Pseudonymetry: Precise, Private Closed Loop Control for Spectrum Reuse with Passive Receivers

Meles G. Weldegebriel*, Jie Wang, Ning Zhang, and Neal Patwari
McKelvey School of Engineering
Washington University in St. Louis, Missouri, USA
*Email: g.weldegebriel@wustl.edu

***Abstract*—Radio astronomy and other passive radio spectrum users have significant challenges avoiding interference from wireless communication systems. Even distant transmitters sometimes interfere with passive users. We propose *Pseudonymetry*, a system that provides (primary) passive users a means to turn off the transmissions of the particular (secondary) wireless transmitter that interferes with it. By controlling the specific transmitter rather than an entire geographical region, Pseudonymetry could increase the spectrum available for wireless systems while ensuring rapid clearing of interferers as necessary for passive use. Pseudonymetry adds a low rate watermark to the secondary (intended) transmitted signal to carry a random, anonymous pseudonym. We show the ability of a passive receiver to decode the watermark, even from a signal received with very low SNR. The passive receiver posts to a centralized database to provide feedback to the secondary transmitters so that they know to vacate the band. We provide analysis that captures the trade-offs in the design of Pseudonymetry, and show initial evidence that a simple amplitude modulation watermarking scheme could enable reliable detection at a distant passive receiver, while resulting in minimal degradation to the error performance of the intended secondary receiver.**

***Keywords*—** Radio Frequency Interference, Radio Astronomy, Coexistence, Passive Receivers, Commercial Wireless Systems

I. Introduction

The increase in demand for wireless services have imposed pressure on spectrum stakeholders to make technological and regulatory reforms on how the spectrum should be allocated and utilized. Coexistence of different wireless systems with heterogeneous access and interference protection rights particularly demand a paradigm shift [1] on how the spectrum should be shared among all current and future users and uses. Dynamic spectrum access techniques have brought about opportunistic access in underutilized portions of the spectrum, by allowing secondary users to use a band when it is free of primary user transmissions. This approach, however, is not applied when the primary users are passive receivers, whose state cannot be determined through spectrum sensing [2]. Radio astronomy systems (RAS), for example, are designed to receive faint signals from distant stars and galaxies [3] and secondary users cannot determine via spectrum sensing whether or not the RAS system is receiving.

Currently, RAS systems are protected by large geographic radio quiet zones (RQZ) [3], where wireless transmissions are partially or fully restricted. Special regulations have also been put in place to protect these passive receivers from radio frequency interference (RFI). Nevertheless, passive receivers still suffer from RFI caused by domestic and commercial transmissions [4]. For example, an airplane in the wrong position in the sky can provide a temporary but strong reflection that allows a signal from a distant transmitter to cause interference with a radio astronomy receiver. Note that a signal causes interference to a passive receiver well below the SNR at which the signal's data can be demodulated. After-the-fact interference removal

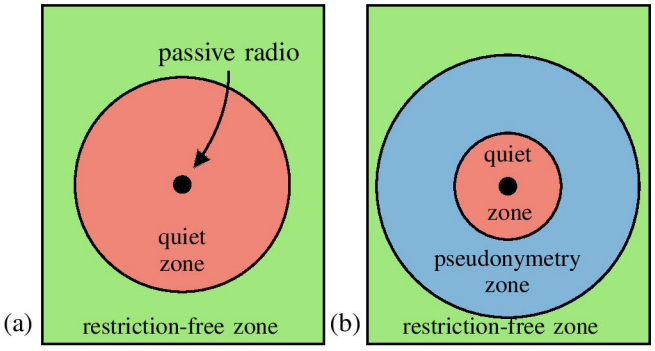

Fig. 1: (a) Radio quiet zones prevent active spectrum use in very wide areas around a passive radio. (b) We propose sharing spectrum in an intermediate area where transmitters might occasionally interfere but Pseudonymetry enables the passive radio to rapidly disable interferers.

[5] is a useful tool, but is unable to completely remove interference, particularly when the signal is at low SNR and via an unknown dispersive channel.

Thus a critical question is, how can passive receivers force an interferer to stop transmitting? In theory, the location of an interference source could be estimated, and once located, someone could force it to turn off; but the process can be human-intensive and slow. As an example, consider it took two years to force a man to turn off a cell-phone jammer he turned on whenever he was driving [6]. Long-distance source localization is coarse, so forcing off *all* transmitters near the estimated source may be too extreme of a solution. At the SNRs at which the source causes interference at the passive receiver, there is typically no way to demodulate the packet data, and thus no way to identify the unique transmitting device.

This paper proposes a protocol to enable a passive receiver to force an interfering transmitter to stop transmitting, even when the interfering data is too low in signal power to demodulate. Our insight is to add low rate pseudonym symbols onto the signals from all coexisting transmitters such that the passive receivers would be able to demodulate the pseudonym even at very low power levels. With this ability, we can develop a class of systems that would enable coexistence between passive receivers and commercial wireless systems. With the ability of the passive receiver to demodulate the pseudonym, they can force the transmitter to switch band.

Currently, coexistence of passive receivers and wireless communications systems take one of two extremes. The first scenario is that the passive receivers are essentially disabled when they are interfered with by the communications transmissions, unable to receive their intended signals. This is particularly true for radio telescopes, which are designed to receive faint signals from billions of miles away. The second scenario is that communications systems may not use the spectrum in a wide area around the passive receiver, called a

2022 IEEE International Conference on RFID (RFID) | 978-1-6654-1046-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/RFID54732.2022.9795976

978-1-6654-1046-5/22/$31.00 ©2022 IEEE

radio quiet zone, for fear of even occasional interference to the passive incumbent users. This area must be extremely wide so that transmitters not even occasionally interfere with the passive user. Neither extreme provides for efficient spectrum use.

The middle ground between the two extremes above is what we propose as Pseudonymetry. We suggest a smaller quiet zone, in which no coexisting wireless system may operate in the spectrum used by the passive user. Outside of this smaller quiet zone, a wireless system may use the spectrum using Pseudonymetry. Finally, very far from the passive users, we would allow wireless systems to operate without using Pseudonymetry.

Pseudonymetry employs a database, separate from the passive receivers and the wireless system operators. When the passive receiver senses an interfering signal, it decodes the signal's pseudonym and writes it to this database. All transmitters must periodically check the database. If they find a pseudonym they used, they must avoid using the frequency bands used by the passive receiver. This process allows a passive receiver the ability to control the particular transmitters causing the interference.

This paper suggests an architecture for Pseudonymetry, a system that would provide a mechanism to allow wireless communications systems to share spectrum with a passive user in some geographical area while allowing the passive user the ability to turn off particular interfering transmitters. As we describe, Pseudonymetry doesn't intrude on the privacy of its wireless communications users, as their identity remains private. We explore the design of the components of the system, and analyze and evaluate a particular watermarking design. We discuss particular questions that remain to be addressed in order to make Pseudonymetry a reality.

II. Related Work

The need for efficient utilization of the radio spectrum has been on the agenda for regulators, policy makers, researchers and industry. There have been tremendous developments in spectrum regulation, wireless systems and technologies that could provide efficient use of the spectrum; but existing approaches are limited. When the idea of cognitive radio (CR) was first conceived [7], it created an opportunity for secondary users to sense the spectrum and opportunistically use it when licensed users are not transmitting. While this innovative approach provided an opportunistic use of the spectrum by secondary users, interference occurs when spectrum sensing measurements and predictions are incorrect [8]. Many methods including cooperative sensing [9] and adaptive database-driven sensing [10] have been proposed to improve the accuracy of spectrum sensing, but RF interference remains a significant challenge. Numerous dynamic spectrum sharing mechanisms have also been proposed to increase the efficiency of spectrum use. These methods share the limited spectrum dynamically in different dimensions: frequency, time, location, users and networks [1]. However, the spectrum is still underutilized and there is a need for spectrum allocation and sharing technologies to allow increased spectrum use.

Passive receivers such as radio astronomy systems occupy wide portions of the spectrum, and also have growing demand for wider frequency bands. However, interference from terrestrial transmitters is a major problem [11]. Today, even geographical isolation [12] is not enough to reduce the interference levels at passive receivers. The number of, and frequency ranges used by, wireless systems has increased; and commercial and personal wireless utilization are increasing close to the reserved quiet zones, causing significant challenges to the normal operation of the passive users. Work to mitigate this problem can be categorized into three approaches: RFI cancellation at passive receiver, power control at transmitters, and multiple access schemes.

RFI Cancellation Schemes: One of the oldest ways to mitigate interference at passive receivers is through radio frequency interference (RFI) cancellation. RAS systems use RFI estimation and cancellation techniques to remove an unwanted signal from a primary signal. For example, [13] detects and removes GSM signals at a passive receiver. A receive antenna array (with 10-30 elements) together with spectral and spatial processing techniques are used to remove the narrow band interference coming from a TDMA GSM signal. Non-linear interference cancellation schemes are also proposed in [14], [15]. They use a two-element receive antenna array [16] to estimate and cancel interference at a radio astronomy receiver. The problem with RFI cancellation is that cancellation is imperfect due to an unknown and changing wireless channel, which can't be estimated perfectly.

Power Control Schemes: The second approach for RFI mitigation at the passive receivers is through control of the transmit power at the interfering wireless device. Different techniques have been proposed for power control. The paper [17] proposes a power control algorithm to reduce the size of the "radio quiet zone" while working below the recommended maximum RFI power level [18]. The innovative research work in [19] presents a base-station antenna signal generation modification approach to suppress interfering signals in the direction of the radio astronomy station. Power control schemes reduce RFI and allow for better geographic coexistence between passive receiver and wireless systems. However, passive receivers are so sensitive that even a reduced level of RFI could prevent normal operation. Pseudonymetry is complementary in that the RAS system can force the interferer to turn off or switch band, thus completely eliminating the interference to the passive receiver.

Multiple Access Schemes: Time and frequency division based multiple access schemes have also been proposed for the coexistence of multiple wireless systems on the same frequency bands. The paper in [20] proposes time division approach where WiFi systems near a radio astronomy receiver share the spectrum based on a predetermined time slots. A general-purpose time-frequency division spectrum access scheme is presented in [21]. Multiple access schemes provide geographic coexistence i.e., passive receivers may operate at the same place with other wireless systems, but not at the same combination of time and frequency at the same time. When multiple access schemes are fully developed to accommodate various wireless systems, they could create access to the frequency band occupied by the passive users; completely eliminating the need for radio quiet zones. However, passive receivers operate on large portions of the spectrum, and having time-synchronized control systems for multiple and heterogeneous wireless systems is a fundamental unsolved problem. A transmitter with poor or incorrect time or frequency synchronization could cause problems with a passive receiver, which would have no means to address the issue. Pseudonymetry provides a complementary capability, a means to force a device to stop using the band.

III. System Components

The overall operation of Pseudonymetry is as follows. We refer here to a passive receiver, such as a radio astronomy system, as the primary user of the band. We assume wireless communications devices may transmit, but are operating with lower priority and as such will vacate the band if asked. We refer to these simply as the transmitters. All such transmitters that want to operate on the same frequency band as the passive receivers must embed a randomly-generated pseudonym in their transmitted signal. The pseudonym and embedding method is designed to have minimal impact on the normal operation of the intended wireless communications system. The pseudonym contains information that can be decoded by the passive receiver even when its signal power is very low, and used to enable the following control mechanism. As passive receivers do not transmit, the closed loop control mechanism must involve a separate communication strategy. Further, the pseudonym does not contain any information about the identity of the transmitter, so direct communication with the transmitter is also not possible.

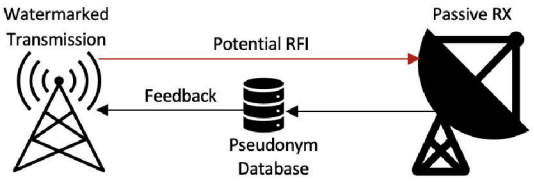

Fig. 2: Pseudonymetry allows a passive receiver to write to a database that prevents an interferer from transmitting.

Instead, Pseudonymetry is designed to work through a database that closes the feedback loop with the transmitter. The passive receiver uploads any pseduonym of an interfering signal to this database, and transmitters are required to periodically check the database and move off the band whenever they find any of their own pseudonyms. In short, a transmitter may transmit in the shared band only if the passive receiver demonstrates that it has not observed the transmitter's signals.

A. Overview

The Pseudonymetry system consists of three components as shown in Figure 2: the transmitter, the passive receiver and the database system. The transmitter is operating as part of a wireless system that intends to share the spectrum with passive users, with priority given to the passive receiver. For example, the wireless transmitter could be a WiFi device or a mobile base station. The passive receiver is any remote receiver such as a radio telescope. We assume a passive receiver that can be used, in parallel with its normal receiver operation, use the received signal whenever there is measurable interference to demodulate the pseudonym. The database system allows authenticated access to passive receivers to write any demodulated pseudonym, and allows transmitters to read the current list of pseudonyms and their time stamps.

B. The Active Transmitter

Broadly, we imagine that a variety of RF watermarking schemes could be possible within a pseudonymetry architecture. However, there are three main features necessary:

1) The watermark must be able to be demodulated even when the transmitter's data cannot. That is, it must be able to be received at SNRs lower than the lowest SNR which would allow decoding of the transmitted data modulation.
2) The watermark should not significantly impact the demodulation of the intended data signal.
3) The watermark should not change the average power of the transmitted signal.

In this paper, we explore a Psuedonymetry system implementation that uses pulse amplitude modulation for its watermarking scheme to embed the pseudonym on to the host signal. We assume the pseudonym is generated in such a way that there are approximately equal number of ones and zeros so that the average energy over all pseudonyms remain approximately constant. Before transmission, the transmitter accesses the database and downloads a list of recent pseudonyms observed by passive receivers. If none of the reported pseudonym & corresponding time stamps match the pseudonyms it has used at those times, then the transmitter is allowed to continue operation in the band. It creates a current pseudonym and sends data packets in the next period of time. This process is repeated by the transmitter before each period of packet transmissions at the active wireless transmitter.

Figure 3 shows the pseudonym generation and embedding scheme. The host signal is amplitude modulated by a pseudonym signal to give the watermarked signal.

Amplitude Watermarking: In this paper, we detail an amplitude-modulation method for the watermarked signal per packet. We create this watermarked transmit signal, $s_p(t)$, as:

$$s_p(t) = [1 + q(t)] \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \sqrt{\mathcal{E}_b} a_{n,k} \phi_{d,k}(t - nT_d), \qquad (1)$$

where T_d is the data symbol (which we refer to as the "d-symbol") period, $\phi_{d,k}(t)$ is the kth orthonormal waveform in our basis for the data symbols, and $a_{n,k}$ is the amplitude of the kth waveform sent during d-symbol period n, and $q(t)$ is the amplitude watermark signal. Note if $q(t) = 0$, the transmitted signal is a standard non-watermarked digital modulated signal. The watermark $q(t)$ multiplies the amplitude of the standard data modulation signal, but at a much slower rate than the data signal. The idea is that digital wireless receivers are already robust to slow changes caused by channel fading to the amplitude of received packets. By mimicking fading in a watermark, we can avoid changing the design of the intended receiver of the data signal.

The watermark $q(t)$ can be generally written as:

$$q(t) = \sum_{l=0}^{L-1} \alpha_l \phi_{p,l}(t - lT_p), \qquad (2)$$

where l is the pseudonym symbol (p-symbol) number[1], α_l is the amplitude of the lth p-symbol and $\{\phi_{p,l}(t)\}_l$ are an orthonormal basis for p-symbol modulation. Note that $T_p \gg T_d$, perhaps by two or three orders of magnitude.

The amplitudes $|\alpha_l|$ over all l in (2) control the percent modulation of the watermark amplitude modulation. The higher the level of modulation on the host signal, the easier it is to demodulate the pseudonym symbols at the passive receiver, but the higher the negative impact on the error performance of the data symbols at the intended receivers.

To study a concrete example, and to provide an analysis of this tradeoff in one setting, we study $L = 1$ pseudonym modulation with $\phi_{p,0}(t)$ set to a rect/NRZ function, that is, $\phi_{p,0}(t) = 1$ for $0 \le t \le T_p$. Further, we assume a transmitter that sends BPSK-modulated data symbols and is a packet radio. Finally, we set T_p to the packet duration, so that we are sending one pseudonym bit per packet. In this case, it requires multiple packets to convey the full pseudonym. We call this the PAM example system in this paper.

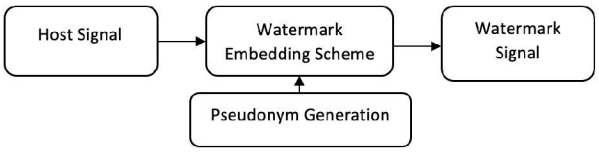

Fig. 3: Pseudonym embedding: a random pseudonym is generated and used to watermark the transmitted signal.

C. The Passive Receivers

Pseudonymetry imposes an additional role on the passive receivers, to demodulate the received pseudonym from any received interference signal, and to write it to the database in Section III-D. Changes in the envelope of the incoming interference signal will be used by the passive receiver to demodulate the pseudonym. In general, the pseudonym demodulator could take different forms, depending on the pseudonym modulation method. Once an interfering signal's pseudonym is correctly demodulated, the passive receiver sends it and the timestamp when it was recorded to the database.

[1]Here we use "p-symbol" to denote the pseudonym symbol and distinguish it from the data symbol.

For the PAM example system described above, the passive receiver can use energy detection for pseudonym demodulation. This is similar to energy detection in [22] but with the additional block of p-symbol decision. In the PAM example, since the data symbol has constant average energy, the energy of the received signal indicates the amplitude, and thus the symbols, of the pseudonym signal. By comparing the energy of the received signal over T_p periods, we can differentiate the different energy levels which represent each pseudonym symbol. In the PAM example, we study wireless transmissions with rare interference where, at a time, pseudonyms from only one transmitter are decoded at the passive receiver. The case for two or more simultaneous interference is an important future work.

D. The Database System

This is a small repository system for pseudonyms from offending transmitters. Whenever the passive receiver senses an interfering signal, it writes the detected pseudonym and the timestamp when it was recorded on to the database. To avoid a growing number of pseudonyms in the database, pseudonyms are deleted every T time units. This time unit is proportional to the average rate at which the wireless transmitters access the database. Since database size affects the system performance, an optimal empirical T value could be determined through repeated experiments.

E. Security and Privacy

One of the challenges in the Pseudonymetry system is to ensure the privacy of the operating transmitters and their ability to operate robustly in the presence of attackers.

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. Given the transmitter is also sending a data signal, it already gives some information away to eavesdroppers in the vicinity of itself. The random pseudonym is available across a larger area, but does not expose more information about who is transmitting.

When the pseudonym is transmitted, it is possible that an eavesdropper [23] detects the signal and demodulates the pseudonym. Detecting the watermarked signal and demodulating the pseudonym by itself does not pose a privacy issue a since the source transmitter is still unknown but it is possible that, in a man-in-the-middle attack [24], the eavesdropper could pass the pseudonym to an attack transmitter near the passive receiver which could re-transmit the pseudonym in order to force this pseudonym into the database and thus to block access for the wireless transmitter.

The man-in-the-middle attack for Pseudonymetry is similar to jamming in some ways. It would prevent use of the channel just like a jammer prevents use of a channel, both attacks force transmitters to switch bands. On the defensive side, both a jammer and a man-in-the-middle attacker are active devices and thus can be located using source localization algorithms. Future work could work to minimize the impact of this man-in-the-middle attack, perhaps by providing system operators quick methods to locate (and thus disable) the attack transmitter.

The database could also provide an additional attack vector. An attacker might attempt to access and either disable the database or try to insert bogus pseudonyms into it. The latter is similar in impact to the man-in-the-middle attack, but can be mitigated by allowing only the passive receiver to insert into the database. The former attack might take the form of a denial of service attack, for example; robustness methods like having redundant copies of the database may help minimize this risk.

IV. Analysis

We evaluate two aspects of the Psuedonymetry system:

1) The performance of a detector that demodulates the watermarked pseudonym at passive receivers at low SNR, as a function of the SNR and as a function of the number of pseudonym bits per transmitted packet.
2) The performance of the intended receiver, which demodulates the intended bits in the presence of the watermark signal.

A. Error Performance at Passive RX

At the passive receiver, when there is an interfering signal, the sampled received signal $r(t)$ is the sum of RFI signal $s_p(t)$ and the noise signal $w(t)$,

$$r(t) = s_p(t) + w(t), \tag{3}$$

where $s_p(t)$ is defined in (1).

For our PAM example system, we study the performance of an energy detector. This detector first correlates with the data symbol waveforms $\{\phi_{d,l}\}_l$ and then squares the output signal amplitudes, rather than using the complex-valued signal itself. The energy detector correlates the squared signal amplitude with the sampled p-symbol basis functions $\phi_{p,l}(n)$. After correlation and sampling at rate T_d, the output X_n is given by:

$$X_n = (1 + q(n)) \sum_{k=0}^{K-1} \sqrt{\mathcal{E}_b} a_{n,k} + W. \tag{4}$$

We assume for this analysis, that the $L = 1$ p-symbol waveform is an NRZ symbol, $\phi_{p,l}(n) = 1$ for the duration of the p-symbol period, and that $\alpha_l = \pm m$ is the amplitude of the pulse for p-symbol 0 or 1. As there are two possible symbols we use p-bit and p-symbol both to mean the pseudonym bit. We denote the energy in the p-bit as $Z = \sum_{n=0}^{N-1} X_n^2$, where $N = T_p/T_d$ is the number of data symbols per pseudonym symbol. We note that since W is zero mean Gaussian with variance σ^2, that the mean and variance of of $Y_n = X + n^2$ are, from the properties of the non-central Chi-squared distribution:

$$\begin{aligned} E[Y] &= \sigma^2(1+\lambda) \\ \text{Var}[Y] &= 2\sigma^4(1+2\lambda), \end{aligned} \tag{5}$$

where $\lambda = \frac{{\mu_n}^2}{\sigma^2}$ is the non-centrality parameter, μ_n^2 is given by $(1-m)^2\mathcal{E}_b$ if p-bit '0' was sent or $\mu_n^2 = (1+m)^2\mathcal{E}_b$ if p-symbol '1' was sent. From the central limit theorem, given that $N = T_p/T_d$ is large, the sum of the energy in each p-bit, Z, is approximately normal with:

$$\begin{aligned} E[Z] &= N\sigma^2(1+\lambda) \\ \text{Var}[Z] &= 2N\sigma^4(1+2\lambda). \end{aligned} \tag{6}$$

In short, the detection must make a decision about Z, a Gaussian measurement with mean and variance that are both different under H_0 and H_1. Under H_0, that p-bit '0' is sent, the mean and variance of the decision variable, Z, are:

$$\begin{aligned} \mu_{z0} &= N(\sigma^2 + (1-m)^2\mathcal{E}_b) \\ \sigma_{z0}^2 &= 2N\sigma^2(\sigma^2 + 2(1-m)^2\mathcal{E}_b) \end{aligned} \tag{7}$$

Similarly under H_1, that p-bit '1' is sent:

$$\begin{aligned} \mu_{z1} &= N(\sigma^2 + (1+m)^2\mathcal{E}_b) \\ \sigma_{z1}^2 &= 2N\sigma^2(\sigma^2 + 2(1+m)^2\mathcal{E}_b) \end{aligned} \tag{8}$$

The optimal Bayesian detector for the normally distributed decision variables, in the case of equally likely p-bits, has threshold γ given by the quadratic formula,

$$\gamma = \frac{b \pm \sqrt{b^2 - 4c}}{2}, \tag{9}$$

where

$$b = \frac{2(\sigma_{z0}^2\mu_{z1} - \sigma_{z1}^2\mu_{z0})}{\sigma_{z0}^2 - \sigma_{z1}^2}, \text{ and} \quad (10)$$

$$c = \frac{\sigma_{z0}^2\mu_{z1}^2 - \sigma_{z1}^2\mu_{z0}^2 - 2\sigma_{z0}^2\sigma_{z1}^2 \ln\frac{\sigma_{z1}}{\sigma_{z0}}}{\sigma_{z0}^2 - \sigma_{z1}^2}. \quad (11)$$

The quadratic formula indicates that there are two decision threshold values, but for all values of N, m and σ^2, c is negative and can be represented as $c = \frac{-\sigma^4 N^2 \beta}{4}$ where β is given by

$$\beta = 8\frac{\mathcal{E}_b}{N_0}\left(1 + m^2 + 2\frac{\mathcal{E}_b}{N_0}(1-m^2)^2\right) + \frac{2}{Nm}\frac{N_0}{\mathcal{E}_b}\left(1 + 8\frac{\mathcal{E}_b}{N_0}(1+m^2)\right)\ln\frac{\sigma_{z_1}}{\sigma_{z_0}} + \frac{32}{Nm}\frac{\mathcal{E}_b}{N_0}(1-m)(1+m)^3\ln\frac{\sigma_{z_1}}{\sigma_{z_0}} \quad (12)$$

For large N, β can be approximated by:

$$\beta = 8\frac{\mathcal{E}_b}{N_0}\left(1 + m^2 + 2\frac{\mathcal{E}_b}{N_0}(1-m^2)^2\right) \quad (13)$$

From (9) and (12), the first threshold can be seen to be purely negative, which since our Z is purely positive, is not a useful threshold. Hence, we take the positive threshold value

$$\gamma = \frac{N\sigma^2}{2}\left(1 + \sqrt{1+\beta}\right) \quad (14)$$

as the optimal threshold.

Using the positive threshold value, we can now evaluate the average probability of p-bit error at the passive RX. The probability of p-bit error given that bit '0' was transmitted, $P_{e|0}$, is the probability that z_0 is greater than γ; the probability of p-bit error given bit '0', $P_{e|0}$ is the probability that z_0 is less than γ. Using a standard normal complementary CDF function $Q(z)$, we can write the overall probability of error P_e as:

$$P_e = \frac{1}{2}\left(P_{e|1} + P_{e|0}\right), \text{ where} \quad (15)$$

$$P_{e|i} = Q\left(\sqrt{\frac{N\left[(1+\beta)^{1/2} - (1 + 4(1-(-1)^i m)^2\frac{\mathcal{E}_b}{N_0})\right]^2}{8(1 + 4(1-(-1)^i m)^2\frac{\mathcal{E}_b}{N_0})}}\right),$$

for $i \in \{0, 1\}$. Figure (4) shows the P_e for different modulation indexes m. As can be seen, p-bit detection is possible even at very low $\frac{\mathcal{E}_b}{N_0}$. For example, for 20% modulation, the average p-bit error at -10 dB is less than 10^{-7}.

Probability of p-bit error vs. p-bits per packet: Next, we analyze the effect of increasing the number of p-bits that are sent over a single packet. Figure 5 shows the results for a packet length of 12,000 d-bits. While it is intuitive that the P_e increases we fit more p-bits into one packet, the results indicate that multiple bits could be sent per packet if m is 20% or higher.

B. Error Performance at Intended RX

Given that our watermark signal is given in (1), we evaluate here the degradation to the probability of d-bit error due to the watermark. For our binary PAM watermarking example system, when a data signal is amplitude modulated with modulation index m, the waveform for the watermarked signal, s_p(t) is:

$$s_p(t) = \begin{cases}(1-m)s(t), & \text{for p-bit '0'}\\ (1+m)s(t), & \text{for p-bit '1'},\end{cases} \quad (16)$$

where $s(t)$ is the waveform for the modulated data signal.

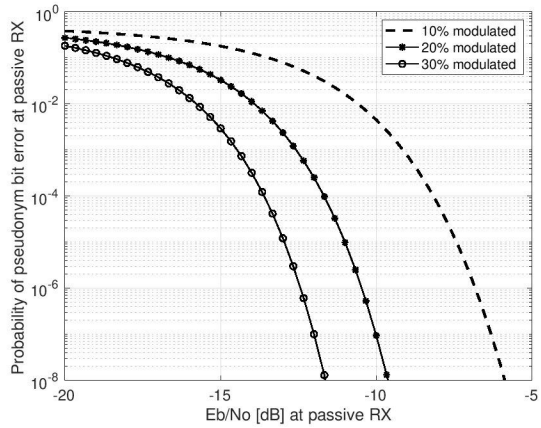

Fig. 4: Probability of p-bit error, P_e, vs. m and the $\frac{\mathcal{E}_b}{N_0}$ of the data bits, for N = 12,000 d-bits per p-bit.

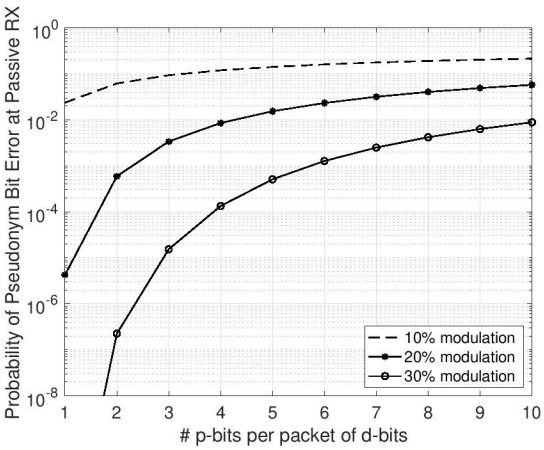

Fig. 5: Probability of p-bit error vs. number of p-bits per packet, for an $\frac{\mathcal{E}_b}{N_0} = 10$ dB.

We consider here of the case when the data is modulated via BPSK, as an example. For equally likely data bits, one can see that the watermark increases or decreases the $\frac{\mathcal{E}_b}{N_0}$ by a factor of $1-m$ or $1+m$, respectively. Thus the average probability of d-bit error is

$$P_{ave} = \frac{1}{2}\left\{Q(\sqrt{2(1-m)^2\frac{\mathcal{E}_b}{N_0}}) + Q(\sqrt{2(1+m)^2\frac{\mathcal{E}_b}{N_0}})\right\}. \quad (17)$$

Figure 6 shows the probability of d-bit error at the intended receiver for m = 0.1, 0.2, and 0.3. The larger the modulation index, the higher the probability of d-bit error. When compared to the normal BPSK signal, the watermarking on the host signal increased the probability of d-bit error but within about 1-3 dB. For example at 10^{-4} d-bit probability of error, the degradation is 0.67 dB, 1.67 dB and 2.67 dB for m = 0.1, 0.2, and 0.3 modulation indexes respectively. This is a measurable but small impact on the intended wireless system, and may be a small cost to be able to co-exist on the passive receiver's band.

Data bit decision as a function of the $\mathcal{E}_b/N_0$ at the passive RX: The probability of d-bit error at low SNR is shown in Figure 7. Intuitively, at very low SNR the d-bit error for normal BPSK signal becomes very high. For example, for a 20% modulated watermarked BPSK signal, d-bit error is more than 0.3 at $\mathcal{E}_b/N_0$ = -10 dB while the corresponding p-bit error is less than 10^{-7}. Thus, although

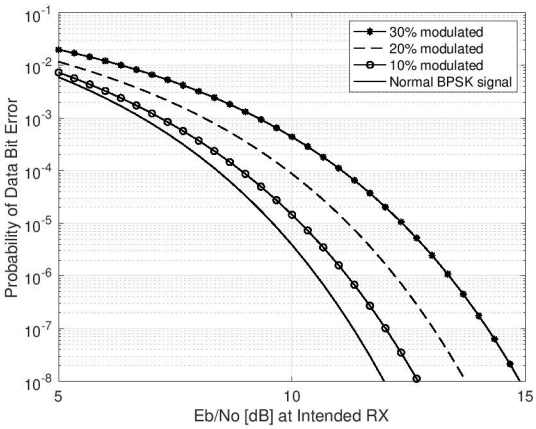

Fig. 6: Probability of d-bit error vs. $\frac{\mathcal{E}_b}{N_0}$ for 3 values of m, vs. BPSK.

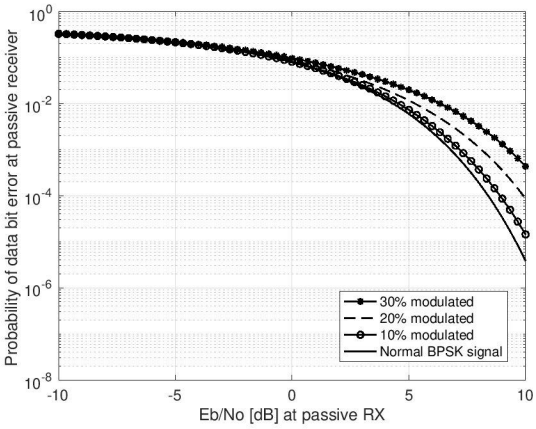

Fig. 7: Probability of d-bit error vs. $\frac{\mathcal{E}_b}{N_0}$ at the passive RX.

the passive receiver can demodulate the pseudonym bits, it cannot possibly demodulate the data bits at low $\frac{\mathcal{E}_b}{N_0}$ values like -10 dB.

V. Conclusion

In this paper, we propose Psuedonymetry, a system that could enable the coexistence of passive receivers and active wireless transmitters in the same spectrum. Psuedonymetry uses RF signal watermarking and a database feedback loop to stop an interfering device from transmitting whenever its signals cause measurable interference to a passive receiver. Future work must probe further into the design and practical experimentation of Pseudonymetry. We hope to study the number of p-bits (and thus how many packets must be received) needed for the system to reliably and rapidly turn off only the intended transmitter. We studied a low-rate amplitude modulation watermarking scheme to convey pseudonyms from the active wireless transmitter to the passive receiver. Through analysis, we demonstrate that reception of a pseudonym is possible even at low $\frac{\mathcal{E}_b}{N_0}$ values at which the data symbols cannot be demodulated. We also show that watermarking causes error performance degradation of about 1-3 dB at the intended data receivers, depending on the watermark modulation index. We hope the capabilities explored in this paper allow efficient and robust sharing between passive and active spectrum users.

References

[1] S. Bhattarai, Jung-Min, B. G. Park, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, 2016.

[2] M. Bentum, A. Boonstra, and W. Baan, "The coexistence of cognitive radio and radio astronomy," *16th Annual Symposium of the IEEE/CVT*, 2009.

[3] C. Wilson, "Propagation prediction in establishing a radio quiet zone for radioastronomy," *The 8th European Conference on Antennas and Propagation (EuCAP 2014)*, pp. 1209–1213, 2014.

[4] C. Wilson, K. Chow, L. Harvey-Smith, B. Indermuehle, M. Sokolowski, and R. Wayth, "The australian radio quiet zone – western australia: Objectives, implementation and early measurements," *2016 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pp. 922–923, 2016.

[5] J. M. Ford and K. D. Buch, "RFI mitigation techniques in radio astronomy," *IGARSS 2014*, pp. 231–234, 2014.

[6] C. Welch, "Florida man drove around as a cellphone-jamming vigilante for two years," *The Verge*. [Online]. Available: https://www.theverge.com/2014/5/1/5672762/man-faces-48000-fine-for-driving-with-cellphone-jammer

[7] J. Mitola, *Cognitive Radio*, 2000.

[8] E. S. Sousa and A. Ghasemi, "Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs," *IEEE Communications Magazine*, pp. 32–39, 2008.

[9] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part ii: Multiuser networks," *IEEE Transaction on Wireless Communications*, vol. 6, no. 6, pp. 2214–2222, 2007.

[10] Y. Liu, R. Yu, M. Pan, and Y. Zhang, "Adaptive channel access in spectrum database-driven cognitive radio networks," *IEEE ICC 2014 - Wireless Communications Symposium*, pp. 4933–4938, 2014.

[11] M. Kesteven, "Radio-frequency interference mitigation in radio astronomy," *The Radio Science Bulletin*, no. 322, pp. 9–18, 2007.

[12] T. Kidd. National radio quiet and dynamic zones. [Online]. Available: https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10299

[13] A. Leshem, A.-J. van der Veen, and E. Deprettere, "Detection and blanking of gsm interference in radio-astronomical observations," *1999 2nd IEEE Workshop on Signal Processing Advances in Wireless Communications (Cat. No.99EX304)*, pp. 374–377, 1999.

[14] M. E. Abdelgelil and H. Minn, "Non-linear interference cancellation for radio astronomy receivers with strong RFI," 2017, pp. 1–6.

[15] M. Abdelgelil and H. Minn, "Impact of nonlinear RFI and countermeasure for radio astronomy receivers," *IEEE Access*, vol. 6, pp. 11 424 – 11 438, 2018.

[16] C. Barnabaum and R. F. BradleyC, "A new approach to interference excision in radio astronomy: Real-time adaptive cancellation," *The American Astronomical Society*, pp. 2598–2614, 1998.

[17] N. N. Krishnan, R. Kumbhkar, N. B. Mandayam, I. Seskar, and S. Kompella†, "Coexistence of radar and communication systems in CBRS bands through downlink power control," *Milcom 2017 Track 5 - Selected Topics in Communications*, pp. 713–718, 2017.

[18] ITU-R, "Protection criteria used for radio astronomical measurements," *Recommendation RA.769-2*, Mar. 2003.

[19] G. Mayhew-Ridgers and P. V. Jaarsveld, "Reducing cellular interference in the karoo radio astronomy reserve," *2012 International Conference on Electromagnetics in Advanced Applications*, pp. 446–449, 2012.

[20] Y. R. Ramadan, Y. Dai, H. Minn, and F. S. Rodrigues, "Spectrum sharing between wifi and radio astronomy," *2016 Radio Frequency Interference (RFI)*, pp. 90–95, 2016.

[21] Y. R. Ramadan, H. Minn, and Y. Dai, "A new paradigm for spectrum sharing between cellular wireless communications and radio astronomy systems," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 110–128, 2017.

[22] W. Jun, H. Jiwei, W. Yunan, and X. Yiqiang, "A design of robust energy detector for cognitive radios," *IC-NIDC2014*, pp. 143–148, 2014.

[23] A. S. Abrar, N. Patwari, and S. K. Kasera, "Quantifying interference-assisted signal strength surveillance of sound vibrations," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2018–2030, 2021.

[24] S. Wetzel and U. Meyer, "A man-in-the-middle attack on UMTS," *WiSe '04: 3rd ACM workshop on Wireless security*, pp. 90–97, 2004.