Dynamic RFI Management in Radio Astronomy using Pseudonymetry

Gregory Hellbourg[(1)], Neal Patwari[(2)], Meles Weldegebriel[(2)], and Ning Zhang[(2)]

[(1)] California Institute of Technology, Pasadena, CA, USA
[(2)] Washington University in St. Louis, St. Louis, MO, USA

***Abstract*—This paper addresses dynamic spectrum management and enforcement by introducing the concept of *pseudonymetry* to reliably and securely identify interfering transmissions during spectral resource blocks allocated to passive services. Identified interfering transmitters are notified through a shared database, and requested to stop their operation to protect the passive service observation.**

I. Introduction

A. Radio Frequency Interference in Radio Astronomy

Radio astronomy studies the radio frequency emissions from distant astronomical sources. These emissions are strongly attenuated by large distances propagations, and are orders of magnitude weaker than man-made communication signals when observed from the surface of the Earth. Radio telescopes operate over large bandwidths ($>$ 100s of MHz) to achieve the required sensitivity to detect these faint signals, beyond the protected bandwidths dedicated to passive services. These instruments are therefore usually located in remote areas, far from metropolitan centers, to minimize the impact of radio frequency interference (RFI). The population growth and the rapid development of airborne and spaceborne transmitters result in an increasing risk of RFI to radio astronomy instrumentation. Strong RFI are usually mitigated using sharp analog filters to prevent the radio astronomy receivers to reach non-linear regimes. Weaker RFI are detected at various stages in the telescope signal processing chain with increasing sensitivity, and the affected data are discarded before scientific analysis. In both cases, RFI leads to a data loss which, in turn, reduces the telescope sensitivity and operational efficiency.

B. Dynamic RFI management

The fast development of the field of telecommunications urges engineers to consider dynamic spectrum access schemes, in which unused spectral resources allocated to primary users are made available to secondary users. This dynamic spectrum management has been succesfully demonstrated with the Citizens Broadband Radio Service [1], [2]. Passive services, such as radio astronomy, may benefit from such schemes, in which spectral resources outside the protected bands could be temporarily allocated to them to conduct sensitive measurements. Such a dynamic process would however require ways of uniquely and robustly identifying transmissions that interfere with a primary user. An RFI monitoring station near the radio astronomy instrument would then be in charge of detecting and identifying interfering emissions, and communicate to them a request to stop their operation. We propose pseudonymetry as a solution for the detection and identification problem.

II. Pseudonymetry

Pseudonymetry is accountable by allowing transmissions to be identified from a watermark, but it is designed to allow the user to remain anonymous. We accomplish this privacy goal by having the transmitter randomly generate a (changing) pseudonym as the identifier to encode in its watermark. Another challenge in RFI identification is that RFI can prevent radio astronomy use of the spectrum even when the RFI is too low in $\frac{\mathcal{E}_b}{N_0}$ (bit energy to noise energy ratio, i.e., SNR in energy terms) to have its data be demodulated. When it cannot be demodulated, packet data cannot be used to identify the device. Our solution is to use a low-rate watermark that can be decoded even at a very low $\frac{\mathcal{E}_b}{N_0}$. In pseudonymetry, a passive monitoring station that identifies a transmitter's pseudonym forces it to stop via an intermediate database. The monitoring station posts the timestamp and pseudonym to the database, and all active transmitters using the protected band must periodically check the database and stop the offending transmission if its used pseudonyms are reported. By this process, we enable privacy-preserving feedback to the active offending transmitter, and thus allow passive receivers to stop interfering emissions [3].

Watermarking must encode the pseudonym so as to not impact reception of the transmitted data, and being able to be demodulated by the monitoring station at very low $\frac{\mathcal{E}_b}{N_0}$. This has led us to investigate amplitude-based watermarking. When using a low amplitude modulation index, this watermarking would appear to the receiver to be similar to channel fading, but with much lower impact. In our future work, we are also investigating frequency shift-based watermarking, which would be smaller in impact than Doppler effects in mobile radio. Both methods allow standard receivers to mitigate the impact of the watermark.

Pseudonymetry works as follows: Wireless devices that are permitted to transmit in the protected spectrum must watermark their transmissions with a pseudonym. These pseudonyms are unique and only known to the transmitting device. At the passive monitor, a receiver demodulates any pseudonym in any measured RFI and writes it to a remote database. An active transmitter must check this database and if it finds its own pseudonym, it must move out of the band.

A main watermarking challenge is to enable pseudonym identification feasible at very low SNR. Our analytical and

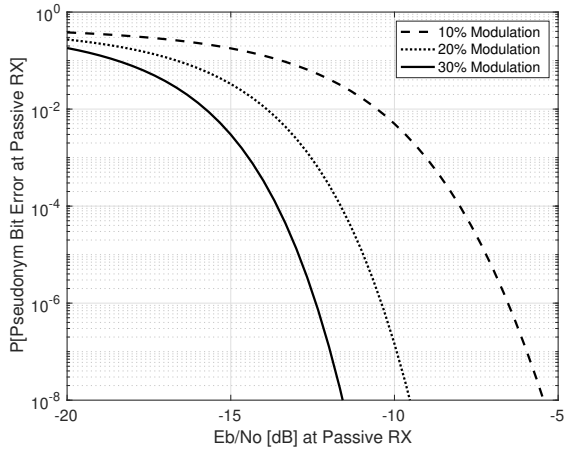

Fig. 1. Probability of pseudonym bit error vs. modulation index m and the $\frac{\mathcal{E}_b}{N_0}$ of the data bits, for $N = 6{,}000$ data symbols per pseudonym bit.

simulation results show that amplitude watermarking with a modulation index of 20% demonstrates that pseudonyms can be demodulated at $\frac{\mathcal{E}_b}{N_0}$ values as low as -15 dB [3]. For example, at $\frac{\mathcal{E}_b}{N_0} = -10$ dB, pseudonym bits can be detected with BERs on the order of 10^{-5} as shown in Fig. 1. For perspective, this is 20 dB lower than the transmitted data bits can be demodulated with this BER. A 20% modulation index means that the transmit signal amplitude increases or decreases by 20% compared to its mean, which represents a 3 dB investment by the transmitter in power for the watermark.

We have also performed experimental tests on PhantomNet [4] that validate these results using RF transmitted signals and a software-defined radio implementation (results in review).

III. Security and Privacy

One of the challenges in the Pseudonymetry system is to ensure the privacy of the operating transmitters, since owner private information can be inferred from both the location as well as the transmission pattern. One way that the system protects privacy is to set the pseudonym to be a random bit string, unrelated to any identification information of the transmitter. Thus the pseudonym itself does not provide information about what device is transmitting, and further breaks the linkability between the pseudonym and original unique identifier. However, through correlation of the transmission record and prior information on the target, there remains privacy risks. To further ensure the privacy leakage is minimized, we propose to leverage differential privacy to quantitatively limit privacy leakage.

On the security protection front, it is crucial to ensure passive receiver's ability to operate robustly in the presence of malicious attackers. To accomplish this, we will adapt recent advances in software attestation to develop proof of correct execution of spectrum decision on user equipment (UE), and complement the watermark-based detection system with spectrum policy enforcement on the UE.

IV. Implementation

Validation of pseudonymetry requires the development of a spectrum monitoring station able to detect weak interfering signals, and capture their raw data to extract their watermarked pseudonym. We implemented a software-defined radio analysis pipeline that captures the in-phase/quandrature (I/Q) samples in a given frequency band, and converts them in real-time into power spectra The spectra are then tested using a power detector, and above-threshold event, typically associated with the presence of a signal, triggers then an I/Q data file writer to either disk for offline processing and archival, or to a circular memory buffer for a fully streamlined pipeline architecture. The I/Q data files are then analyzed using a pseudonym reader, and pseudonyms are then written into a shared database. The current implementation is based on the Aaronia RTSA suite [5], and an alternative GNU Radio flowchart will follow. Current tests involve the monitoring of passive services protected bands (e.g. 1,400-1,427 MHz) and cellular uplink bands to validate the I/Q data writing process. Over-the-air testing with synthetic transmissions are planned to validate the full real-time pipeline.

V. Conclusion

Dynamic spectrum access presents a unique opportunity for passive services, such as radio astronomy, to gain access to portions of the spectrum that are lost due to heavy active users usage. The enforcement of dynamic access regulation is however critical to ensure the fairness of the system. Pseudonymetry offers a unique solution for spectrum sharing that preserves communication user privacy while enabling a radio astronomy receiver to shut off the particular transmitter causing it measurable RFI, even at a low SNR. The concept has currently been validated in a wired experimental setting, and will soon be tested in various over-the-air configurations.

ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under the Spectrum Innovation Initiative (SII) Spectrum and Wireless Innovation enabled by Future Technologies grant #2229428 "Collaborative Research: SWIFT: Closing the Loop for Accountable Interference-free Spectrum Sharing with Passive Radio Receivers"

References

[1] Mun, Kyung. "CBRS: New shared spectrum enables flexible indoor and outdoor mobile solutions and new business models." White Paper, Mar (2017): 25.

[2] Caromi, Raied, Michael Souryal, and Wen-Bin Yang. "Detection of incumbent radar in the 3.5 GHz CBRS band." 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2018.

[3] Weldegebriel, Meles G., Jie Wang, Ning Zhang, and Neal Patwari. "Pseudonymetry: Precise, Private Closed Loop Control for Spectrum Reuse with Passive Receivers." 2022 IEEE International Conference on RFID (RFID).

[4] Banerjee, Arijit, Junguk Cho, Eric Eide, Jonathon Duerig, Binh Nguyen, Robert Ricci, Jacobus Van der Merwe, Kirk Webb, and Gary Wong. "PhantomNet: Research infrastructure for mobile networking, cloud computing and software-defined networking." *GetMobile: Mobile Computing and Communications*, 19(2), pp. 28–33, 2015.

[5] https://aaronia.com/en/products/software/rtsa-software