Collaborative Research: SWIFT: Closing the Loop for Accountable Interference-free Spectrum Sharing with Passive Radio Receivers

Neal Patwari[1], Ning Zhang[1], and Greg Hellbourg[2]

[1]Washington University in St. Louis, [2]Caltech

Abstract

NSF Award #2229427, 2229428: We are developing, implementing, and testing methods to share spectrum reliably with passive radio users, like radio telescopes, by providing new feedback & accountability mechanisms, which we call **pseudonymetry**. With a secure and reliable feedback mechanism, we can handle the *worst-case* interference and design sharing systems for the average case. Our work hopes to increase the efficiency of use of valuable spectrum resources, which are important for multiple scientific, government, and commercial purposes, without allowing interference between users. We are experimenting on the POWDER testbed as well as at the Owens Valley Radio Observatory.

Motivation

What if a passive receiver could identify enough info about the particular interfering TX to force it off? Could we enable more efficient spectrum sharing that provides passive receivers the control to remove interferers?

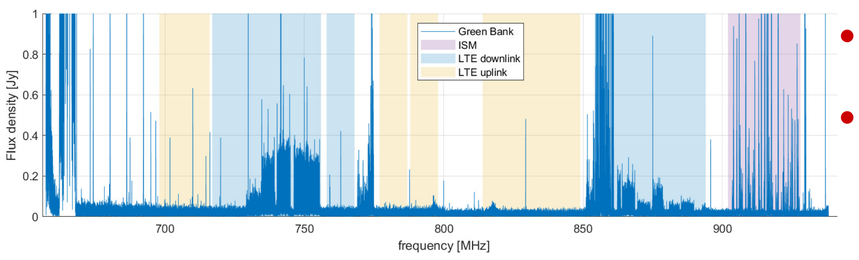
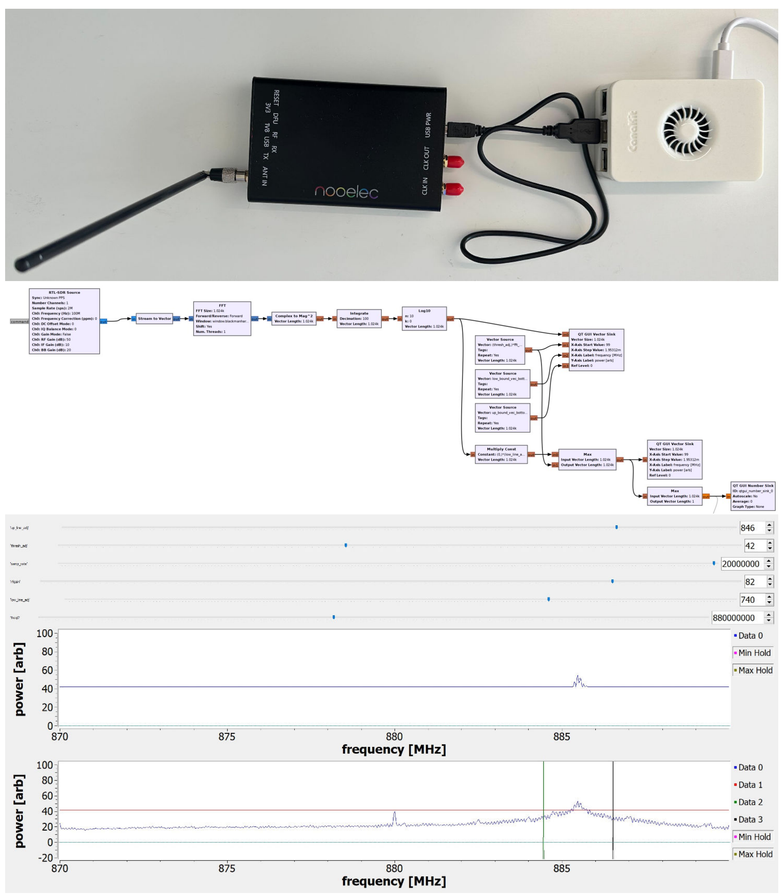


Figure: RFI flux density scan captured with the Green Bank Telescope, WV, in the National Radio Quiet Zone, on 8 Apr. 2019, averaged over 356 seconds. The data is expressed in Jansky, 1 Jy $= 10^{-26}\text{Wm}^{-2}\text{Hz}^{-1}$ [5].

Embedded Spectrum Monitor



We developed a low-cost spectrum monitor based on a Great Scott Gadget HackRF front-end and a Raspberry Pi running GNU Radio. The system is able to monitor a 0-6 GHz range with a 20 MHz instantaneous bandwidth. Per frequency thresholds are user-set. The baseband data download is triggered upon above-threshold signal detection. The collected baseband data is then processed by an offline processing pipeline dedicated to the pseudonym extraction and database interaction.

Further work will include testing the system with controlled pseudonym-embedded transmissions at the Owens Valley Radio Observatory.

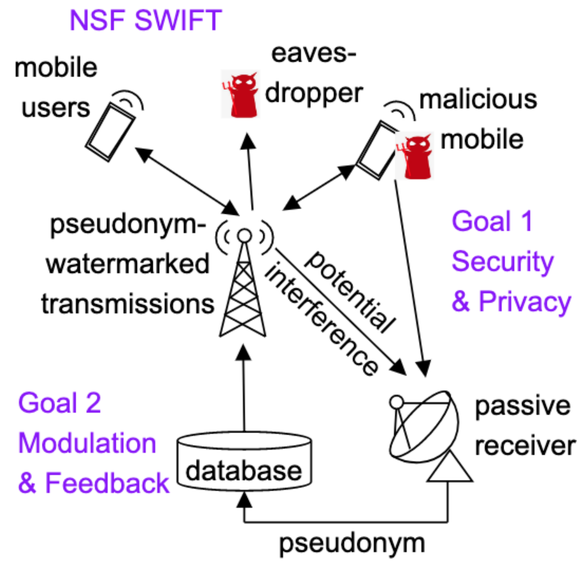
Want to Know More?

`https://pseudonymetry.com`

Pseudonymetry Idea

Add feedback loop to a spectrum sharing system [1]:

- Watermark each packet w/ a random *pseudonym*
- Passive receiver demods pseudonym & uploads to DB
- Devices must check DB; switch band if its pseudonym reported



Research Progress

- How does a transmitter's watermarking impact data reception at intended receivers?
- How well are pseudonyms received vs. $\mathcal{E}_b/N_0$

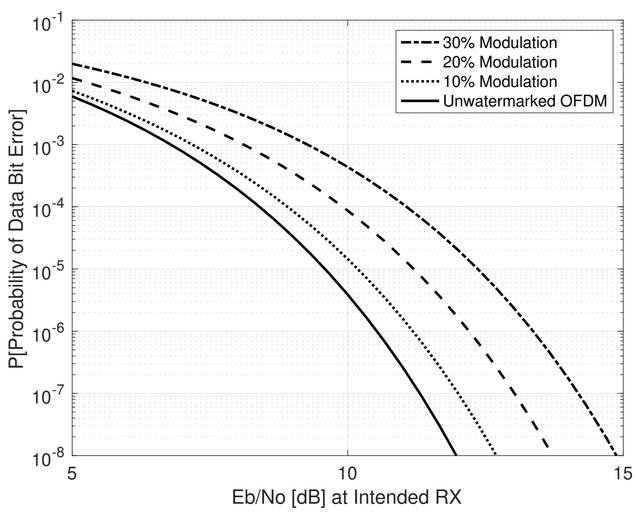


Figure: Probability of data bit error vs. $\mathcal{E}_b/N_0$ for 3 modulation indices.

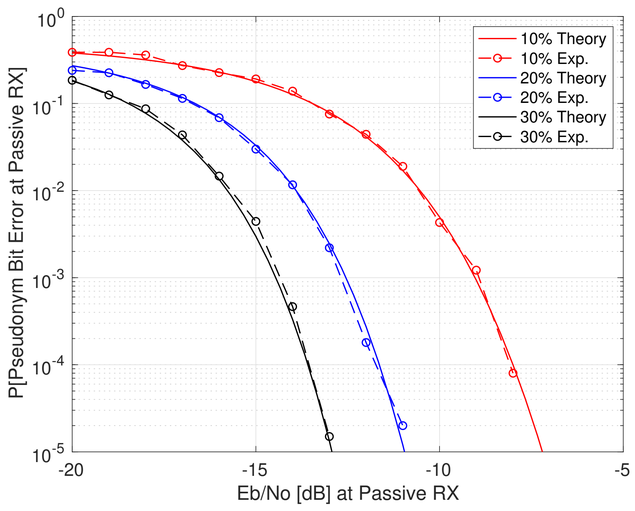


Figure: Experimental results on PhantomNet, vs. theoretical

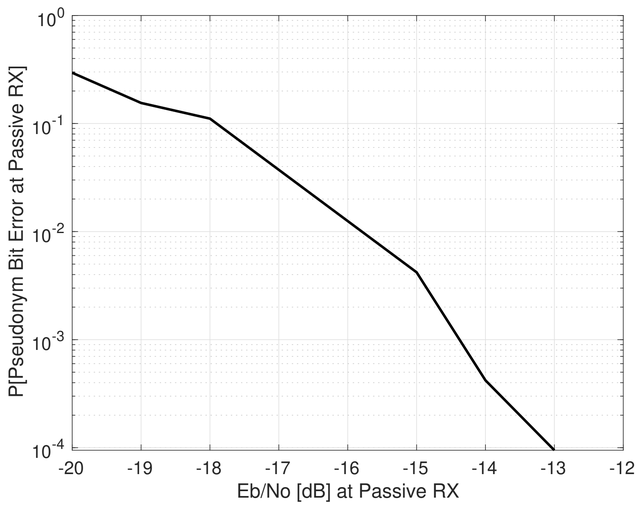
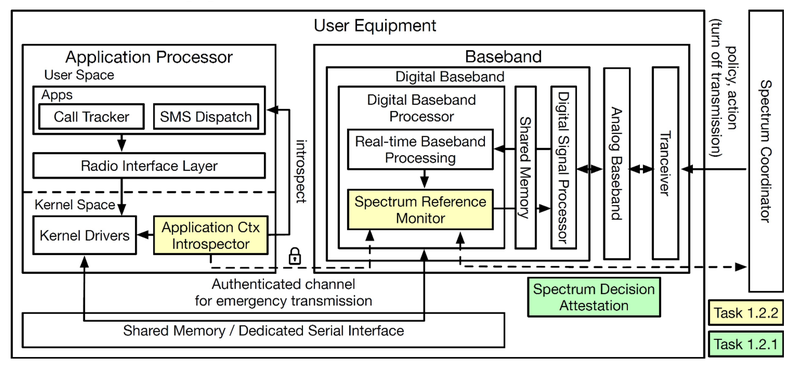


Figure: Over-the-air Pseudonymetry Experiment. Pseudonyms are transmitted over a separate subchannel in an OFDM signal.

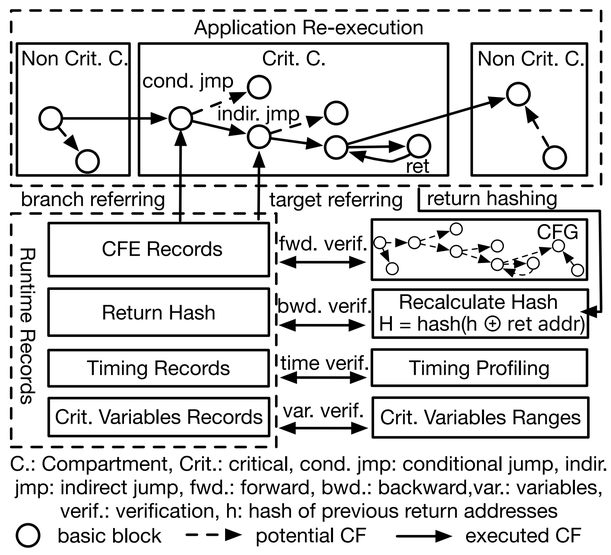
Security and Privacy

There are several security and privacy objectives in this project.

Privacy Protection: We assume the Pseudonymetry database and the Passive RX are both trusted. From the privacy perspective, the attacker's goal is to infer private spectrum user information by correlating transmitted pseudonyms. In our preliminary work [1], this is addressed by randomizing the watermark ID used in the transmission. However, using the pseudonym alone does not eliminate the possibility of correlating multiple transmissions from the same pseudonym to infer the user's pattern of life. Yet, when the watermark IDs are completely randomized, it significantly increases both the processing time and storage overhead of the system. Furthermore, it is important to be aware of the privacy risk of leakage from the intelligent control driving decisions in the spectrum management [3].



Security Protection: While much of the existing literature of co-existence focuses on spectrum management, little has been done to examine the enforcement on the user equipment. From the security perspective, our project aims to complement the interference detection system by completing the end-to-end protection via novel transmission policy enforcement mechanisms. In our recent work [4], we proposed a new real-time attestation system, shown below, that leverages software compartmentalization to enable a trade-off between the level of details on measurement and performance. This enables attestation of not only the correctness of spectrum operations, but also its timeliness.



References

[1] Meles Weldegebriel, Neal Patwari, Ning Zhang and Jie Wang, "Pseudonymetry: Precise, Private Closed Loop Control for Spectrum Reuse with Passive Receivers", in *IEEE Intl. Conf. on RFID - Workshop on Digital Spectrum Twinning*, Las Vegas, 17 May 2022.

[2] Meles Weldegebriel, Neal Patwari, Ning Zhang and Greg Hellbourg, "Watermarking of OFDM for Pseudonymetry: Analysis and Experimental Results", in *IEEE ICC - Workshop on Catalysing Spectrum Sharing via Active/Passive*, Denver, Scheduled for June 9, 2024.

[3] Han Liu, Yuhao Wu, Zhiyuan Yu, Ning Zhang, "Please Tell Me More: Privacy Impact of Explainability through the Lens of Membership Inference Attack", to appear in *IEEE Symposium of Security and Privacy*, Oakland, May 2024.

[4] Jinwen Wang, Yujie Wang, Ao Li, Yang Xiao, Ruide Zhang, Wenjing Lou, Y. Thomas Hou, Ning Zhang, "ARI: Attestation of Real-time Mission Execution Integrity", in *USENIX Security Symposium*, Anaheim, Aug 11 2023

[5] Green Bank Telescope Interference Protection Group, Online: `https://www.gb.nrao.edu/IPG/`.