Multi-band Multi-site GNSS RFI Monitoring Results After a Year of Operation

Aiden Morrison, Nadezda Sokolova

SINTEF Digital, Communication Technologies and Platforms Dept.

Trondheim, Norway

Email: {aiden.morrison, nadia.sokolova}@sintef.no

Abstract *– An international network of Radio Frequency Interference (RFI) monitoring stations covering all L-band Global Navigation Satellite System (GNSS) signals has provided large amounts of data on the occurrence rates and characteristics of the detected sources. As the stations are primarily deployed by roadways the measurements include a large number of Personal Privacy Device (PPD) style jammers as well as an unexpectedly large contingent of spurious emissions and co-authorized users. Important results include the high levels of variability in month-to-month activity levels of sites indicating that site survey activities must be conducted over longer periods to obtain accurate occurrence rate information.*

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 guidance, 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, allowing for the aggregation of site-specific RFI statistics as well as potentially allowing individual devices to be fingerprinted and connected to multiple events within or between multiple stations . The data generated by the system is a superset of that produced by monitors employed by the STRIKE3 initiative [1], including each of a spectral mask as in Figure 1 indicating how the given event has deformed the local spectral noise floor, the text report per

Figure 2 containing site related information (location, antenna type, start time of event) [2] [3], as well as the spectral analysis given in Figure 4 both directly emailed to stakeholders at low latency. By including these three pieces of information after a minimal reporting latency the ARFIDAAS system is designed to help site operators take appropriate action in response to detected RFI events which may range from taking no action in the case of narrowband spurious emissions, to noting potential disruptions in long term GNSS monitoring data at the detection time, to reporting the presence of a persistent and strong source to local spectrum management authorities. The inclusion of the waterfall plots of the type shown in Figure 4 within the notification emails was intended to help site operators further distinguish between intentional and unintentional RFI events by exposing the time-frequency structure of the signals, with the knowledge that most 'chirp' signals are intentional GNSS jamming.

This is the author accepted manuscript/postprint version of an article published in European Journal of Navigation.

The system also automates the process of uploading the captured RF data of the event to cloud-storage which is available to interested researchers, and in the near future will automate the process of monthly site statistics reporting based on this uploaded data. This paper discusses system implementation details and presents results and interesting observations based on extended data sets available from some of the longer running monitoring stations including full-year ranges.

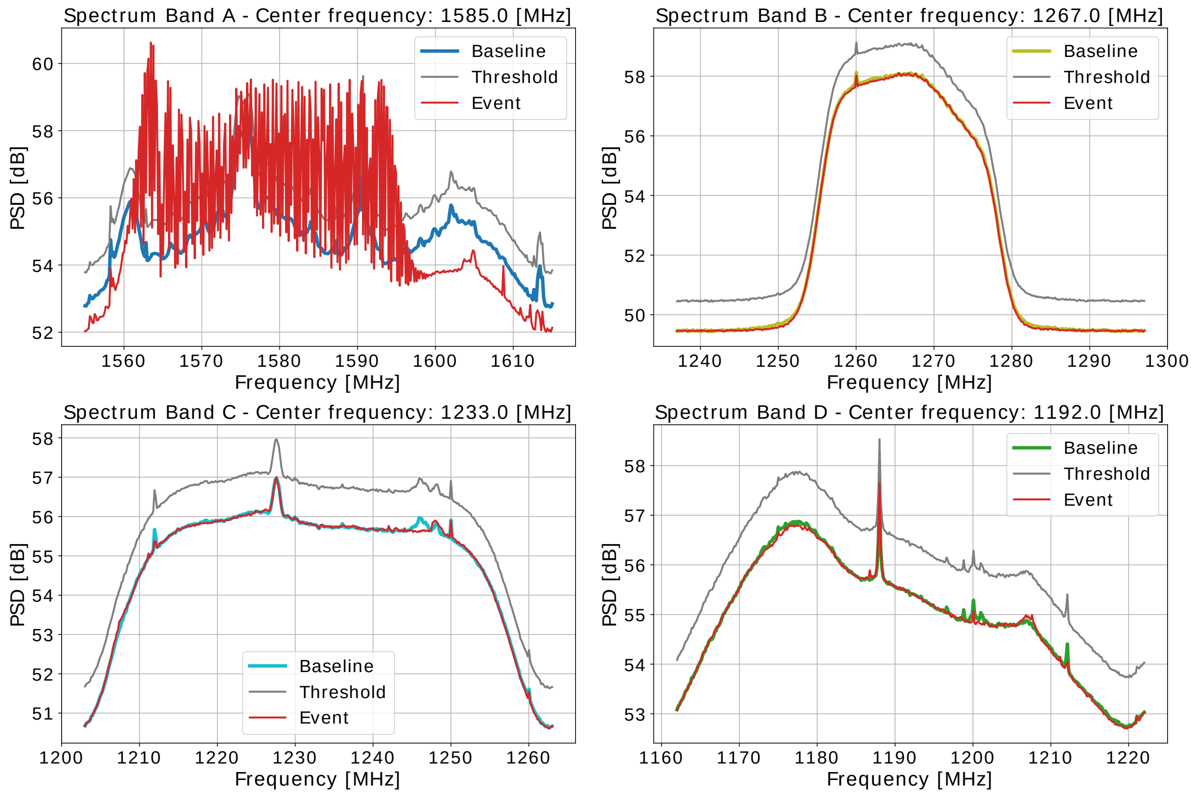

Figure 1: Spectrogram of one of the four simultaneously monitored bands reported by the ARFIDAAS system on detection of an RFI event to site stakeholders. Here the RFI event is chirp modulated and impacts only Band A.

ID: ARFIDAAS_NLR_2021_8_31_10_52_54
2021-8-31T10:52:54Z Input file: Event064.DAT Detection duration: 2.0 seconds
Analysis window: 0.34 seconds Bandwidth: 60.0 [MHz]
Monitoring bands' center frequency: A: 1585.0 [MHz]. B: 1267.0 [MHz]. C: 1233.0 [MHz]. D: 1192.0 [MHz].
Antenna type: AT1675
Location: Netherlands, Amsterdam, site: NLR, coordinates: 52N, 5E
Event origin: 0x00000811

Baseline: RF front end parameters
Avg highband power:-89.91 [dBm] at input
Avg lowband power:-78.88 [dBm] at input
Avg AGC value A: 574.07. Avg AGC value B: 512.00. Avg AGC value C: 512.00. Avg AGC value D: 512.00.

Event064: RF front end parameters
Avg highband power:-84.34 [dBm] at input
Avg lowband power:-78.21 [dBm] at input
Avg AGC value A: 592.10. Avg AGC value B: 495.89. Avg AGC value C: 532.33. Avg AGC value D: 570.67.

Event064: Frequency analysis
Band A - Center frequency: 1585.0 [MHz]
Event 1: Event type: WB. Start: 1561.58 [MHz]. End: 1595.731 [MHz]. Max diff: 6.38 [dB]. Mean diff: 1.69 [dB]

Figure 2: Example subset of reporting data included in event notification emails sent by the ARFIDAAS system.

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 analysing 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 3, where the hardware and software elements are represented by blue squares while the online component is represented by stylized clouds.

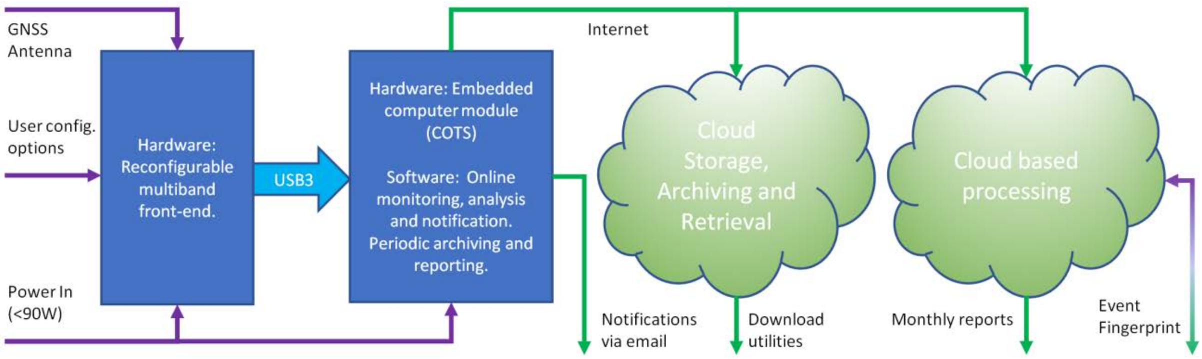

Figure 3. The high level architecture of the ARFIDAAS system showing the three main system elements, plus input and output data and connections.

The software component running on the local computer is designed to minimize the latency of event reports to site stakeholders via emails as reaction time is considered a critical parameter in how useful the data is to the affected users. Referring to Figure 5, the latency between an event detection (part A), and the transmission of a report package (part C) is approximately 40 seconds. An event classifier (part D) which attempts to determine the modulation type and characteristics such as frequency span and sweep rate in the case of chirp signals then operates on the captured raw data prior to cloud upload (part E) of the data and reporting ensemble.

The motivation for separating the classifier operation from the initial reporting process is based on the trade-off between the quantity and quality of the information provided and the amount of time required to complete the processing. Since the human site operators can determine the nature of the source from spectrograms such as that in Figure 4, the classifier data is not considered essential for prompt reporting.

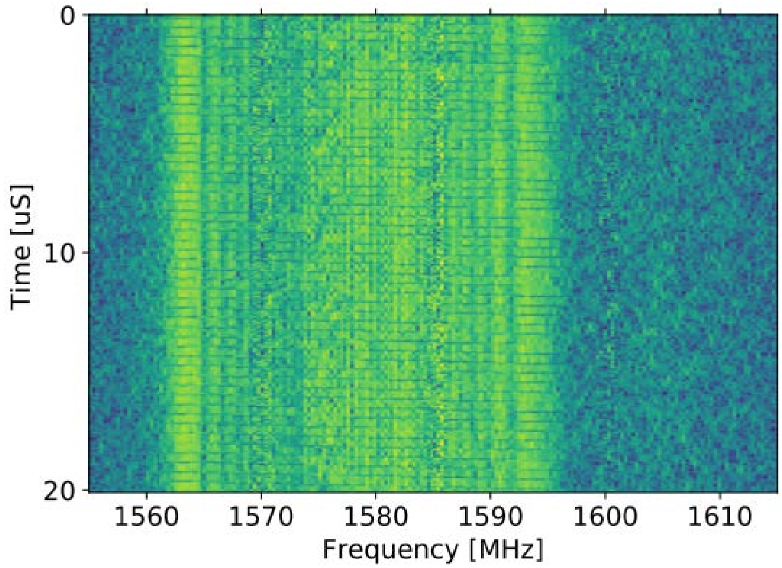

Figure 4: Example of a high sweep repetition rate chirp event in the L1 band. While the bandwidth of approximately 35 MHz is well within the measurement range of the ARFIDAAS system, the sweep repetition rate of approximately 2 MHz is at the limit of the time resolution of the waterfall representation.

The uploaded classifier data is aggregated in the cloud and used for long term statistical analysis of threats and threat evolutions such as the RFI type classifications shown in Figure 6 that represents a full year of data for one monitoring site. Other pieces of information typically extracted from the classifier include but are not limited to absolute and relative band occupancy (e.g. how often is L5 impacted versus L1 versus both at the same time), time of day occurrence histograms, tabulation of power level impacts by event, and high level occurrence rate data expressed in units of both total time affected and as a percentage of time the station was affected.

Figure 5: Local software flowchart.

Separately a planned future development is the provision of event fingerprinting to provide site operators and the overall network of stations with additional information on specific jamming devices. Ideally this fingerprinting will be capable of distinguishing between individual jamming devices even when their intended signal is the same by using power level, frequency and other signal characteristics variations. If this identification is feasible, the database of collected events can be used to build up a behavioural map of frequently seen jamming devices to attempt to predict and prevent their future activities.

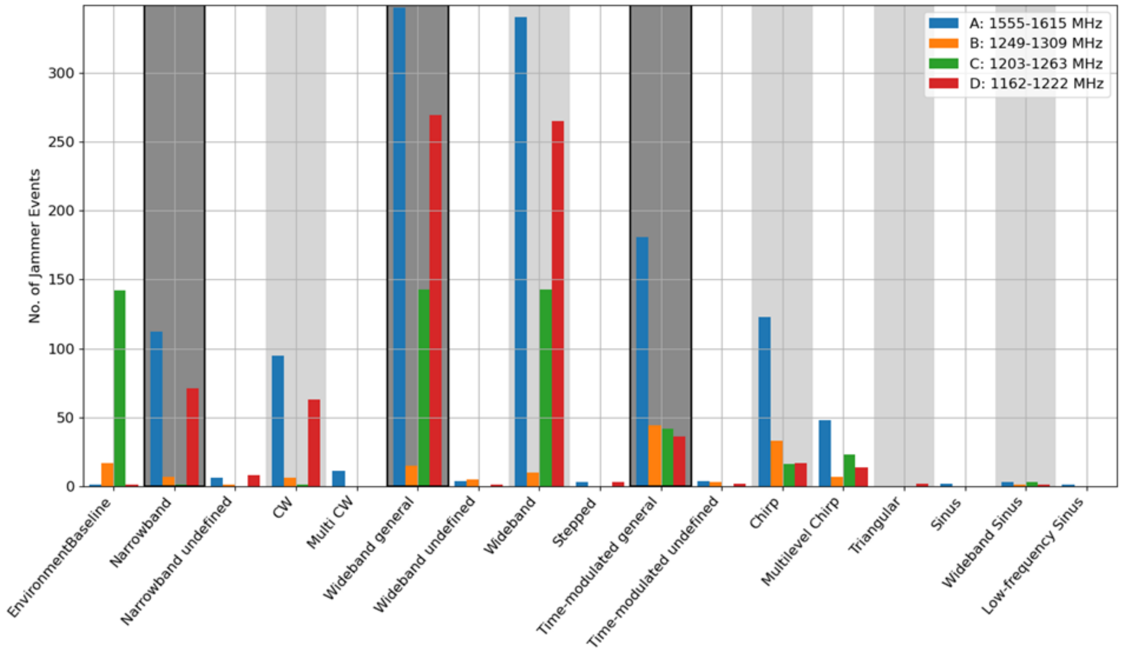

Figure 6: RFI source classifications captured on each of the four bands from a full year of monitoring data in Asker, Norway. Note that the three dark categories are aggregates which include the sub-categories to their right.

3. Network deployment and results

The ARFIDAAS network presently comprises ten deployed monitoring stations. A map indicating the approximate locations of these stations is shown in Figure 7 as green markers. ARFIDAAS monitoring stations have been deployed primarily to locations that can meet certain criteria that have eased in the installation and operation while also increasing the odds of capturing live examples of jamming events. The latter point was addressed by preferentially selecting locations which were adjacent to busy roadways based on the belief that observing larger volumes of car and truck traffic would increase the chances of observing in-car jammers/Personal Privacy Devices (PPDs) in the wild. Other site selection criteria included the availability of a sufficiently fast upload connection to support notification and cloud storage of captured data as well as virtual private network access to the station to perform maintenance or the availability of a local specialist to help with updates and troubleshooting. In aggregate, the ARFIDAAS network has captured nearly 20 terabytes of multi-frequency GNSS RFI events, making it the largest such database known by the authors to exist in a centralized form openly available to interested parties. Additional blue markers are included in Figure 7 indicating the locations where ARFIDAAS monitoring stations are planned for deployment within the term of 2022. Notably, near future deployments are intended to include a series of four stations along the Aurora-Borealis [4] road segment in northern Finland.

Figure 7: Locations of presently deployed ARFIDAAS systems in blue, with expected 2021-2022 deployment sites in red.

Regardless of the deployment location, a common factor proved to be the presence in the GNSS signal bands of undesirable yet unfortunately legal uses. Retrospective analysis of these site specific sources indicate that primary RADAR stations, weather radar stations, amateur radio users, and military jamming exercises are responsible for the majority of these events with malfunctioning consumer electronics such as Wi-Fi access points have also been identified. The E6 band in particular has proven to be frequently interfered with by co-authorized users of the band, which is not illegal but does impose limitations on the use of the GNSS signals in this band in these affected areas per [5].

Another interesting observation based on long term monitoring of sites has been that characterizing a site requires an observation period of several months, as month to month variability in the occurrence rates of jamming activity can exceed an order of magnitude. An example of this variability is exposed when the ARFIDAAS collected data is analysed in terms of the occurrence rate of RFI signals falling within the +/- 10.23 MHz bands around the L1, E5a, and E5b centre frequencies at the site hosted by the NLR (Amsterdam, Netherlands) within 2020. As shown in Table 1 the annual average of E5a RFI amounts to 3.9 seconds per day but spiked to 27 seconds per day in July before dropping to only 1.6 seconds per day in august 2020.

Table 1: An example of extreme month to month variability in RFI band occupancy.

	Annual 2020		July 2020		August 2020	
Frequency band	Occurrence rate	Time equivalent	Occurrence rate	Time equivalent	Occurrence rate	Time equivalent
L1/E1	2.2×10^{-4}	19 s/day	2.8×10^{-4}	24 s/day	1.9×10^{-4}	16 s/day
L5/E5a	**4.5×10^{-5}**	**3.9 s/day**	**3.1×10^{-4}**	**27 s/day**	**1.8×10^{-5}**	**1.6 s/day**
E5b	1.2×10^{-5}	1.0 s/day	3.5×10^{-5}	3 s/day	8.5×10^{-6}	0.7 s/day

If the aggregate data for the month of July was used to attempt to characterize the RFI environment at this site, the average level of E5a RFI would be overstated by a factor of 17 compared to the actual annual average. This observation is valuable in that it indicates that such attempts to characterize the typical RFI environment of sites should be based on windows much longer than one month.

An attempt was made for other sites to try and correlate high monthly RFI variability with site traffic rates per [6] and [7], but the results were unclear. For one of the sites operated in Norway the volume of traffic passing is plotted in Figure 8 we can see monotonically increasing traffic activity between January and March of 2021, yet over this same period in Figure 9 there are distinct clusters of activity and gaps. Taken together these observations suggest that traffic volume alone is not a good predictor of short term RFI activity levels in the L5/E5 band. Based on the information shown in Appendix A, traffic volume does serve as a good predictor of total RFI activity, however when combined with these observations it is clear that the period of observation and site-specific activity can still dominate on the sub-year time scale.

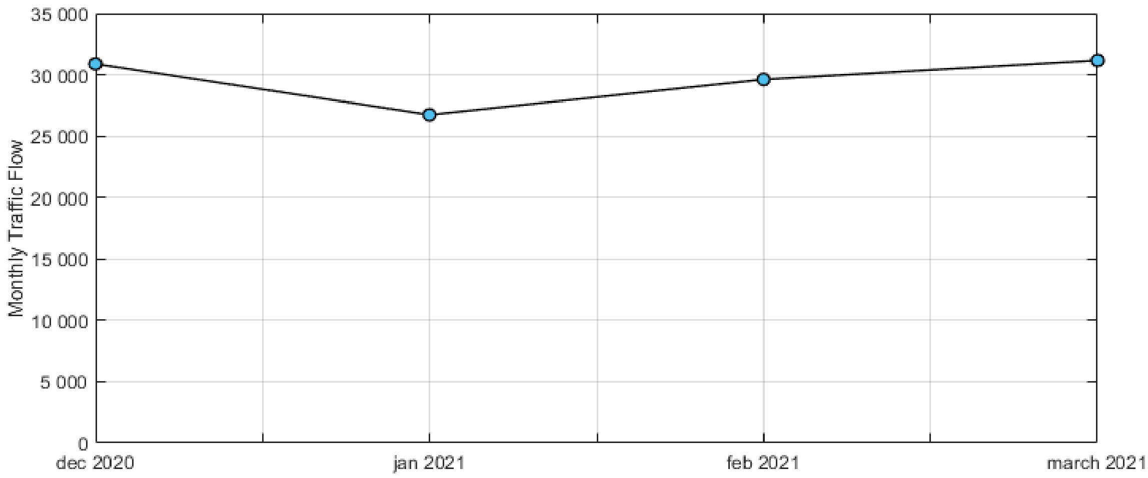

Figure 8: Traffic flow rates adjacent to one of the ARFIDAAS monitoring stations, (data source: https://www.vegvesen.no/trafikkdata) The period shown corresponds to that of Figure 9.

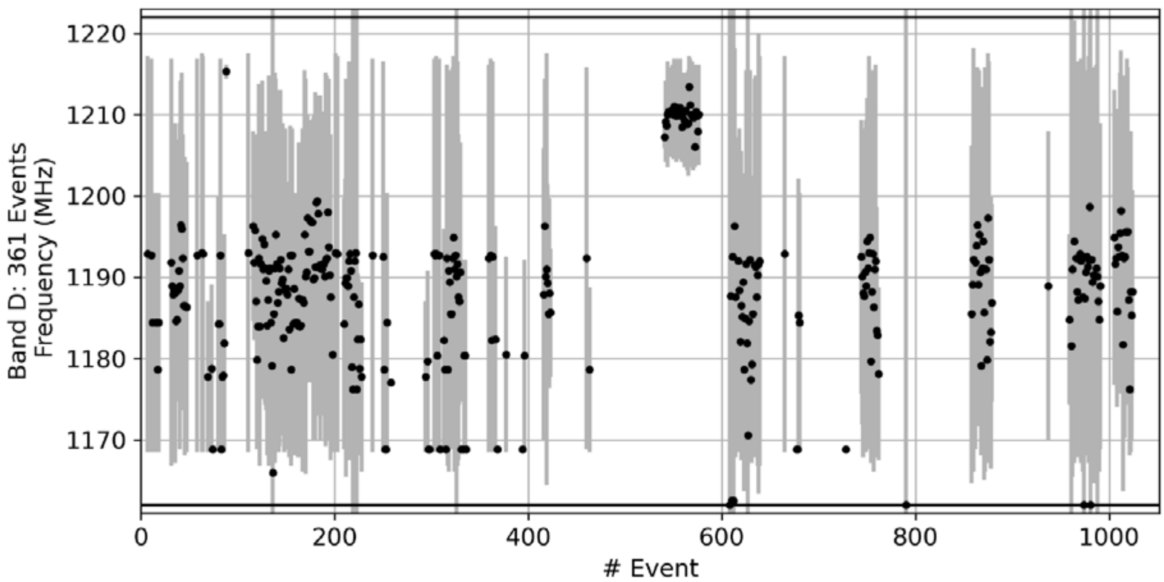

Figure 9: E5 band occupancy of RFI events between January and march of 2021.

An additional notable observation is the ratio of narrowband or CW events detected within the 1560-1610 MHz band and the number detected between 1170 and 1280 MHz combined as shown in Figure 10. Despite the fact the upper GNSS bands occupy approximately half the amount of spectrum as the lower GNSS bands the occurrence rate of narrowband and CW events within the upper 50 MHz can be nearly ten times more than the number captured in the lower 100 MHz of spectrum during the same periods. Based on discussions with the national spectrum management authority of Norway (Nkom) it is believed that the majority of narrowband and CW events in the L-band are due to malfunctioning GNSS receivers self-oscillating or otherwise leaking power in the L1 band, ostensibly without jamming themselves. If these events were uniformly distributed over the L-band we would expect to see approximately a 2:1 ratio of low band events to high band events rather than the observed 1:10 ratio. If the explanation of the source of these narrowband events is accurate then we might expect to see an increasing prevalence of E5, L2, E6 RFI events as low-cost dual-frequency receivers begin to proliferate in the marketplace.

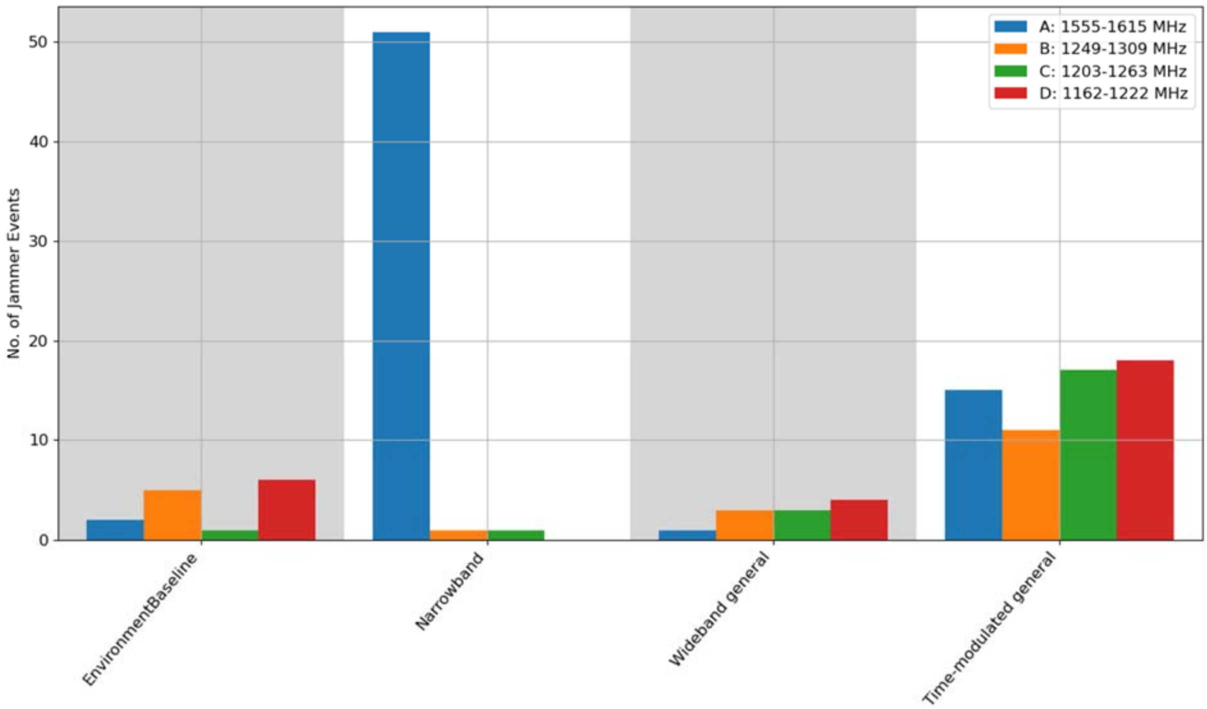

Figure 10: Most captured upper L1 band RFI is narrowband in nature

In comparison to other studies of RFI and jamming sources such as those in [8], the data captured by the ARFIDAAS system has expanded the envelope of devices observed in the wild in terms of bandwidth and sweep rate. When focusing on chirp events specifically, the ARFIDAAS system has observed sources that have bandwidths in a single band of greater than 100 MHz (assuming the signal does not have dead-bands when it leaves the monitored edge of the spectrum). Other devices have been observed with chirp repetition rates of approximately 2 MHz which is a repeat rate on the edge of ability of the reporting software to discriminate between this and a general wideband modulation due to the limits of the used FFT window size limiting the time resolution.

4. Conclusions and data availability

The large quantities of RFI observation data produced by the ARFIDAAS monitoring stations have allowed the authors to observe multiple important real-world aspects of interference signal characteristics including the fact that sites cannot be accurately characterized with only a few months of data. Other factors can now be predicted based on collected ARFIDAAS data, such as the expected increase in narrowband RFI in the E5 and L2 bands due to the availability of low-cost multi-frequency modules on the market.

While the system is optimized to provide rapid reporting to site stakeholders, the centrally collected data is available to allow fine-grained classification and analysis of the collected events, and the production of long-term site and network statistics.

5. 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 [9], preferably one of those being jammer characterization. Radio Frequency Fingerprinting 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 [10].

As of 2021 a new version of the ARFIDAAS hardware and firmware has been designed which is intended to improve the performance of the ARFIDAAS systems. The first of these is that an unexpectedly high number of jammers encountered in the wild have modulation patterns which extend below the typical 1555 MHz lower coverage edge of the system when using a 60 MHz sampling frequency centred at 1585 MHz which results in aliasing in to upper edge of the band near GLONASS G1. To mitigate this the new firmware and software versions support sampling rates up to 75 MHz which limits aliasing effects without sacrificing coverage of B1 or G1 centre frequencies. The new firmware versions have also been adapted to provide better automatic gain control (AGC) feedback response, while the new hardware provides both an increase in AGC resolution as well as an increase in the sampling bit depth from 3-bits to 4-bits per sample. The latter change is expected to be particularly helpful in categorization of CW and narrowband events with high power.

Software evolution within the cloud components in support of fingerprinting and localization will be pursued through 2024. The complexity and large amount of work required for labelling signal data for building the machine learning models has been partially addressed through the large library of collected RFI events combined with automated classification.

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 ARFIDAAS systems for their assistance.

Appendix A: Traffic flow rate comparison

The Norwegian Public Road Administration (NPRA) provides detailed traffic measurement data and maps of available traffic measuring stations such that it is possible to compare the traffic flow an adjacent major roadway for some of the ARFIDAAS stations. In Figure 11 and Figure 12 hourly histograms of RFI and traffic flow are plotted for the E6 motorway directly adjacent to the Trondheim B monitoring station. In this representation there is a clear overall correspondence between traffic volume and observance of RFI events, with the potentially notable exception of a spike and subsequent trough in jamming activity from 15:00-1600 and 16:00-17:00. While the underlying cause of this deviation is not known, it is speculated by the authors that jammer use may be motivated by a desire to hide an early departure from work from a potential fleet management or vehicle tracking system.

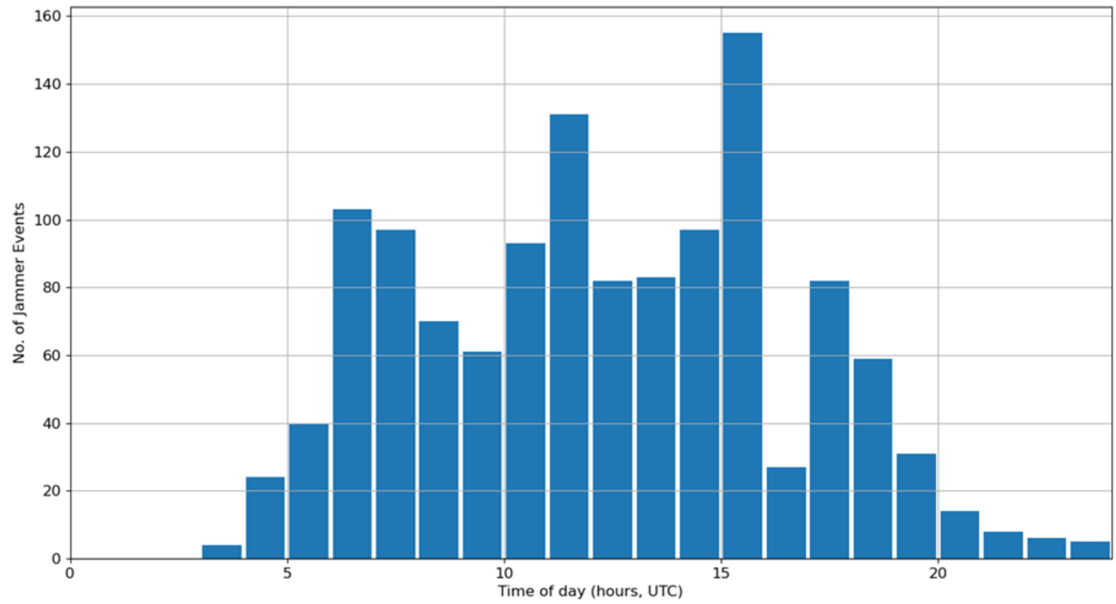

Figure 11: Histogram of jammer events occurrence during a day. Site: TrondheimB, Norway; time period: 01.11.2019-31.03.2021.

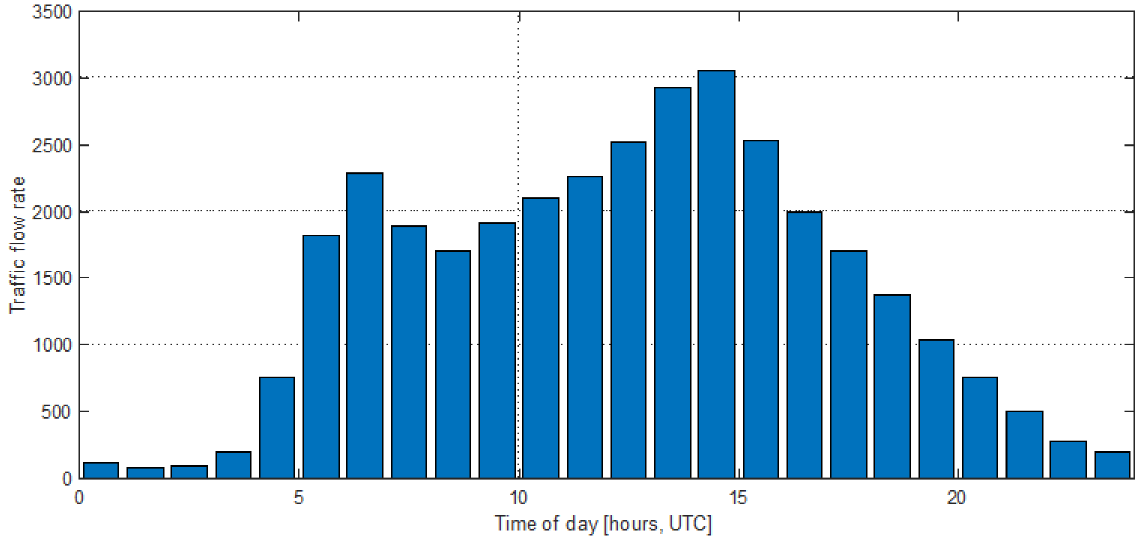

Figure 12: Hourly traffic flow histogram. Site: TrondheimB, Norway; time period: 01.11.2019-31.03.2021. Data source: https://www.vegvesen.no/trafikkdata

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]. Morrison A., Sokolova N., Håkegård J. E., Bryne T. H. and L. Ruotsalainen (2020), A Multi-Site Quad-Band Radio Frequency Interference Monitoring Alerting and Reporting System, in proceedings of the 2020 European Navigation Conference (ENC GNSS), 22-25 Nov. 2020, Dresden, Germany.

[4]. Finnish Transport Infrastructure Agency, Vt 21 Kolari- Kilpisjärvi (Aurora), available at https://vayla.fi/vt21kolari-kilpisjarvi

[5]. Morrison A., N. Sokolova, N. Gerrard, A. Rødningsby and C. Rost (2021), RFI Considerations for Utility of the Galileo E6 Signal, in proceedings of the 34th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2021), 20-24 Sept. St. Louis, Missouri, US.

[6]. Rødningsby A., Morrison A., Sokolova N., Gerrard N. and C. Rost (2020), RFI Monitoring of GNSS Signals on Norwegian Highways, in proceedings of the 33rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2020 Virtual), 21-25 Sept.

[7]. Gerrard N., A. Rødningsby, A. Morrison, N. Sokolova and C. Rost (2021), GNSS RFI Monitoring and Classification on Norwegian Highways – An Authority Perspective, in proceedings of the 34th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2021), 20-24 Sept. St. Louis, Missouri, US.

[8]. Bauernfeind, R. , Kraus, T., Sicramaz Ayaz, A., Dötterböck, D. and B. Eisfeller, Analysis, Detection and mitigation of incar gnss jammer interference in intelligent transport systems, Deutscher Luft und Raumfahrtkongress 2012.

[9]. Trener på elektronisk krigføring - kan forstyrre navigasjon i bil og mobiltelefoner, dresseavisen, 24. February 2020, available 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

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

Aiden Morrison received his PhD degree in 2010 from the University of Calgary, where he worked on ionospheric phase scintillation characterization using multi frequency civil GNSS signals. Currently, he works as a senior research scientist at SINTEF. His main research interests are in the areas of GNSS and multi-user collaborative navigation systems and GNSS RFI monitoring and analysis.

Nadezda Sokolova received her PhD degree in Telecommunications from Norwegian University of Science and Technology (NTNU). She also holds a MSc degree in Geomatics Engineering from University of Calgary, Canada, and a MSc degree in Space and Aeronautical Engineering from Narvik University College, Norway. Currently, she works as a senior research scientist at SINTEF Digital and adjunct associate professor at the Engineering Cybernetics Department, NTNU, focusing on high integrity resilient multi-sensor navigation.