A multi-site quad-band radio frequency interference monitoring alerting and reporting system

Morrison, Aiden J.

IEEE
2020

Morrison , A J , Sokolova , N , Hakegard , J E , Bryne , T H & Ruotsalainen , L 2020 , A multi-site quad-band radio frequency interference monitoring alerting and reporting system . in E Lange (ed.) , 2020 European Navigation Conference (ENC) . IEEE , European Navigation Conference , Dresden , Germany , 23/11/2020 . https://doi.org/10.23919/ENC48637.2020.9317522

http://hdl.handle.net/10138/341251
https://doi.org/10.23919/ENC48637.2020.9317522

A Multi-Site Quad-Band Radio Frequency Interference Monitoring Alerting and Reporting System

Aiden Morrison[*], Nadezda Sokolova[*], Jan Erik Håkegård[*], Torleiv Håland Bryne[*], Laura Ruotsalainen[**]

[*]SINTEF Digital, Connectivity Technologies and Platforms Dept.,
Trondheim, Norway
email: Aiden.Morrison@sintef.no

[**]Department of Computer Science, University of Helsinki,
Helsinki, Finland
email: Laura.Ruotsalainen@helsinki.fi

Abstract: *This paper reviews the motivation behind and development of a deployable Radio Frequency Interference (RFI) detection, alerting and reporting system which simultaneously monitors all Global Navigation Satellite System (GNSS) L-band signal transmission for disruption, captures interference events, characterizes them, notifies stakeholders of event occurrence and lastly marshals the captured data to cloud storage. Results of a multi-site international deployment program are presented and discussed.*
Topic Area: *PNT Security and Robustness*

1. Introduction

GNSS signals are extremely vulnerable to intentional or unintentional RFI due to the vanishingly small amount of power reaching the earth's surface making even small amounts of in-band power a serious concern for users relying on GNSS systems for navigation, guidance, control or timing. Simultaneously, an increasing number of machine control, autonomous drone and vehicle applications are dependent on multi band multi constellation GNSS reception in as many as four simultaneous bands between 1.1 and 1.6 GHz. To address this challenge, the Advanced RFI Detection Analysis and Alerting System (ARFIDAAS) was developed to simultaneously monitor all GNSS L-band navigation signals and notify site stakeholders of detected RFI events at short latency. Due to the potential for significant operational disruption, an ideal RFI monitoring system would notify relevant site operators of the presence and approximate characteristics of detected RFI shortly after detection of the event while also saving raw IF samples of the captured event in a centralized location for subsequent analysis. The data generated by the system is a superset of that produced by monitors employed by the STRIKE3 initiative [1], including both the text report containing site related information (location, antenna type, start time of event) [2], as well as the spectral analysis given in Fig. 5 both directly emailed to stakeholders at low latency. The system also automates the process of uploading the captured RF data of the event to cloud storage which is available to interested researchers. This paper discusses system implementation details and presents preliminary results based on the initial system deployment period.

2. System Architecture

The architecture of the ARFIDAAS system is best understood as comprising three main system components. The first component a reconfigurable front-end which provides continuous measurements of the monitored spectrum, power levels, and automatic gain control (AGC) feedback states. The second is a collection of software components individually responsible for activities such as analyzing the collected data for signs of RFI matching the criteria selected by the user, for capturing qualifying events and for the subsequent initial analysis, notification of stakeholders and upload of the captured data. The third component is the hosting provided by the cloud which forms a centralized collection of all events from all deployed ARFIDAAS systems, within which subsequent finer grained analysis and fingerprinting activities can be conducted. A conceptual diagram of the system is shown in Figure 1, where the hardware and software elements are represented by blue squares while the online component is represented by a stylized cloud.

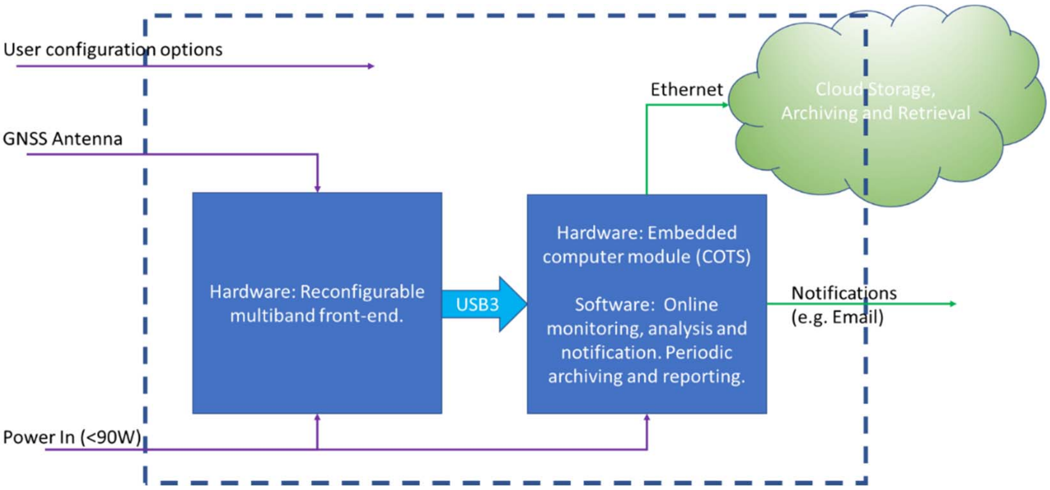
User configuration options
GNSS Antenna
Power In (<90W)
Ethernet
Cloud Storage, Archiving and Retrieval
Hardware: Reconfigurable multiband front-end.
USB3
Hardware: Embedded computer module (COTS)
Software: Online monitoring, analysis and notification. Periodic archiving and reporting.
Notifications (e.g. Email)

Figure 1. The high level architecture of the ARFIDAAS system showing the three main system elements, plus input and output data and connections.

3. System Hardware

The ARFIDAAS hardware front-end is essentially a software defined radio front-end tuned for L-band operation but with additional features to specialize the device for RFI monitoring over the GNSS signal sub bands. As indicated in Figure 2, the ARFIDAAS front-end hardware is subdivided into functional blocks.

In red, the RF signal handling section takes the input from the attached active or passive antenna and applies a series of amplification, filtering, and splitting operations to produce six total signal taps. The upper path includes a SAW filter which isolates 58 MHz of spectrum covering signals between Beidou B1 and GLONASS G1, while the lower path filter is wider, nominally 104 MHz covering L5 through E6. The filtering and amplification stages were chosen along with supplied antenna bias voltage to ensure that regardless of incident RFI power received by the antenna, no component of the RF signal chain can be driven outside of its rated power envelope. The filtered, amplified, and split signals are fed to the RF mixer blocks in dark blue as well as the RF power measurement blocks in green. In the former, the signal is mixed to complex baseband and passed through anti-aliasing filters while in the latter a direct measurement of total in-band power is created, which independent of the operation of the automatic gain control features of the system allows incident power level in both the upper (L1) and lower (L5 through E6) signal bands to be estimated.

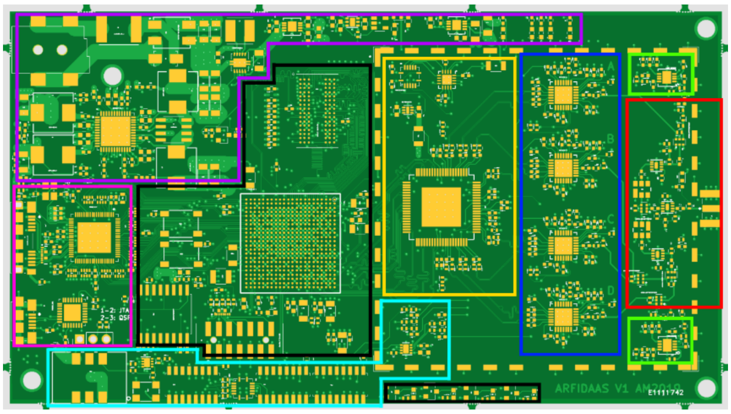

Figure 2. ARFIDAAS Front-End hardware with functional blocks highlighted.

The yellow bordered region contains the eight channels of digitization necessary to capture the four complex baseband signals from the mixing stage, as well as feedback and filtering components to servo the variable gain amplifiers in the mixers as part of the AGC.
The cyan region contains clock generation and distribution components, fed from a common crystal oven oscillator. Three primary synchronous clocks are generated here, including the 30 MHz reference tone used by the IF mixers in their phase locked loops, as well as the sampling clock of the ADC and the system clock of the FPGA.
The black region contains the FPGA and support components including indicator lights, while the purple domain denotes the region of the board dedicated to power supplies. The pink region contains the USB3 configuration and sample streaming interface as well as a USB2 to serial interface used for debugging.

4. System Software

Software running on the ARM cores of the FPGA is responsible for collecting complex baseband sample data along with AGC bin population data, in band power measurements and other voltage/temperature parameters for transmission to the attached monitoring system while also accepting commands from the monitoring system to allow configuration of the operating mode of the system including but not limited to sampling rate, band centre frequencies and AGC parameters.
The software running on the attached monitoring computer is subdivided in to several logical blocks that each implement a separate aspect of the system's overall functionality and communicate with each other using message passing over ZeroMQ as illustrated in
Figure 3 and
Figure 4.

In
Figure 4, the interchange of information between the overall application supervisor program and the sub-module responsible for interfacing with the hardware front-end and monitoring for event detection based on user selectable detection settings is shown. When an event is detected, and captured by Piece A, a message is passed via the supervisor to another component (creatively called 'Piece B') which executes initial event analysis, classification and report generation. One of the outputs of this software component includes an analysis of the captured event to indicate to a stakeholder where in the spectrum RFI is localized and whether it may be considered narrowband or wideband, as well as its relative power level to help inform the user

about whether they need to take immediate remedial action based on their application requirements.

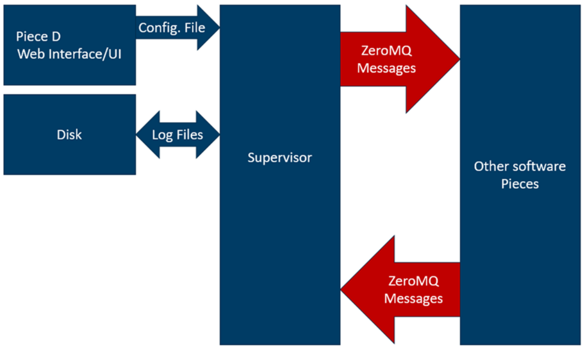

Figure 3. Software high level.

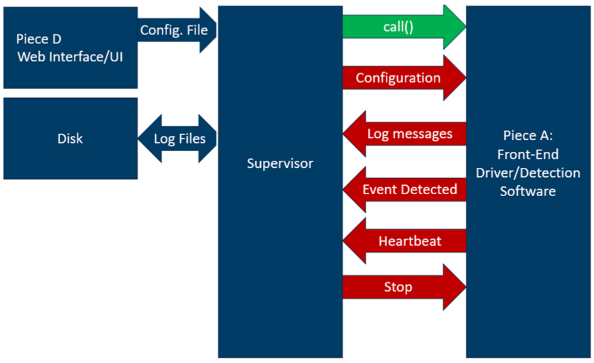

Figure 4. Software detail of one component..

After the initial analysis and reporting is completed by Piece B, a message is once again passed via the supervisor to a 3rd software component referred to as Piece C which is responsible for sending notification emails to the users subscribed to the local mailing list as well as uploading the captured data samples and locally generated report to cloud storage.

5. Environment Characterization and Event Capture

To help distinguish between active interference events and normal background activity at a given site, the system automatically captures an environment baseline event at startup (and periodically thereafter), then checks for deviations from this profile when classifying captured events. An example of the produced baseline and RFI event data is given in Figure 5, where each of normal GNSS signals, site specific spectrum sharing and illegal RFI are present.

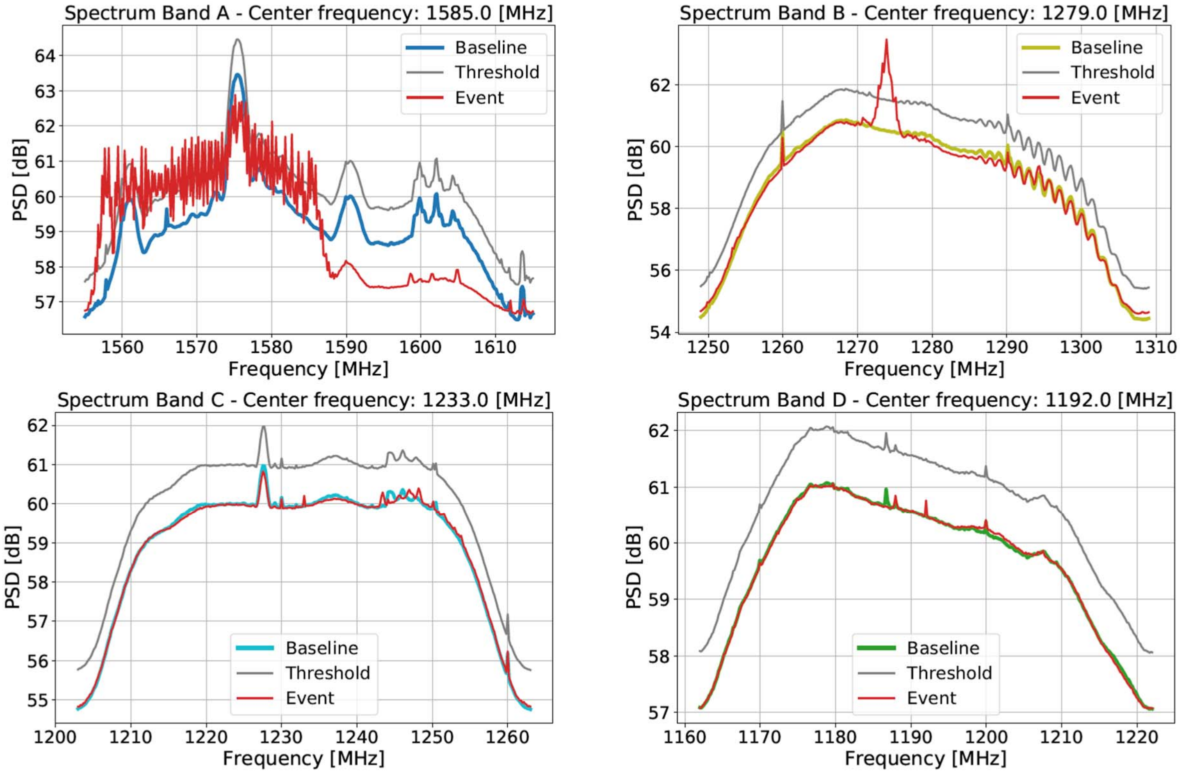

Figure 5. An example of the environment baseline and RFI event captured in Trondheim, Norway.

While the system is sensitive enough to detect the locally elevated noise floor caused by individual GLONASS satellites around 1602 and 1246 MHz as well as changes when different GLONASS frequency channels are in view, the more obvious signal features are those generated by the main lobes of GPS L1CA, and Galileo E1 at 1575 MHz, the side-lobes of the Galileo E1A near 1560 and 1590 MHz and the GPS L2C signal near 1227 MHz. Here a wideband 'chirp' jammer is present in the L1 band from 1555 MHz through 1585 MHz. The apparent ripples in the E6 spectrum between 1290 and 1300 MHz are believed to be artifacts introduced by the system SAW filter roll off region as they are present regardless of antenna model or the use of a GNSS signal simulator and are not a feature of the signal environment.

6. International Deployment

The six initial deployment locations were selected based on the availability of friendly research personnel who were able to assist in observing and updating the system as necessary during its initial trial period, as well as able to provide access to a suitable GNSS antenna feed in a weather proof location with high speed internet access. The requirement of high speed internet access is dictated by the ability of the system to produce large volumes of data even under relatively benign conditions, for example one six second RFI event occurring hourly produces over 800 GB of data which must be uploaded to cloud storage. Hosting sites used between November 2019 and February 2020 were two SINTEF facilities in Trondheim, the University of Helsinki, Indra Navia’s office in Asker, The Dutch Aerospace Research Laboratory (NLR) in Amsterdam, and the ESTEC facilities in Noordwijk. Regardless of the deployment location a common factor proved to be the presence in the GNSS signal bands of undesirable yet unfortunately legal uses.

7. Co-Authorized Spectrum Users

In Fig. 5, an undesirable local signal is present in the form of a RADAR system near 1274 MHz which is undesirable as it overlays the E6 and B6 signals, but is unfortunately legal where this instance of the system is deployed. An unexpected common theme encountered when deploying instances of the ARFIDAAS system to different sites was that at every site without exception there was an observation of signals within the GNSS bands which were strong enough to be readily observed yet are authorized co-users of the spectrum. An example of this type of undesirable yet legal interference is that of Direction Measuring Equipment (DME) which operates in the aeronautical radio navigation system (ARNS) band between 960-1215 MHz [3] thus potentially overlapping and interfering with the E5 band.

In some countries such as the Netherlands where two of the ARFIDAAS stations were deployed, it is legal to use frequencies in the vicinity of 1294 MHz for amateur radio purposes, which while narrow-band have been encountered at unexpectedly high power levels. In one instance a signal in this band was traced back to an amateur radio source who was utilizing a 300 Watt amplifier to feed a dish with 28 dBi of gain which was coincidentally pointed at the location of the monitor antenna from a distance of only a few km [2].

In another case, the Norwegian military announced a week-long series of tests and training including electronic warfare, during which stations in Oslo and Trondheim were triggered by broadband interference between 1240 and 1300 MHz, as well as narrower band signals which appeared to be centered on and possibly targeting the band used by the previously mentioned RADAR signal seen in Fig. 5.

8. Example Events

It is helpful to group RFI events in to at least three distinct categories, namely those of unintentional RFI emissions, intentional jamming, and ambiguous events. In all three cases the signals represent the injection of additional power in to a sensitive GNSS reception band, and a degradation of tracking and observable generation performance even if small in magnitude. The three subplots of Fig 6 show examples of these with an unintentional tone signal on the left, an intentional use of a chirp jammer to attack the L1 band on the right, and a signal with an ambiguous motivation in the middle.

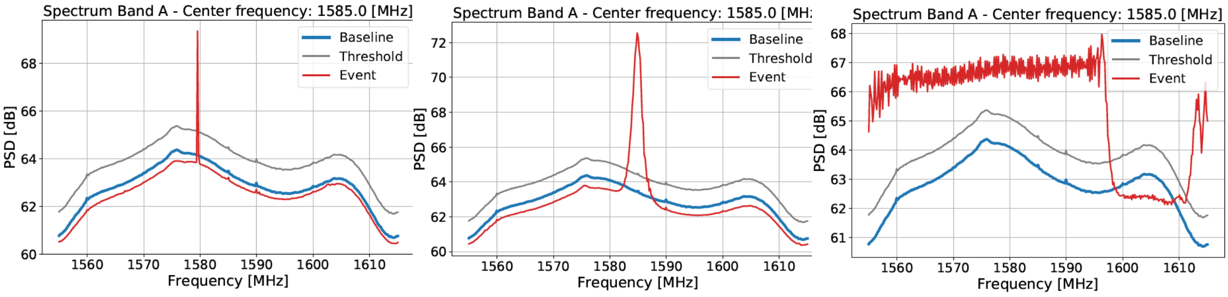

Figure 6. Three different types of RFI event observed at a single monitoring station within a 24 hour period. The wideband event in the rightmost plot includes aliasing from below 1555 MHz to appear above 1610 MHz.

An educated guess as to whether an observed signal is jamming or spurious emission can be made by inspecting the spectral content of the signal as well as its fine-grained time-frequency behavior. Typically, a jammer with a relatively narrow bandwidth will directly target the main lobe of the signal of interest, or will use a single or multi-level FM modulation to cover a band of frequencies including one or more main-lobes of interest.

Using this reasoning, the narrowest signal shown in Fig. 6 is not thought to be intentionally generated jamming targeting the L1 band as the centre frequency does not appear to be targeting the main lobe of any given signal component. By contrast the middle signal overlaps with only the upper side-lobe of the E1a signal, which is not commonly used in mass market consumer GNSS devices. While it is not strictly necessary for a jammer to spectrally overlap with a victim signal, the jamming effectiveness is much higher when energy is deposited where the victim signal PSD is high. In cases where the jamming signal does not overlap with the victim signal, the jammer is relying on digital or analog saturation effects to degrade GNSS reception. In the former case the jammer can dominate the available bits of sampled signal effectively pushing the desired GNSS signal further below the noise floor pre-correlation, while in the second case the analog circuitry will be pushed in to saturation, pushing the desired GNSS signal further below the noise floor pre-sampling. In other cases, components of the generated jamming signal may alias or fold to appear to cover additional regions of the signal within the victim receiver such as in the wideband modulation case on the right side of Fig. 6. Here the GLONASS L1 band is not actually covered by the transmitted signal from the jammer, however an aliased image of a portion of the signal transmitted below 1555 MHz has folded in to the spectrum between 1610 and 1615. If the ARFIDAAS system used the same centre frequency but a slightly lower sampling rate of for example 50 MHz, the jammer would appear to cover the entire band due to spectral aliasing.

In the time-frequency domain such a jammer appears as in Fig. 7, where it can be observed that the sweep rate of the signal is approximately 4 microseconds, that the sweep rate is not constant but increases slightly between 1580 and 1600 MHz, and that the extent of the sweep signal is not uniform, but exhibits 3-5 MHz excursions in both start and end frequencies.

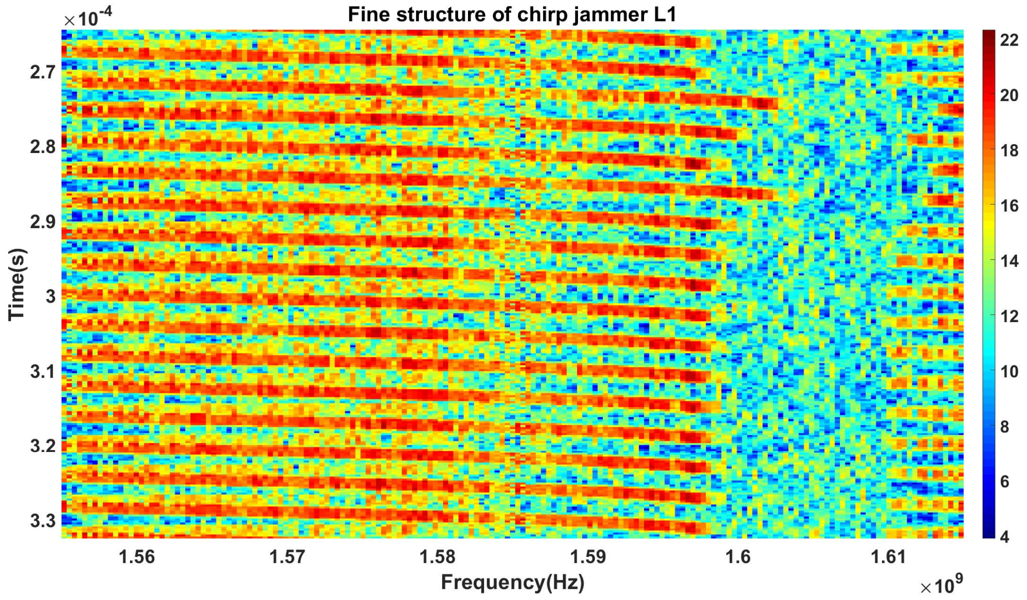

Figure 7. Time-frequency structure of a broadband L1 chirp jammer with aliasing.

It is not known whether these variations in sweep rate or frequency range are intended to be countermeasures against real time characterization and adaptive filtering, or simply unintentional characteristics of the jammer.

In the case of the middle signal shown in Fig. 6, it appears that the signal may be the product of an improperly assembled jamming device. The authors take this position as the fine grained structure of the signal shown in Fig. 8 exposes that the modulation of the signal is in fact a chirp, with a period similar to other jammers observed but with an anomalously small sweep range. Due to the authors experience with electronics design and production it is believed that this signal is emitted by a GNSS jammer device that has one or more incorrect resistor/capacitor elements installed in the signal generation circuitry which results in an unintentionally small sweep range modulating the correct carrier of 1585 MHz.

This choice of centre frequency is a sensible choice for a chirp jammer intended to interfere with each of GPS, GLONASS, Galileo and Beidou simultaneously as it is roughly equidistant between the B1 signal main lobe at 1561 MHz, and the upper edge of GLONASS L1 FDMA near 1610 MHz.

In other cases believed to be caused by malfunctioning or improperly shielded electronic equipment, rake structures can cover the entirety of any of the GNSS signal bands. Typically intentional jamming events will contain energy in the L1 band at a minimum, making it sensible to discard even powerful L5/L2E/E6 only events as not being caused by intentional GNSS interference.

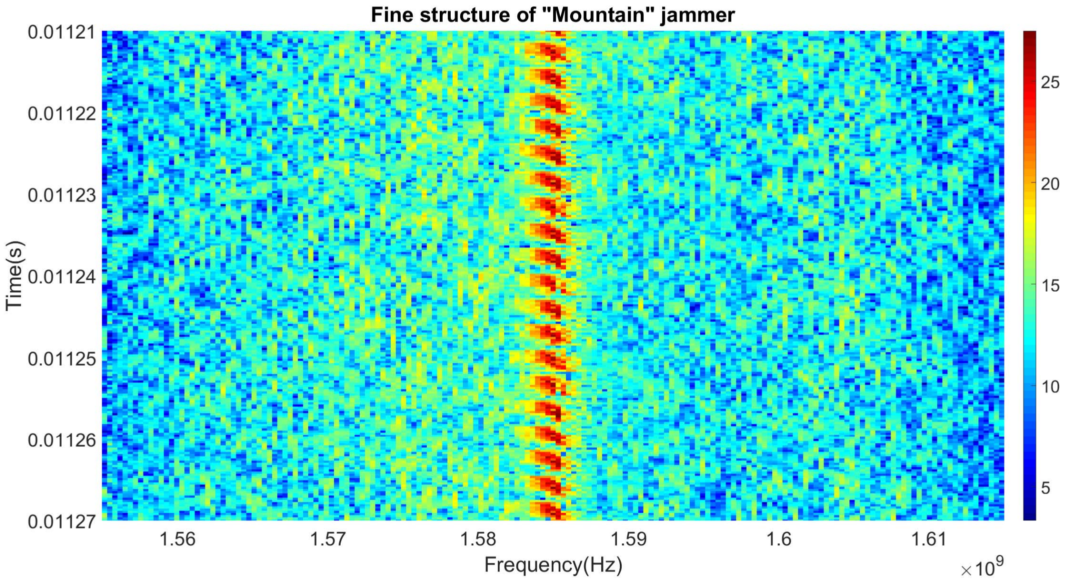

Figure 8. Time-frequency structure of ambiguous signal source shows 'chirp' structure.

9. February 2020 Site statistics

The number of events detected at each of the six deployed sites available in February are presented in Table 1 over the date range of 1 through 25 February 2020. The reason for not producing the full month of data is related to a concentrated cluster of events starting 25 February which produced over 100 events at the main Trondheim site alone covering the entirety of GLONASS L2 through E6. It is believed that this cluster of events was caused by Norwegian defense exercises [6]. While this activity certainly represents jamming of GNSS signals, it is not considered to be a typical occurrence and is so intentionally omitted.

Table 1. Observations of GNSS RFI events over the six initial deployment sites between 1 and 25 February 2020.

Site Location	Trondheim A (SINTEF)	Amsterdam (NLR)	Trondheim B (SINTEF)	Asker (Indra Navia)	Noordwijk (ESTEC)	Helsinki (UofH)
Number of events	156	139	78	41	3	0
Multi-frequency observed?	no	yes	no	yes	no	n/a

It is immediately obvious that different deployment locations appear to experience vastly different rates of RFI occurrence, which is true due to both site characteristics and site specific system configuration options. For example, while the Trondheim B site has direct line of sight to a four lane highway while the primary Trondheim A site only has visibility to local two lane roads, the Trondheim B site was configured to not trigger unless L1 band interference was encountered while the primary Trondheim site would trigger on both or either individually. Similarly the Helsinki site when first deployed in November 2019 would often trigger on local radar signals in the L2 band, leading to the same restriction of sensitivity to be employed. Neither the ESTEC nor the UofH sites have direct visibility to a major roadway, limiting the exposure to vehicle borne jammers and resulting in a far lower event occurrence rate than sites the sites which do.

A second observation is that approximately half of all captured events are due to unintentional EMI, having a narrow bandwidth characteristic with a centre frequency distant from the main lobes of L1 band GNSS signals.

10. Conclusions and data availability

Despite employing a very limited number of stations in the opening phases, the ARFIDAAS system has already captured several hundred RFI events including numerous instances of unintentional as well as intentional GNSS and RADAR jamming. While this version of the system is optimized for initial analysis and alerting of stakeholders at short latency, it is intended to evolve the system to perform higher level analysis on the data captured in the cloud storage to automatically produce meaningful statistics of the captured data such as for example how often L5 experiences interference along with L1 interference, and to attempt to collect geographically diverse information on the characteristics of utilized jammers in terms of bandwidth, modulation type, and sweep rate. An additional point of concern for the future is the potential to detect well executed spoofing attacks that do not trip the sensitive power level monitoring employed by the ARFIDAAS system. In parallel with these improvements it is intended to deploy another 12 stations as appropriate hosting locations become available.

11. Future Work

Characterization of the RFI devices is an important step towards securing the society from intentional GNSS interference. It enables their identification and eventually catching the suspects using the devices. In addition, detection of jamming and especially its type is complex and requires the use of a number of different techniques [6], preferably one of those being jammer characterization. Radio Frequency Fingerprinting (RFF) is a signal classification problem enabling characterization of jammers based on their specific features. Transmitters have their unique features due to the specific coding and modulation of the signals, and hardware related issue such as band-pass filters, local oscillators and power amplifiers [7].

In our future work, we will evolve the capabilities of the ARFIDAAS system hardware and software to provide wider dynamic range and frequency coverage while also reducing notification latency and providing users with additional signal structure analysis within the notification. In parallel we intend to develop novel deep learning methods for characterizing GNSS jamming devices based on the acquired contaminated signals. So far, there is not much research done using deep learning for mitigating the effects and localizing GNSS jammers. One reason for this is the complexity and large amount of work required for labelling signal data for building the machine learning models. Therefore, in addition to using conventional Time-Frequency-Transformations and presenting the data with and image [8], we will consider semi-autonomous data labelling methods such as active learning [9]. Labelled data allows us to characterize the jammers using deep learning techniques that have been showing promising results in other fields, such as Convolutional Neural Networks (CNN) in image processing. However, the sad truth is that the fight against intentional interference is a constant battle. Therefore, in addition to developing methods for classifying the existing jammers sophisticatedly by using the supervised deep learning methods, we have to prepare for the possibly emerging novel interference means. An autoencoder is a neural network that is able to learn structure within the data and to compress it unsupervised so that the representation includes meaningful attributes. In order to make the interference mitigation and jammer identification methods more adaptive to the change of the operation environment, our future work addresses also the development of RFF methods based on autoencoders [10].

12. Acknowledgements

The authors would like to thank the European Space Agency (NAVISP program) and the Norwegian Space Centre for funding the development of the ARFIDAAS system, as well as the Norwegian Council of Research for funding system deployment activities. Additional thanks to the hosts of the first wave of ARFIDAAS systems for their assistance.

References

[1] STRIKE3- Monitor, Detect, Characterize, Standardize, Mitigate and Protect. Last accessed on 24.09.2019 http://www.gnss-strike3.eu/

[2] A. Morrison, "Advanced RFI Detection, Alerting, and Analysis System (ARFIDAAS)", NAVISP Industry Days 22-23 January 2020. Last accessed on 12.08.2020 https://navisp.esa.int/uploads/files/documents/ARFIDAAS%20-%20%20Aiden%20Morrison%20-%20Sintef%20AS.pdf

[3] M. De Angelis, R. Fantacci, S. Menci and C. Rinaldi, "Analysis of Air Traffic Control Systems Interference Impact on Galileo Aeronautics Receivers", Proc. of the IEEE International Radar Conference, Arlington, VA, USA, 9-12 May, 2005. DOI: 10.1109/RADAR.2005.1435897

[4] R. Bauernfeind, T. Kraus, A. Sicramaz Ayaz, D. Dötterböck and B. Eissfeller, "Analysis, Detection and Mitigation of In-Car GNSS Jammer Interference in Intelligent Transport Systems", Proc. of 61. Deutscher Luft- und Raumfahrtkongress, Berlin, 10-12 Sept., 2012.

[5] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, COL R. Ford and M. D. Higgins, "GNSS Vulnerabilities and Existing Solutions: A Review of the Literature", IEEE Access journal, Vol.4, 2016, DOI:10.1109/ACCESS.2020.2973759

[6] "Trener på elektronisk krigføring – kan forstyrre navigasjon i bil og mobiltelefoner," Adresseavisen, 24. February 2020, accessible at: https://www.adressa.no/nyheter/trondelag/2020/02/24/Trener-p%C3%A5-elektronisk-krigf%C3%B8ring-kan-forstyrre-navigasjon-i-bil-og-mobiltelefoner-21163474.ece

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

[8] Morales-Ferre, R.; Wang, W.; Sanz-Abia, A.; Lohan, E.-S. Identifying GNSS Signals Based on Their Radio Frequency (RF) Features—A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator. Data, 5, 18. 2020.

[9] O. Topala, S. Gecgela, E. Eksioglua, G. Kurt, Identication of Smart Jammers: Learning-based Approaches Using Wavelet Preprocessing. Physical Communication, Vol 39, 2020. DOI: 10.1016/j.phycom.2020.101029.

[10] M. Cheginiab, J. Bernardc, P. Bergerd, A. Sourinb, K. Andrewsa, T. Schreck. Interactive labelling of a multivariate dataset for supervised machine learning using linked visualisations, clustering, and active learning. Visual Informatics Volume 3, Issue 1, Pages 9-17. 2019.

[11] Jiabao Yu, Aiqun Hu, Fen Zhou, Yuexiu Xing, Yi Yu, Guyue Li, Linning Peng, "Radio Frequency Fingerprint Identification Based on Denoising Autoencoders", Proc. of the International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2019.