter-drone system is able to force the channel-BER between the drone and its remote controller over 1% in either direction will be referred to as the counter-drone system's effective area. With a moderate coding rate, a below 1% channel-BER would allow to reach an information-BER that suffices for the repetitive nature of drone remote control. For example, using Golay (23, 12) code and relying on (5), the channel-BER of 1% allows to reach information-BER of about 10^{-5} after decoding.

The drone is assumed to operate at an elevation of $100\,\mathrm{m}$ above ground level, while the other nodes are at ground level unless stated otherwise. The ground-to-air channel between the remote controller and the drone is in practice clearly distinguishable from the conventional ground-to-ground channel between the remote controller and the counter-drone system [40]. Furthermore, a third, air-to-air, channel model is required if any two of the three nodes are in the air. Therefore, in order take these differences into account, we rely on empirical studies that have characterized the air-to-air, ground-to-air, and ground-to-ground channels in wireless drone communications, and take the path loss exponents in those channels to be 2.0, 2.2, and 3.3 respectively [41], [42].

A. Verification of Analytical Expressions

Before using the analysis techniques developed in Section III for studying the three scenarios, we first verify their accuracy in comparison to simulated results. We begin by checking the probabilities of correct detection and false alarm by the counter-drone system in FD and HD mode (i.e., with and without SI). Using Propositions 1 through 4, we have evaluated the receiver operating characteristic (ROC) curves and plotted them together with the simulated results in Fig. 8. The reactive jammer with noise ($\mathrm{RJ_n}$) or frequency-swept interference ($\mathrm{RJ_s}$) is guaranteed to correctly detect the presence of the signal-of-interest with low enough threshold, while the follower jammer ($\mathrm{FJ_n}$) is not guaranteed to choose the correct channel which is why the probability of correct detection for the follower jammer is lower than for the other schemes in Fig. 8. Also, we observe flattening of the ROC curves as the

residual SI level increases when using noise as interference, but not when using a deterministic signal. Overall, the results indicate that the estimations are closely matched with the simulations.

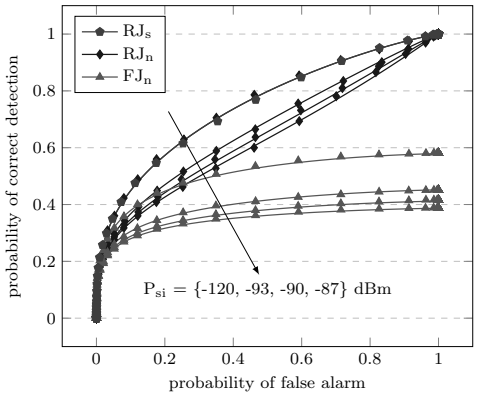


Fig. 8. Receiver operating characteristic curves of the counter-drone system with different detection strategies and at varying levels of self-interference. Solid lines represent the analytical and marks the simulated results.

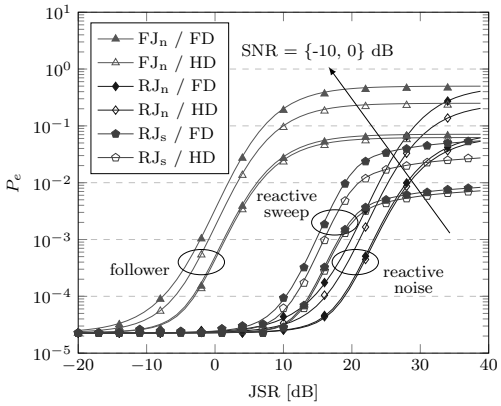


Fig. 9. Bit error rate at a frequency-hopped BFSK receiver under reactive or follower jamming at different SNRs at the counter-drone system. The detection threshold at the counter-drone system is chosen so that the false alarm rate is 1%. Solid lines represent the analytical and marks the simulated results.

With confidence in detection estimation accuracy, we present the demodulation results by building on the detection analysis. That is, we compare the estimated and simulated channel-BERs at the drone, whereas the counter-drone system is first required to detect the signal transmitted by the remote controller. Using additionally Propositions 5 and 6, we estimate the BER at the drone depending on the strategy and mode of the counter-drone system. The results are presented in Fig. 9. As expected, follower jamming becomes effective at lower JSRs than reactive jamming because it is able to overcome the processing gain of frequency hopping. Also, reactive frequency-swept interference has the potential to become effective at lower JSRs than reactive noise jamming, since the interference is concentrated to just 10% of the total bandwidth during a single symbol transmission. Similarly, FD operation mode becomes effective at lower JSRs than HD because it is able to spend more time in jamming mode.

It is interesting to note that, as the SNR at the counter-drone system worsens, the performance difference between FD and HD counter-drone system diminishes. That is because the FD system stops taking advantage of its ability to jam continuously due to the missed detections. Together the results in Fig. 8 and Fig. 9 cover the analysis techniques presented in Section III and indicate a good match between estimated and simulated results. This allows us to confidently present the following scenarios relying purely on the analytical functions. Using the analytical functions is significantly less computing intensive than running simulations, especially considering the vast amount of data points that will be considered next to cover the scenarios.

B. Scenario 1 (Minimizing Intrusion Area)

In the first scenario, we consider a defensive counter-drone system as illustrated in Fig. 10. The counter-drone system is positioned in front of an area that is to be restricted to drones. This could be, e.g., national border, prison or airport perimeter. The drone operator aims to control the drone to enter the area behind the counter-drone system and the counter-drone system aims to minimize the area behind itself in which the drone can be remote-controlled. Using all of the derived analytical functions in alignment with Fig. 6, we study which counter-drone system strategies and operation modes are most efficient in reducing the intrusion area. That is, for the given remote controller and counter-drone system positions, modes and strategies, BERs at the drone and remote controller are evaluated for all the possible drone positions in that area, and operable area is taken to be that where the BER at both the drone and remote controller remains below 1%. The operable area depends on the position of the remote controller relative to the counter-drone system and Fig. 10 illustrates how the different strategies and operation modes limit the operable area of the remote-controlled drone at different remote controller positions. The illustration shows that FD operation outperforms HD to some extent in any case due to more time spent jamming, but the efficiency of the different strategies is a more significant factor than the operation mode.

In Fig. 11, the area that can be covered by a malicious drone behind a counter-drone system is plotted for different jamming strategies and modes depending on the remote controller's distance from the counter-drone system. Due to the differences in the ground-to-air and ground-to-ground channels, the counter-drone system is at a significant disadvantage compared to the drone when detecting the remote control signals. As such, when the remote controller is far away from the counter-drone system, i.e., the remote control signal received by the counter-drone system is weak, constant jamming outperforms other strategies. Of course this increases the detectability of the counter-drone system. If detectability is not a concern, then

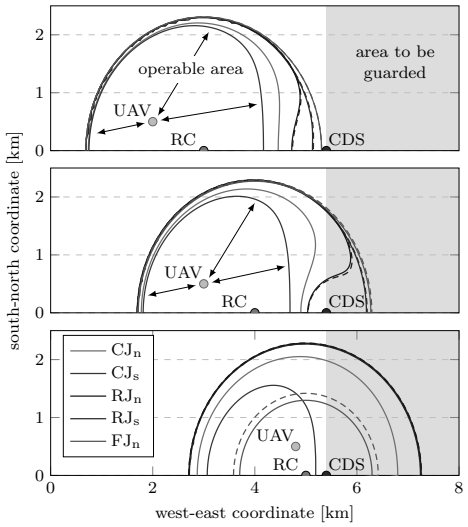


Fig. 10. Operable area of a remote-controlled drone against a counter-drone system. Results for counter-drone system in FD mode are plotted in solid lines and HD in dashed lines.

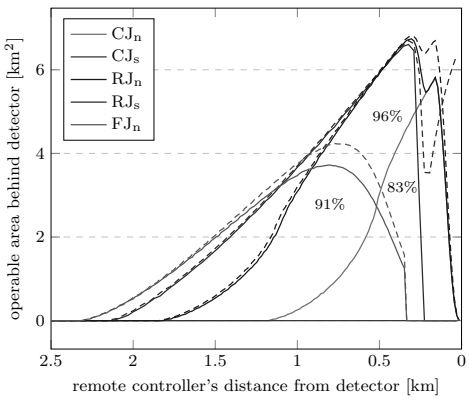


Fig. 11. Area behind the counter-drone system in which a malicious drone can be controlled. The reactive and follower jammers are operated with a constant false alarm rate of 10%. Results for FD counter-drone system are plotted in solid lines and HD in dashed lines.

using constant jamming and switching to follower jamming after confidently detecting the remote control signals would be the optimal strategy for reducing the operable area. It is also evident that, compared to HD reactive and follower jammers, their FD counterparts reduce the operable area somewhat. Depending on the strategy, the operable area is reduced by 4% to 17%. This is due to the FD counter-drone system being able to spend more time in jamming mode than its HD counterpart. Resultantly, as hinted in Table I, FD operation mode allows to improve the efficiency of the counter-drone system.

C. Scenario 2 (Maximizing Operable Area)

In the second scenario, we consider the defensive drone point of view and trying to extend the area that a drone can survey as illustrated in Fig. 12. The malicious counter-drone system aims to neutralize the drone in order to carry out some activity in the surveyed area unseen and the drone aims to maximize the area in which it can operate. Given that the counter-drone system is either HD or FD and uses some neutralization strategy, the question then is which operation mode between the remote controller and drone is most beneficial from the drone's perspective. We consider that the remote controller and drone use the same energy per bit ratio in both FD and HD operation modes. That is, in FD mode the symbol transmission time is doubled but the transmission power is halved compared to the HD mode.

Fig. 12 gives results for some node placements. The actual area in which the drone can be remote-controlled decreases as the counter-drone system approaches the remote controller. Due to the different channel models, if the drone is transmitting and receiving at the same time (i.e., FD mode), it becomes a much easier target than in the HD time division mode when the counter-drone system needs to detect the signals from the remote controller. Therefore, using FD for two-way communications between the remote controller and drone make the drone system highly vulnerable to jamming attacks. Fig. 13 gives the operable areas as depending on the counter-drone system's distance from the remote controller. The operable area in FD mode can be reduced to as little as couple percent of that in HD mode. That is, using FD operation mode instead of HD for two-way communications reduces the operable area of the drone when under attack from a counter-drone system (cf. Table I). The results highlight the relative vulnerability of FD two-way communications between a drone and its remote controller compared to HD operation. This is a considerable issue that affects many potential FD drone applications.

D. Scenario 3 (Detecting Counter-Measures)

In the third scenario, we analyze the drone's ability to detect intentional interference from the counter-drone system. In practice, this could help to make sure that the drone does not enter the area in which it would be immobilized and this could again be applicable in a situation where the drone is surveying an area. The counter-drone system aims to disable the drone in order to reduce the situational awareness about the area and the drone aims to avoid becoming disabled by detecting the counter-measures applied by the adversarial counter-drone system. In this scenario we only consider the follower jammer, which can be the most difficult to detect.

Fig. 14 illustrates the scenario — the drone is positioned at a distance from the remote controller, leaving it to be vulnerable to jamming attacks. For every viable counter-drone position, the propositions from Section III are then used to evaluate probability that the counter-drone system detects and correctly jams the remote control link, the BER that this jamming inflicts, and the probability by which the drone can detect the follower jamming. The effective jamming area, in

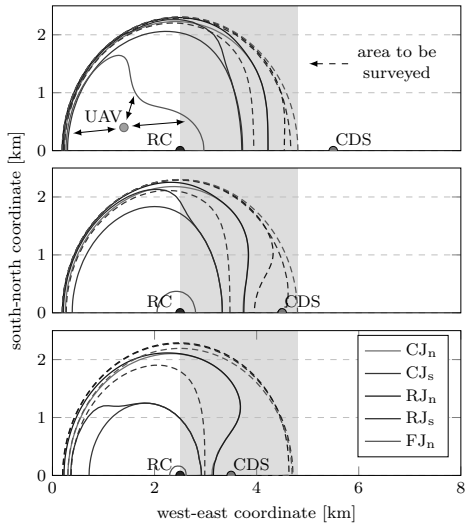


Fig. 12. Area in which a drone can be controlled. The reactive and follower jammers are operated in FD mode with a constant false alarm rate of 10%. Solid lines represent operable area in FD remote control mode and dashed lines in HD mode.

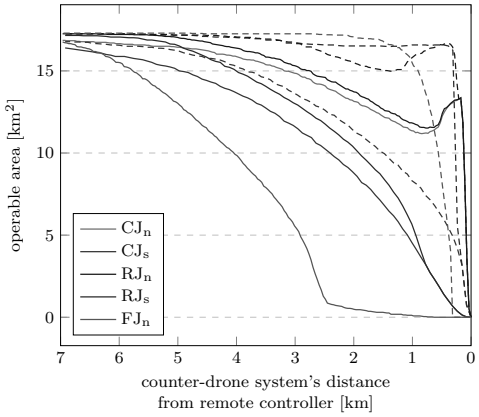


Fig. 13. Illustration of the area in which a drone can be controlled. The reactive and follower jammers are operated in FD mode with a constant false alarm rate of 10%. Solid lines represent operable area in FD remote control mode and dashed lines in HD mode.

which the counter-drone system needs to be positioned to push the BER at the drone or remote controller above 1%, is shown in red. The counter-drone system detection area, in which the counter-drone system needs to be positioned so that the drone can detect it, is shown in blue. The results show that jamming detection in FD mode can lead to up to 60% increase of the detection area compared to HD mode. The FD-enhanced drone has a considerable advantage over its HD-limited counterpart because simultaneous transmission and detection capability allows to detect the jamming attacks more consistently. Without that capability, HD drone is limited to detecting the counter-drone system's attacks only when the counter-drone system targets a wrong channel or is too late with its attack against a recently vacated channel. As such, jamming detection in FD mode is more certain to be able to detect the malicious interference before becoming immobilized by it. Depending on the direction from which the counter-drone system approaches, HD detection might miss the adversary altogether before becoming paralyzed.

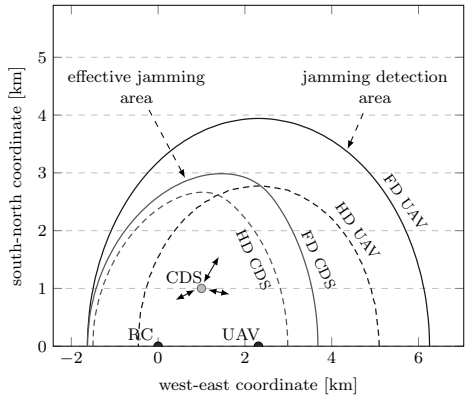


Fig. 14. Jamming detection by drone systems with HD and FD capabilities. For illustration, the effective jamming area is also plotted, which allows to get some sense about the drone's capability to detect ineffective interference and avoid entering an area where interference becomes effective.

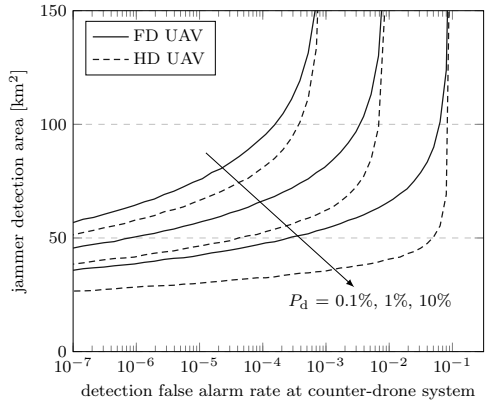


Fig. 15. Comparison of areas in which HD and FD drone system can detect a counter-drone system that is using the follower jamming strategy. The area depends on the detection thresholds at either node and the operation mode.

In Fig. 15, counter-drone system detectability is plotted depending on the false alarm rate used by the counter-drone system. Furthermore, P_{d} is the target detection rate at the drone, i.e., the percentage of jamming attempts that are required to be detected. As the counter-drone system lowers its detection threshold, it becomes less discerning about the channels that it attacks and consequently becomes detectable

from a greater distance. Conclusively, enhancing the drone with FD signal detection capabilities simultaneously to feedback signal transmission considerably improves its ability to detect interference from the counter-drone system (cf. Table I).

E. Energy Efficiency and Elevation

Since high-power jamming consumes a lot of energy, it could be beneficial to take into account the energy efficiency of different counter-drone strategies. For example, constant jamming strategy is clearly the most wasteful when there are no malicious drones. In this work we simplify the analysis and consider only the time when the threat has realised (i.e., there is a drone in the vicinity). Fig. 16 shows the drone's operable area reduction divided by the counter-drone system's average output power (i.e., the energy efficiency). It can be observed that FD operation facilitates doubling the jamming energy consumption over HD operation. However, this does not unfortunately result in equivalent reductions in the drone's operable area. When looking at the area that the counter-drone system is able to protect at given energy consumption, the HD operation mode utilises the energy more efficiently. This is reasonable, because after the 1% BER threshold is crossed, there is no benefit to increasing the BER any further by using more energy. Furthermore, follower jamming can be the most energy efficient strategy, but that requires the nodes to be positioned so that the follower jammer is able to target the correct channels.

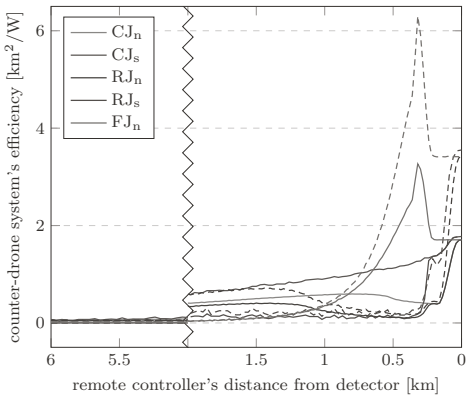


Fig. 16. Energy efficiency of counter-drone systems with different strategies and operation modes.

One of the main characteristics that separates drone and general physical-layer reliability studies is the difference in the air-to-air, ground-to-air, and ground-to-ground channels. Specifically, the ground-to-air channel between a drone and its remote controller is much less prone to degradation than the ground-to-ground channel between a typical counter-drone system and a remote controller. So far, we have assumed that the counter-drone system is on the ground, which is a fair assumption considering practical systems. However, it is plausible that the counter-drone system be elevated (using, e.g., a tethered drone or antenna tower) to an altitude similar as the drone. This would level the playing field. In Fig. 17, we compare the counter-drone system's performance when on the ground and elevated to the same altitude as the drone. The results show that an airborne counter-drone system outperforms a terrestrial system regardless of the operation mode and strategy. However, by lifting the counter-drone system, also the relative performance of different strategies changes. For example, follower jamming becomes most efficient.

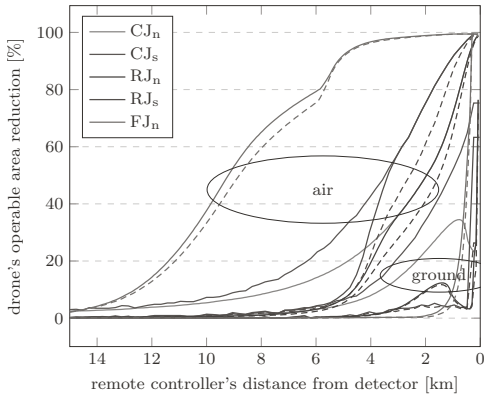


Fig. 17. Performance of the counter-drone system from ground and air.

V. Conclusions

In this article, we have presented a systematic approach for the reliability analysis of remote-controlled drones and counter-drone systems operating in FD and HD modes. We developed analytical tools to evaluate the detection and demodulation probabilities of frequency-hopped BFSK with channelized energy detectors and noncoherent demodulators under adversarial or self-induced interference. We verified the analytical methods through comparison to simulated results and then used the methods to study three different scenarios, showing what can be expected to be the actual impact of either operation mode in terms of the coverage or operation area. Analysis of the three scenarios showed that FD radio technology has clear benefits in remote-controlled drone and counter-drone systems. Specifically, FD operation mode can improve the effectiveness of counter-drone systems and allows drone systems to detect interference from the counter-drone system at a greater distance. However, there are also potential drawbacks to using FD over HD operation mode, especially in two-way communications. That is because FD operation between a remote controller and drone simplifies targeting that link for the counter-drone system, resulting in significantly reduced operable area for the drone, although achieving better spectral efficiency.

References

[1] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] K. Pärlin, T. Riihonen, V. Le Nir, M. Bowyer, T. Ranstrom, E. Axell, B. Asp, R. Ulman, M. Tschauner, and M. Adrat, "Full-duplex tactical information and electronic warfare systems," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 73–79, Aug. 2021.

[3] T. Riihonen, D. Korpi, M. Turunen, and M. Valkama, "Full-duplex radio technology for simultaneously detecting and preventing improvised explosive device activation," in *Proc. International Conference on Military Communications and Information Systems*, May 2018.

[4] K. Pärlin, T. Riihonen, G. Karm, and M. Turunen, "Jamming and classification of drones using full-duplex radios and deep learning," in *Proc. International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2020.

[5] N. Ebrahimi, H.-S. Kim, and D. Blaauw, "Physical layer secret key generation using joint interference and phase shift keying modulation," *IEEE Trans. Microw. Theory Tech.*, vol. 69, no. 5, pp. 2673–2685, May 2021.

[6] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[7] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[8] M. Abughalwa, L. Samara, M. O. Hasna, and R. Hamila, "Full-duplex jamming and interception analysis of UAV-based intrusion links," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1105–1109, May 2020.

[9] M. Abughalwa and M. O. Hasna, "A secrecy study of UAV based networks with fountain codes and FD jamming," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1796–1800, Jun. 2021.

[10] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

[11] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, Mar. 2019.

[12] B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV communication networks over 5G," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 114–120, Oct. 2019.

[13] L. Zhang and N. Ansari, "A framework for 5G networks with in-band full-duplex enabled drone-mounted base-stations," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 121–127, Oct. 2019.

[14] H. Wang, J. Wang, G. Ding, J. Chen, Y. Li, and Z. Han, "Spectrum sharing planning for full-duplex UAV relaying systems with underlaid D2D communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1986–1999, Sep. 2018.

[15] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, M. Guizani *et al.*, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad hoc networks*, vol. 111, Feb. 2021.

[16] J. Wang, Y. Liu, and H. Song, "Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–29, Mar. 2021.

[17] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[18] X. Lu, L. Xiao, C. Dai, and H. Dai, "UAV-aided cellular communications with deep reinforcement learning against jamming," *IEEE Wireless Commun. Mag.*, vol. 27, no. 4, pp. 48–53, Aug. 2020.

[19] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, and E. S. Lohan, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 249–291, Oct. 2019.

[20] H.-M. Wang, X. Zhang, and J.-C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 32–39, Oct. 2019.

[21] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[22] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[23] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[24] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[25] D. Torrieri, "The information-bit error rate for block codes," *IEEE Trans. Commun.*, vol. 32, no. 4, pp. 474–476, Apr. 1984.

[26] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security Privacy*, vol. 14, no. 1, pp. 47–54, Feb. 2016.

[27] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[28] J. Bird and E. Felstead, "Antijam performance of fast frequency-hopped M-ary NCFSK–an overview," *IEEE J. Sel. Areas Commun.*, vol. 4, no. 2, pp. 216–233, Mar. 1986.

[29] E. B. Felstead, "Follower jammer considerations for frequency hopped spread spectrum," in *Proc. Military Communications Conference*, vol. 2, Oct. 1998, pp. 474–478.

[30] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. United States Department of Commerce, National Bureau of Standards, 1964, vol. 55.

[31] A. Mizera, J. Pang, and Q. Yuan, "Reviving the two-state Markov chain approach," *IEEE/ACM Trans. Comput. Biol. Bioinformatics*, vol. 15, no. 5, pp. 1525–1537, Sep. 2018.

[32] J. Marcum, "A statistical theory of target detection by pulsed radar," *IEEE Trans. Inf. Theory*, vol. 6, no. 2, pp. 59–267, Apr. 1960.

[33] S. Atapattu, C. Tellambura, and H. Jiang, *Energy detection for spectrum sensing in cognitive radio*. Springer, Feb. 2014.

[34] L. Miller, J. Lee, and D. Torrieri, "Frequency-hopping signal detection using partial band coverage," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 29, no. 2, pp. 540–553, Apr. 1993.

[35] E. W. Ng and M. Geller, "A table of integrals of the error functions," *Journal of Research of the National Bureau of Standards*, vol. 73, no. 1, Mar. 1969.

[36] S. Stein, "Unified analysis of certain coherent and noncoherent binary communications systems," *IEEE Trans. Inf. Theory*, vol. 10, no. 1, pp. 43–51, Jan. 1964.

[37] D. W. Bliss and S. Govindasamy, *Adaptive wireless communications: MIMO channels and networks*. Cambridge University Press, May 2013.

[38] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in *Int. Conference on Military Communications and Information Systems*, May 2018.

[39] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open Journal of the Commun. Soc.*, vol. 1, pp. 60–76, Nov. 2019.

[40] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins, "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, Jul. 2018.

[41] J. Allred, A. B. Hasan, S. Panichsakul, W. Pisano, P. Gray, J. Huang, R. Han, D. Lawrence, and K. Mohseni, "Sensorflock: an airborne wireless sensor network of micro-air vehicles," in *Proc. Int. Conf. on Embedded Networked Sensor Systems*, Nov. 2007, pp. 117–129.

[42] N. Ahmed, S. S. Kanhere, and S. Jha, "On the importance of link characterization for aerial wireless sensor networks," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 52–57, May 2016.

Karel Pärlin received his M.Sc. degree in electrical engineering from Tallinn University of Technology, Estonia, in 2017. He is currently pursuing his D.Sc. degree in communication engineering at Tampere University, Finland. His research interests include adaptive signal processing, signal processing for communications, and physical layer security.

Taneli Riihonen [S'06, M'14, SM'22] received his D.Sc. degree in electrical engineering from Aalto University, Finland, in 2014. He is currently a tenure-track Associate Professor with the Faculty of Information Technology and Communication Sciences, Tampere University, Finland. His research interests include physical-layer OFDM(A), multi-antenna, multihop, and full-duplex wireless techniques with current research interest includes the evolution of beyond 5G systems.

Vincent Le Nir received his Ph.D. degree in electronics from the National Institute of Applied Sciences, France, in 2004. He is currently a senior researcher at the Royal Military Academy in Brussels, Belgium. His research interests are related to digital communications and signal processing in the wireless and wireline domains, MIMO communications, space–time coding, OFDM and multicarrier-code-division multiple-access, turbo-equalization, software defined and cognitive radio.

Marc Adrat received his Diploma and Dr.-Ing. degrees in electrical engineering from RWTH Aachen University, Germany, in 1997 and 2003, respectively. He is currently the head of the Software Defined Radio (SDR) research group at Fraunhofer FKIE in Wachtberg, Germany. His research interests include digital signal processing for mobile tactical radio communications as well as emerging technologies like in-band full-duplex communications. Since over 10 years, he is a guest lecturer at RWTH Aachen University for a course on channel coding.

PUBLICATION 7

Known-Interference Cancellation in Cooperative Jamming: Experimental Evaluation and Benchmark Algorithm Performance

K. Pärlin, T. Riihonen, M. Turunen, V. Le Nir and M. Adrat

IEEE Wireless Communications Letters 2023. In press
DOI: 10.1109/LWC.2023.3284006

Known-Interference Cancellation in Cooperative Jamming: Experimental Evaluation and Benchmark Algorithm Performance

Karel Pärlin, Taneli Riihonen, Matias Turunen, Vincent Le Nir, and Marc Adrat

***Abstract*—Physical layer security is a sought-after concept to complement the established upper layer security techniques in wireless communications. An appealing approach to achieve physical layer security is to use cooperative jamming with interference that is known to and suppressible by the legitimate receiver but unknown to, and hence not suppressible by, the eavesdropper. Suppressing known interference (KI), however, is challenging due to the numerous unknowns, including carrier and sampling frequency offsets, that impact its reception. This letter presents a measurement campaign that captures this challenge and then demonstrates the feasibility of solving that challenge by cancelling the KI using the frequency offsets least mean squares (FO-LMS) algorithm. Results show that KI suppression directly improves processing the signal-of-interest and that cooperative jamming effectively provides security at the physical layer.**

***Index Terms*—Cooperative jamming, physical layer security.**

I. Introduction

WIRELESS communications are by nature broadcast, which on one hand means that multiple receivers can receive the same transmitted signal, but on the other hand it means that one receiver can receive the superposition of multiple transmitted signals. The former results in significant concern for the security of wirelessly transmitted information because of the susceptibility to eavesdropping, while the latter causes concern about robustness because of the vulnerability to interference. In order to secure wirelessly transmitted information, encryption is typically used on the upper layers of the communication model. In general, cryptographic systems can be implemented to provide reasonable security, but their functioning does rely on secure key exchange and limited adversarial computational capabilities. As such, there is significant interest in complementing the upper layer security at the physical layer [1] and the solution to achieving physical layer secrecy is often seen to be the other side of the broadcast transmission nature — the superposition of multiple signals.

Specifically, if an interference signal can be transmitted so that it superposes the signal-of-interest at the eavesdropper but not at the intended receiver, then that could secure the transmission. This could be achieved by either having the transmitter itself or a separate cooperative jammer produce the interference, such that only the eavesdropper is affected [2]. Targeting an eavesdropper this way requires the nodes to be positioned favorably, but also that the interference transmitter is capable of directing the interference and knows how the devices are positioned. This awareness, however, can be difficult to obtain in practice, especially if the adversary is passive.

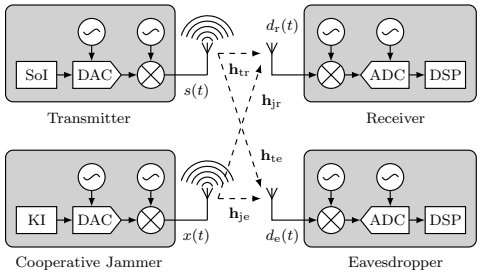


Fig. 1. System model of cooperatively jammed wireless communications.

An alternative, that does not rely on such knowledge, is to cover the whole area with interference but suppress it at the receiver. Instead, this relies on the receiver having the technological capability to cancel the interference from the total received signal and it knowing the transmitted interference signal. The latter is achieved if the receiver itself transmits the interference. This results in self-interference (SI), but that can be suppressed using SI cancellation methods as in in-band full-duplex (IBFD) radios [3]. Such interference-transmitting receivers effectively block out near-by eavesdroppers [4]. However, they also block out near-by non-adversarial nodes, unless those nodes possess known-interference cancellation (KIC) capabilities and know the interference signal. Known interference (KI) from another radio is more complicated to cancel than SI due to oscillator inaccuracies [5] and methods to do so are scarce [6]. Still, information theoretical works often assume perfect KIC [7], [8] somewhat negligently.

In this work, we help bridge that gap between theory and practice by carrying out an extensive KI measurement campaign[1], demonstrating the practicality of KIC, and studying its impact on signal-of-interest processing. We consider a four-node network as in Fig. 1, where the jammer can be an IBFD node or not, but the focus is on how the interference affects the receiver and eavesdropper. The signal-of-interest is an IEEE 802.15.4 waveform, basis for many Internet-of-Things applications [9], and we use the waveform agnostic frequency offsets least mean squares (FO-LMS) algorithm [10] for KIC.

Manuscript received 9 May 2023; accepted 4 June 2023. Date of publication August 31, 2023; date of current version August 31, 2023. The associate editor coordinating the review of this paper and approving it for publication was L. Yang.

K. Pärlin, T. Riihonen, and M. Turunen are with Tampere University, Faculty of Information Technology and Communication Sciences, Korkeakoulunkatu 1, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi).

V. Le Nir is with Royal Military Academy, Signal and Image Center, Avenue de la Renaissance 30, B-1000 Brussels, Belgium.

M. Adrat is with Fraunhofer Institute for Communication, Information Processing and Ergonomics, Fraunhofer Straße 20, 53343 Wachtberg, Germany.

This research work was supported by the Academy of Finland and the Finnish Scientific Advisory Board for Defence.

Digital Object Identifier 10.1109/LWC.2023.3284006

[1]Measurement dataset is available at https://dx.doi.org/10.21227/9mty-pf96

II. Known-Interference Cancellation

The challenges of KIC follow from the system model in Fig. 1. The transmitter broadcasts a signal $s(t)$ that is of interest to the receiver and eavesdropper. The jammer, on the other hand, broadcasts a signal $x(t)$ that, in its discrete-time baseband complex form $x(n)$, is known to the receiver but not to the eavesdropper. Then, the discrete-time signal at the receiver becomes a superposition of those two so that

$$d_{\mathrm{r}}(n) = \mathbf{h}_{\mathrm{jr}}^{H}\mathbf{y}_n e^{j\sum_{i=1}^{n}\epsilon(i)} + \mathbf{h}_{\mathrm{tr}}^{H}\mathbf{s}_n + v(n), \tag{1}$$

where $\mathbf{h}_{\mathrm{tr}}$ and $\mathbf{h}_{\mathrm{jr}}$ are the channel impulse responses from transmitter and jammer to the receiver respectively, $\{\cdot\}^{H}$ denotes conjugate transpose, $v(n)$ is measurement noise with variance σ_{v}^2, $\mathbf{y}_n$ accounts for sampling $x(t)$ with time-varying sampling frequency offset $\eta(i)$ according to (2) in [10], and the multiplicative term $e^{j\sum_{i=1}^{n}\epsilon(i)}$ accounts for the carrier frequency offset and phase noise. The received signal at the eavesdropper becomes

$$d_{\mathrm{e}}(n) = \mathbf{h}_{\mathrm{je}}^{H}\mathbf{x}_n + \mathbf{h}_{\mathrm{te}}^{H}\mathbf{s}_n + v(n), \tag{2}$$

where $\mathbf{h}_{\mathrm{te}}$ and $\mathbf{h}_{\mathrm{je}}$ are the channel impulse responses from transmitter and jammer to the eavesdropper respectively, and we can ignore the frequency offsets, since the signals are assumed to be unknown to the eavesdropper anyway.

Not knowing $x(n)$, the eavesdropper is stuck with the superposition of the received signals. The receiver, however, can subtract $x(n)$ from the received signal if it is able to estimate $\mathbf{h}_{\mathrm{tr}}$, $\eta(n)$, and $\epsilon(n)$, resulting in

$$e_{\mathrm{r}}(n) = d_{\mathrm{r}}(n) - \hat{\mathbf{h}}_{n-1}^{H}\hat{\mathbf{y}}_n e^{j\sum_{i=1}^{n}\hat{\epsilon}(i-1)} \tag{3}$$

where $\hat{\mathbf{h}}_{n-1}$, $\hat{\epsilon}(n-1)$, and $\hat{\eta}(n-1)$ are respectively the estimates of the channel impulse response $\mathbf{h}_{\mathrm{tr}}$, carrier frequency offset, and sampling frequency offset at iteration n, and $\hat{\mathbf{y}}_n$ is the result of resampling $x(n)$ with $\hat{\eta}(n-1)$. With very good parameter estimates, the error in (3) approximates to $e_{\mathrm{r}}(n) \approx \mathbf{h}_{\mathrm{tr}}^{H}\mathbf{s}_n + v(n)$, containing just the signal-of-interest and measurement noise. In practice, KIC is likely to result in some residual KI that degrades the signal-of-interest processing.

The signal-to-interference-plus-noise ratios (SINRs) with and without KIC are defined as

$$\gamma_{\mathrm{r}} = \frac{E\left[|\mathbf{h}_{\mathrm{tr}}^{H}\mathbf{s}_n|^2\right]}{E\left[|e_{\mathrm{r}}(n) - \mathbf{h}_{\mathrm{tr}}^{H}\mathbf{s}_n|^2\right]} \tag{4}$$

and

$$\gamma_{\mathrm{e}} = \frac{E\left[|\mathbf{h}_{\mathrm{te}}^{H}\mathbf{s}_n|^2\right]}{E\left[|d_{\mathrm{e}}(n) - \mathbf{h}_{\mathrm{te}}^{H}\mathbf{s}_n|^2\right]} = \frac{E\left[|\mathbf{h}_{\mathrm{te}}^{H}\mathbf{s}_n|^2\right]}{E\left[|\mathbf{h}_{\mathrm{je}}^{H}\mathbf{x}_n|^2\right] + \sigma_{\mathrm{v}}^2}, \tag{5}$$

where $E[\cdot]$ is the statistical expectation operator.

In this work, we use the adaptive FO-LMS algorithm [10] as the reference KIC method. At every iteration, FO-LMS updates [10, Algorithm 1] the parameter estimates by minimizing the error in (3) so that

$$\hat{\mathbf{h}}_n = \hat{\mathbf{h}}_{n-1} + \mu_{\mathrm{h}}\hat{\mathbf{y}}_n e^{j\phi(n)} e_{\mathrm{r}}^{*}(n), \tag{6a}$$

$$\hat{\epsilon}(n) = \hat{\epsilon}(n-1) + \mu_{\epsilon}\Im\left\{\hat{\mathbf{h}}_{n-1}^{H}\hat{\mathbf{y}}_n e^{j\phi(n)} e_{\mathrm{r}}^{*}(n)\right\}, \tag{6b}$$

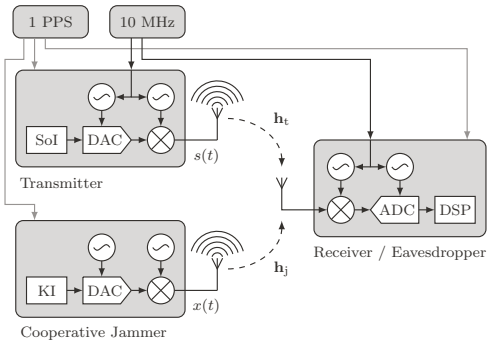
$$\hat{\eta}(n) = \hat{\eta}(n-1) + \mu_{\eta}\Re\left\{\hat{\mathbf{h}}_{n-1}^{H}\hat{\mathbf{y}}_n' e^{j\phi(n)} e_{\mathrm{r}}^{*}(n)\right\}, \tag{6c}$$

where $\hat{\mathbf{y}}_n'$ is the derivative of $\hat{\mathbf{y}}_n$ and $\phi(n) = \sum_{i=1}^{n}\hat{\epsilon}(i-1)$.

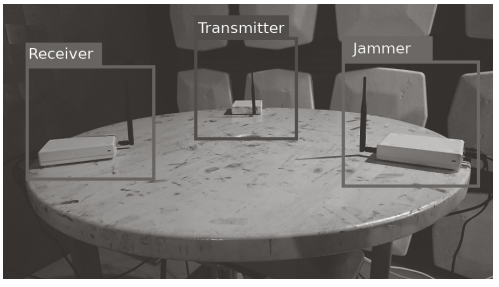
III. Measurement Campaign

In order to study the performance of the described KIC approach, we carried out an extensive experiment using the setup illustrated in Fig. 2a. The setup implements the system model with some simplifying modifications. Firstly, the receiver and eavesdropper were implemented using the same hardware, leaving the distinction to be made in software. Secondly, a reference timing generator was used that *optionally* provides initial synchronization across the devices and emulates that step required in practical implementation. Finally, the transmitter and receiver were connected to a reference frequency generator, which makes processing the signal-of-interest more straightforward and allows us to focus the analysis on the KIC performance but in no way simplifies cancelling the KI.

As shown in Fig. 2b, the measurements were carried out in an anechoic chamber. The three nodes were implemented using USRP-2900 software-defined radios that were positioned on the edges of a table in the middle of the chamber with approximately $0.5\,\mathrm{m}$ between any two devices. The radios were configured to $2.45\,\mathrm{GHz}$ center frequency with $8\,\mathrm{MHz}$ sampling rate. The USRPs provide approximately $90\,\mathrm{dB}$ transmit gain range and both transmitting node gains were varied over that range with $5\,\mathrm{dB}$, and some additional $2.5\,\mathrm{dB}$, steps. The entire resulting measurement grid[1] was recorded on a drive using the receiver. The receiver gain was kept fixed at a level that took full advantage of the DAC dynamic range when both transmitted signals were at their highest power.



(a) Diagram of the measurement setup



(b) Photograph of the measurement setup

Fig. 2. Setup for over-the-air experiments in an anechoic chamber.

The signal-of-interest was taken to be IEEE 802.15.4 that specifies the physical layer and medium access control sublayer for low data rate wireless connectivity with fixed, portable, and moving devices with no battery or limited energy consumption requirements [9]. It is the basis for several well-known high-level communication protocols such as Zigbee and 6LoWPAN amongst others. IEEE 802.15.4 specifies multiple physical-layer implementation variants. In this work, we used the $2.4\,\mathrm{GHz}$ option that is aligned with our chosen measurement carrier frequency, but is also the most common IEEE 802.15.4 physical layer variant, since it provides the maximum data rate and highest number of RF channels. This variant uses O-QPSK modulation and direct sequence spectrum spreading with about $9\,\mathrm{dB}$ of processing gain, offering $250\,\mathrm{kbit/s}$ data rate in a $2\,\mathrm{MHz}$ channel bandwidth.

For each gain configuration, we made ten separate recordings, each of which consisted of 512 signal-of-interest frames. The KI was $4\,\mathrm{MHz}$ bandlimited noise created with a pseudo-random number generator and filtering. This approach would also straightforwardly facilitate generating the same signal across legitimate nodes in practice, relying only on a pre-shared secret seed to avoid transferring and storing the complex-valued baseband jamming waveform into each device. Furthermore, except for a short burst (2048 samples in length) in the beginning of the KI that optionally facilitates auto-correlation based KI start detection, the KI does not repeat making it difficult for an adversary to estimate the KI signal and sets this work apart from previous KIC experiments [6]. The following analysis takes advantage of the measurement simplifications but also demonstrates the use of the repeated start sequence. That is, the signal-of-interest demodulator always knows where each transmitted frame starts in the received signal streams since the aim is to focus on KIC performance. The KI canceller, however, either knows where the KI starts in the received streams or detects its start through auto-correlation. In either case, the KI canceller is then still affected by the carrier and sampling frequency offsets.

IV. Experimental Results

The signal-of-interest and KI are illustrated in Fig. 3, which shows the power spectral density of the received superposed signals without KIC, with KIC, and with perfect KIC (i.e., the signal-of-interest received without the KI). In this case, we have chosen a point in the measurement grid where the received KI is much more powerful than the received signal-of-interest. This view already indicates that the reference KIC method suppresses the KI significantly, albeit not perfectly. For a more detailed analysis, Fig. 4 shows the residual KI power without and with cancellation when there is no signal-of-interest received. Either auto-correlation is used to detect the start of the KI or the coarse time synchronization from the shared timing generator is relied on. The latter results in a more robust cancellation at low received interference powers as the correlation-based signal detector can in that range misjudge the start of the signal beyond the extent that the FO-LMS algorithm can handle (i.e., the offset is larger than the estimated channel impulse response length).

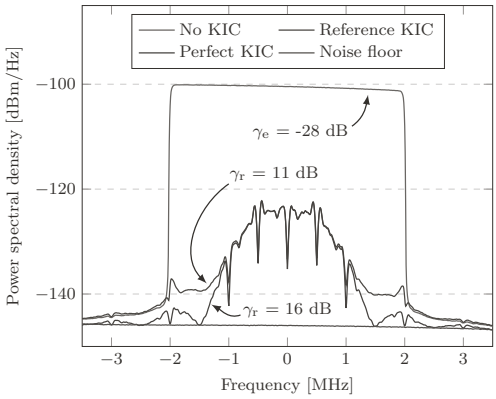


Fig. 3. Power spectral densities of the superposed KI and signal-of-interest without KIC, with proposed KIC, and with perfect KIC.

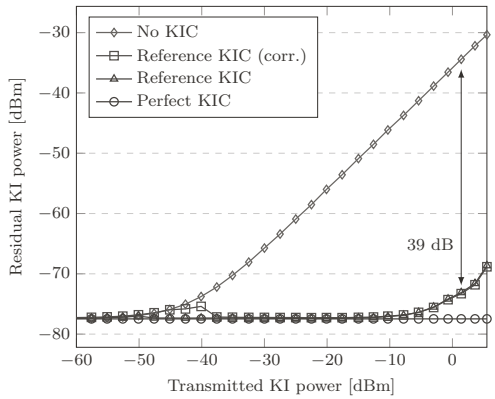


Fig. 4. Efficiency of the reference KIC method without the signal-of-interest and without or with existing coarse time synchronization.

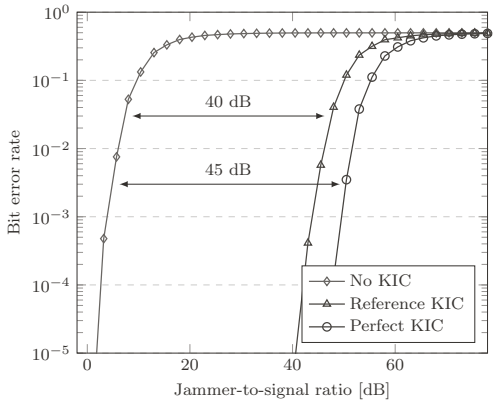
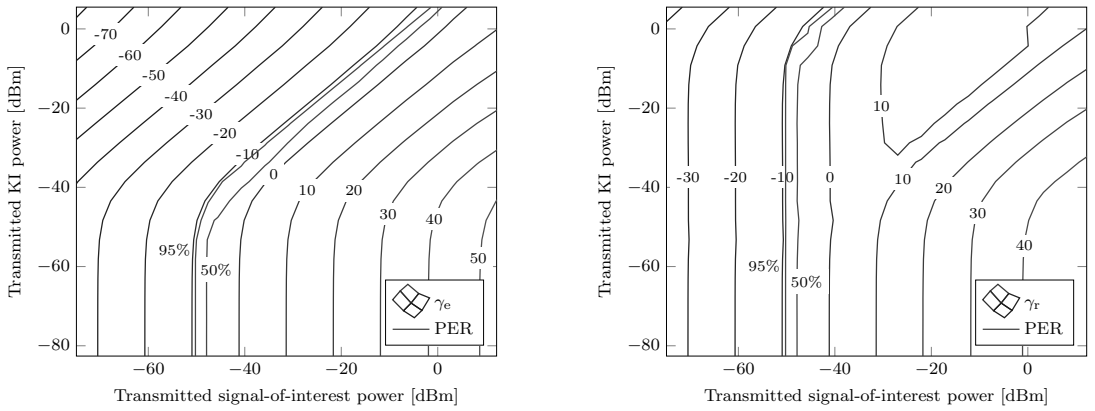


Fig. 5. Performance of the reference KIC when the known interference is received with a fixed power of $-34\,\mathrm{dBm}$, on top of which the signal-of-interest power is varied, resulting in the jammer-to-signal ratio on x-axis.



(a) No KIC (b) Reference KIC

Fig. 6. SINRs at the eavesdropper, γ_e, and receiver, γ_r, (i.e., without and with KIC) along with the PERs with regards to the transmitted signal powers.

Altogether this gives a baseline understanding of how well the method can potentially perform. The results exhibit that FO-LMS is able cancel the KI at most by about $39\,\mathrm{dB}$ before being limited by the nonlinearities and noise within the KI at high KI powers. Given that the estimated carrier and sampling frequency offsets were on the order of kilohertz and hertz respectively, the performance is nonetheless very good. In Fig. 5, the analysis is extended to include the signal-of-interest. In this case, the signal-of-interest gain is varied and the KI gain is set to $85\,\mathrm{dB}$ or $0\,\mathrm{dB}$. The former allows us to get the results with and without KIC, while the latter acts as a reference case that would be achieved with perfect KIC. We look at the bit error rate at the receiver when demodulating the signal-of-interest. Firstly, the bit error rate curve is significantly affected by the powerful jamming signal, as expected. Secondly, KIC directly translates to improved signal-of-interest demodulation, i.e., the results in Fig. 4 are consistent with those in Fig. 5, despite the added signal-of-interest. Unfortunately this also means that the residual KI remaining after the reference KIC prevents the demodulation performance from reaching that as after the perfect KIC.

The entire measurement grid is presented in Fig. 6 by plotting SINRs before and after the KIC together with the 95% and 50% packet error rate (PER) thresholds. The results characterize the reference KIC performance over a wide range that in practice may occur depending on the transmitted signal powers and node placements. We see that there is a significant portion of the grid, where SINR without the KIC is too poor to successfully demodulate most of the packets, but KIC improves the SINR enough to facilitate successful demodulation. In alignment with the above results, it is also clear that for high power KI, the reference KIC is unable to suppress the KI all the way to the noise floor, causing some SINR degradation. Similarly, the reference KIC is affected by a powerful signal-of-interest, which results in the flat SINR area in the upper right corner of Fig. 6b. Still, the reference KIC facilitates a significant shift in the SINR.

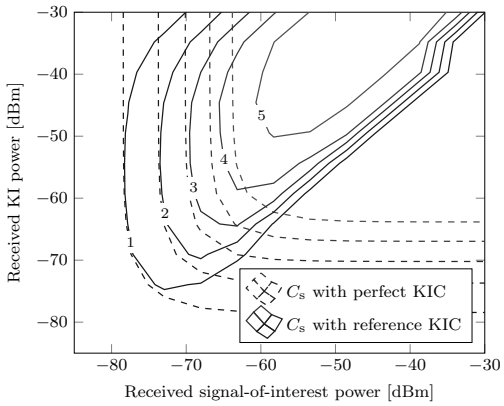


Fig. 7. Secrecy capacity, C_s, in bps/Hz with perfect and reference KIC.

That shift in the SINR consequently provides security at the physical layer. This is evident by contrasting the results from Fig. 6 with that of the perfect KIC and calculating the secrecy capacity that the legitimate receiver has over the eavesdropper given either reference or perfect KIC at the receiver. The secrecy capacity, $C_s = \max\{\log_2(1+\gamma_r) - \log_2(1+\gamma_e), 0\}$, is plotted in Fig. 7 with regards to the received KI and signal-of-interest powers. It is clear that the reference KIC does not always allow to achieve quite the same secrecy capacity as perfect KIC would. At high KI and low signal-of-interest powers (i.e., upper left corner), this is due to the reference method's inability to deal with nonlinearities in the KI. When the signal-of-interest power is relatively high compared to the KI power (i.e., lower right corner), this is because the signal-of-interest hampers the KIC. However, the physical layer security provided by the reference KIC is still significant, especially considering that without KIC the secrecy capacity is zero since then $\gamma_r = \gamma_e$ in the experiments.

V. Conclusion

In this letter, we studied the practicality of cooperative jamming with an arbitrary known interference (KI) waveform for the purpose of providing physical layer security in the presence of an eavesdropper. Specifically, we looked at the capability of the frequency offsets least mean squares (FO-LMS) adaptive algorithm to suppress a KI signal that is received through an unknown channel with carrier and sampling frequency offsets. We also analyzed how the KI suppression affects the subsequent signal-of-interest processing. To facilitate the analysis in this work, and to support further research into this topic, a comprehensive measurement dataset was collected and is released alongside this letter.[1] The experimental results demonstrated that the FO-LMS is well capable of suppressing a KI signal even when the KI is superposed with a signal-of-interest. The algorithm is, though, unable to deal with nonlinearities and phase noise in the received KI, which can result in some residual KI after the cancellation and therefore leaves room for improvement of the KI cancellation method. Still, despite these limitations, the results showed that this approach is useful for providing physical layer security in the presence of an eavesdropper. Furthermore, this approach could be used to prevent adversarial nodes from wirelessly communicating within an area while not overly hampering legitimate nodes therein.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[3] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Tech.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[4] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[5] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, "Effect of frequency offset on cooperative jamming cancellation in physical layer security," in *Proc. IEEE Globecom Workshops*, Dec. 2018.

[6] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 240–243, Feb. 2020.

[7] R. H. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 764–777, Feb. 2010.

[8] L. Sun, Y. Zhang, and A. L. Swindlehurst, "Alternate-jamming-aided wireless physical-layer surveillance: Protocol design and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1989–2003, Dec. 2020.

[9] "IEEE standard for low-rate wireless networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020.

[10] K. Pärlin, T. Riihonen, V. Le Nir, and M. Adrat, "Estimating and tracking wireless channels under carrier and sampling frequency offsets," *IEEE Trans. Signal Process.*, vol. 71, pp. 1053–1066, Mar. 2023.