Watermarking of OFDM for Pseudonymetry: Analysis and Experimental Results

Meles G. Weldegebriel*, Jie Wang*, Greg Hellbourg†, Ning Zhang‡ and Neal Patwari*‡
*Electrical & Systems Engineering; ‡ Computer Science & Engineering
Washington University in St. Louis; Email: {g.weldegebriel, jie.w, zhang.ning, n.patwari}@wustl.edu
† Cahill Center for Astronomy and Astrophysics
California Institute of Technology; Email: ghellbourg@astro.caltech.edu

2024 IEEE International Conference on Communications Workshops (ICC Workshops) | 979-8-3503-0405-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCWORKSHOPS59551.2024.10615923

***Abstract*—This paper presents new results for *pseudonymetry*, a closed-loop feedback mechanism in which active transmissions are watermarked with a pseudonym that, if it interferes with a protected passive radio receiver, can be demodulated and used to force the transmitter off of the band. This paper addresses amplitude-based watermarking of orthogonal frequency division multiplexing (OFDM) packets. We quantify the ability of a passive receiver to decode the watermark at very low signal-to-noise ratio (SNR) and the impact on the intended communication link. We demonstrate, using a testbed of software-defined radios, that the experimental implementation of pseudonymetry matches the theoretical analysis very closely. Our results quantify a fundamental trade-off in the design of pseudonymetry for OFDM and provide a practical pseudonym receiver design.**

***Index Terms*—Spectrum Sharing, RF Interference, Watermarking, Passive and Active Users**

I. Introduction

The radio spectrum is a finite and fundamental resource utilized for wireless communications, radio navigation, radio astronomy, and Earth sensing services [1]. Sharing spectrum between uses is a critical part of meeting growing demand in all of these uses. However, the *worst case* of radio frequency interference (RFI) has dominated spectrum policy debates. Policy sometimes requires overly conservative propagation models for sharing [2] that do reliably protect primary users, but precludes reuse in large areas in which secondary users would be very unlikely to interfere [3], [4]. For example, the FCC allocation of the 6-7 GHz band for indoor Wi-Fi 7 was fought by incumbent microwave tower operators who argued against the sharing mechanism because, despite the propagation model, there may be *some* interference, and "it will be impracticable, if not impossible, for the FCC to identify and remove specific devices causing interference" [5].

In spite of the large geographic radio quiet zones (RQZ) and regulatory interference protection rules, the current trend towards more intensive use of the radio frequency (RF) spectrum means that passive receivers such as radio telescopes increasingly suffer from interference from multiple sources [6]. Coexistence between passive and active radio services has taken these predominant approaches: 1) RFI detection and cancellation [7]. Even though various detection mechanisms have been studied, accurate cancellation remains an unsolved problem. 2) Use of interference thresholds and propagation models to define exclusion / radio quiet zones. Imperfect propagation modeling invariably means that either spectrum is underutilized or interference sometimes occurs. 3) Manual or "nascent technologies" [7] cooperation between passive and active users. For example, a CBRS system may operate within the NRQZ with official approval and manual configuration [8].

This paper extends work on *pseudonymetry* [9], an interference remediation cooperative protocol in which the passive receiver can identify the source of observed interference, and submit its pseudonym (its randomly chosen identifier) to a database, which ensures that the transmitter changes band. *Pseudonymetry* provides accountable coordination so that in the worst case, that an active user interferes with a passive user, the passive user can provide feedback to the active user to turn off or switch the band. However, watermarking imposes a key tradeoff, as studied in [10], [11]. The watermarking must be designed to be demodulated at very low SNR to allow the identification of interfering transmissions as soon as they reach the signal detection levels of sensitive passive receivers, which was presented in [9] for narrowband transmitters. As most commercial wireless systems use multi-carrier modulation, it is critical to evaluate the watermarking of OFDM signals, both the demodulation of the watermark, and its impact on OFDM data demodulation.

We extend [9] in this paper with three contributions, all publicly available [12]. First, we develop **new analysis** for the performance of an amplitude-based watermark on OFDM signals. Second, we present a **robust receiver implementation** for watermark demodulation at low SNR. Finally, we **experimentally deploy** our system on POWDER [13] and show that the experimental results match that of our analysis.

The rest of the paper is organized as follows. Section II describes the system model. In Section III, we present theoretical analysis. Experimental results and discussions are given in Section IV, before concluding in Section V.

This material is based upon work supported by the U.S. National Science Foundation under Grants CNS-1827940 and CNS-2229427.

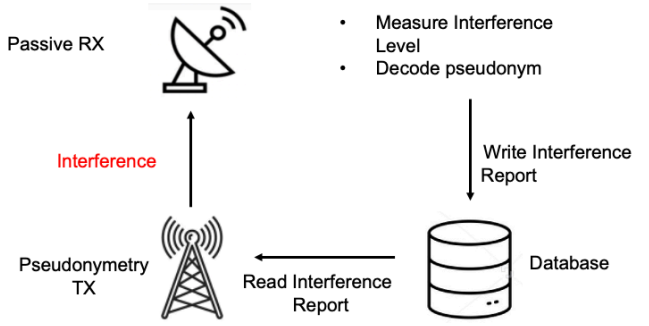

Fig. 1. Pseudonymetry architecture with cooperation between the pseudonymetry transmitter and the passive receiver through a database.

II. System Model

The operation of pseudonymetry is shown in Fig. 1, as introduced in [9]. We refer to passive receivers such as radio telescopes as the *primary users* of the band. Pseudonymetry transmitters are the *secondary users* who use OFDM modulation for data communication. The database is a repository system for storing interference reports, each consisting of the decoded pseudonym and its timestamp, sent from the passive receiver as discussed in [9]. Each pseudonymetry transmitter must watermark its transmitted signal with a low-rate *pseudonym* that it randomly generates and stores. The watermark must be able to be decoded by the passive receiver even when its received power is below the threshold for demodulation of the OFDM packet. When there is interference, the passive receiver uploads an interference report to the database. Pseudonymetry transmitters must check the database periodically and move off the particular channel if interference is reported matching their pseudonym(s) used while on that channel. In short, a pseudonymetry transmitter may transmit in the shared channel only if the database indicates that its use does not interfere with the primary user of the band.

A. Pseudonym Generation and Watermarking of OFDM

In this paper, we analyze a special case of the watermarking scheme, the pulse amplitude modulation (PAM) watermarking scheme in [9]. The watermarked transmit signal, $s_p(t)$, is given by:

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

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, generally written as:

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

where l is the pseudonym symbol (p-symbol) number[1], α_l is the amplitude of the lth p-symbol and $\{\phi_{p,l}(t)\}_l$ is an orthonormal basis for p-symbol modulation. The choices of the magnitude of $q(t)$ is a tradeoff between watermark detection at the passive receiver and impact of watermarking on the data signal demodulation at the intended receivers. Higher amplitude modulation on the data signal improves watermark detection but degrades data demodulations.

According to the chosen pseudonym bits, the amplitude of each data packet is sequentially amplified or attenuated according to the *modulation index*. This change in the signal amplitude at the pseudonymetry transmitter results in slow, patterned changes in the received power. The role of the passive receiver is to detect these changes and make pseudonym bit decisions by comparing a short-term average received power to a threshold.

Although an optimal threshold can be derived (as we do in Section III), it is based on parameters unknown to the receiver. Instead, in this paper, we simplify the receiver design by requiring the pseudonym to contain an equal number of zeros and ones. In this case, the average power of the received signal, across the pseudonym bits, is used as the threshold. We show this threshold approximates the optimal threshold.

This requirement limits the number of possible pseudonyms that can be randomly selected for transmission. We show that it can be compensated by marginally increasing the length of pseudonyms. If the pseudonym is K bits, with our requirement, we have $\binom{K}{K/2}$ pseudonyms to choose from instead of the 2^K possible pseudonyms without the assumption. Stirling's approximation for factorials implies a pseudonym bit efficiency of:

$$\eta = \frac{\binom{K}{K/2}}{2^K} \approx \sqrt{\frac{2}{\pi K}}. \quad (3)$$

Pseudonyms having equal number of zeros and ones need approximately $\frac{1}{2}\log_2\left(\frac{\pi}{2}K\right)$ more bits than without the assumption. For instance, when $K = 50$, our assumption requires about three extra bits.

B. Heuristic Approach to Threshold Estimation

In this paper, we use a heuristic approach to estimate a pseudonym receiver threshold. At the passive receiver, when there is an interfering signal from the pseudonymetry transmitter, the received sampled signal $r(n)$ is,

$$r(n) = s_p(n) + w(n), \quad (4)$$

where $s_p(n)$ is the RFI signal from a pseudonymetry transmitter, and $w(n)$ is centered and circular complex Gaussian noise. The average power over one p-symbol is,

$$Z = \frac{1}{N} \sum_{n=0}^{N-1} |r(n)|^2, \quad (5)$$

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

where N is the number of samples per pseudonym symbol. We compute Z in (5) for each of the K symbols in the pseudonym.

Next, we use the Z values in a robust estimator of the threshold. The threshold is sensitive to extreme values of Z (e.g., caused by other interfering signals, or temporal fading). To avoid sensitivity to extreme values, we disregard the smallest and largest 15% of the samples of Z, and set the threshold to the average of the remaining 70% of Z values. We show in Section IV that our heuristic approach is both simple and close to the (ideal) optimal threshold.

III. Performance Analysis

Here, we derive theoretical formulas for the probability of pseudonym bit error at the passive receiver, as well as for the probability of data bit error at the intended (secondary) OFDM receiver.

A. Pseudonym Detection at the Passive Receiver

When an OFDM signal waveform is amplitude modulated using the PAM example system described in [9], the watermarked OFDM signal is formulated as:

$$s_p(n) = \frac{1}{M}\sum_{k=0}^{M-1}[1+\alpha_l]X_k e^{j2\pi\frac{kn}{M}}, \tag{6}$$

where M is the number of subcarriers in the OFDM signal, and X_k is the complex symbol value on the kth subcarrier. For the binary PAM watermarking scheme, $l \in \{0,1\}$ and we use $\alpha_0 = -m$ for p-bit '0' and $\alpha_1 = +m$ for p-bit '1'. In our approach, we use $m \ll 1$ not to alter the data signal significantly.

From the pseudonym receiver's perspective, the values of X_k are random, selected from a finite constellation of possible symbol values. From the central limit theorem (CLT), when M is large, $s_p(n)$ appears to be a complex Gaussian random variable. Thus, $r(n)$ in (4), is also viewed as complex Gaussian.

We assume that $r(n)$ has independent and identically distributed real and imaginary components. Under these assumptions, the common variance for the real and imaginary components of $r(n)$ is:

$$\sigma_r^2 = \text{Var}\left[\text{Re}\{r(n)\}\right] = \frac{(1+\alpha_l)^2\mathcal{E}_s + N_0}{2}, \tag{7}$$

where $\mathcal{E}_s$ is symbol energy and N_0 is the noise power spectral density. Since the real and imaginary components of $r(n)$ are independent Gaussian random variables with zero mean, $|r(n)|^2$ is an exponential random variable with scale parameter $2\sigma_r^2$ [14]. Hence, from CLT for large N, the average power in each p-bit, Z given in (5), is approximately normal with mean $2\sigma_r^2$ and variance $4\sigma_r^4/N$.

Pseudonym Bit Decision: We derive the pseudonym bit detector as a Bayesian decision between H_0 or H_1, the hypotheses that pseudonym bit '0' or '1' is sent, respectively. From (7), the two hypotheses can be written as:

$$\begin{aligned} H_0 &: Z \sim \mathcal{N}\left\{(1-m)^2\mathcal{E}_s + N_0,\ \frac{((1-m)^2\mathcal{E}_s + N_0)^2}{N}\right\} \\ H_1 &: Z \sim \mathcal{N}\left\{(1+m)^2\mathcal{E}_s + N_0,\ \frac{((1+m)^2\mathcal{E}_s + N_0)^2}{N}\right\}. \end{aligned} \tag{8}$$

Assuming equally likely pseudonym bits, the Bayesian decision rule can be written as:

$$\frac{P[z|H_1]}{P[z|H_0]} \underset{H_0}{\overset{H_1}{\gtrless}} 1, \tag{9}$$

Equation (9) is quadratic in Z with two solutions,

$$\frac{N_0\lambda}{2\beta} \pm \sqrt{\left(\frac{N_0\lambda}{2\beta}\right)^2 + \frac{{N_0}^2\lambda^2}{2Nm\beta\frac{\mathcal{E}_s}{N_0}}\ln\frac{1+(1+m)^2\frac{\mathcal{E}_s}{N_0}}{1+(1-m)^2\frac{\mathcal{E}_s}{N_0}}}, \tag{10}$$

where we define λ and β as:

$$\begin{aligned} \lambda &= 1 + 2(1+m^2)\tfrac{\mathcal{E}_s}{N_0} + (1-m^2)^2\left(\tfrac{\mathcal{E}_s}{N_0}\right)^2 \\ \beta &= 1 + (1+m^2)\tfrac{\mathcal{E}_s}{N_0}, \end{aligned} \tag{11}$$

Since Z is a positive quantity, there is only one relevant detection threshold:

$$\gamma = \frac{N_0\lambda}{2\beta}\left[1 + \sqrt{1 + \frac{2\beta}{Nm\frac{\mathcal{E}_s}{N_0}}\ln\frac{1+(1+m)^2\frac{\mathcal{E}_s}{N_0}}{1+(1-m)^2\frac{\mathcal{E}_s}{N_0}}}\right], \tag{12}$$

For large N, the threshold is approximately,

$$\gamma \approx \frac{N_0\lambda}{\beta}. \tag{13}$$

The probability of pseudonym bit error given H_0 and H_1 is expressed as:

$$\begin{aligned} P_{e|0} &= P(Z > \gamma|H_0) \text{ and} \\ P_{e|1} &= P(Z < \gamma|H_1) \end{aligned} \tag{14}$$

Using a standard normal complementary CDF function $Q(z)$, the average probability of error P_e is:

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

$$P_{e|I} = Q\left\{(-1)^I\sqrt{N}\left(\frac{\lambda}{2\beta(1+(1-(-1)^I m)^2\frac{\mathcal{E}_b}{N_0})} - 1\right)\right\},$$

for $I \in \{0,1\}$. As can be seen from (15), the average probability of p-bit error is a function of the modulation index m, the number of data samples per pseudonym symbol N, and the energy per bit $\frac{\mathcal{E}_b}{N_0}$. It is interesting to note that keeping m and $\frac{\mathcal{E}_b}{N_0}$ constant, we can achieve lower probability of p-bit error by spreading the pseudonym symbols over higher number of data samples. However, increasing N results in lower pseudonym data rate and higher pseudonym decoding time at the passive receiver. In this paper, we assume one pseudonym symbol per one OFDM packet.

Analytical results for the probability of pseudonym bit error are shown in Fig. 2. The three lines in the plot indicate the

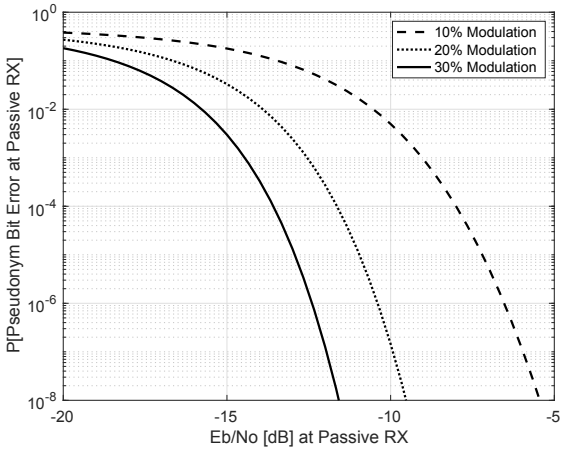

Fig. 2. Probability of p-bit error vs. m and the $\frac{\mathcal{E}_b}{N_0}$ of OFDM data bits. Plots are for $N = 6{,}000$ data samples per p-bit.

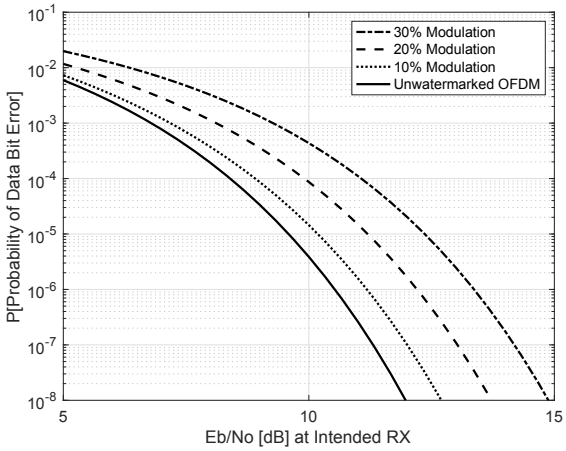

Fig. 3. Probability of d-bit error vs. $\frac{\mathcal{E}_b}{N_0}$ for 3 values of modulation indices. Plots are for $N = 6{,}000$ OFDM data samples per p-bit.

probability of p-bit error for $N = 6000$ and three modulation indices $m = 0.1$, 0.2, and 0.3 at different $\frac{\mathcal{E}_b}{N_0}$ values at the watermark detector. Clearly, p-bit detection is possible even at low $\frac{\mathcal{E}_b}{N_0}$.

B. Error Performance at the Intended Receivers

Here, we evaluate the performance degradation of OFDM data demodulation at the intended secondary receivers due to the watermark. For the PAM example system, the waveform for the watermarked signal, s_p(t) is given by:

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

where $s(t)$ is the unwatermarked OFDM signal. From (16), the watermark decreases and increases the $\frac{\mathcal{E}_b}{N_0}$ by a factor of $(1-m)^2$ and $(1+m)^2$ for p-bit '0' and '1', respectively. Thus, the average probability of data bit error at the intended receiver is:

$$P_{ave} \approx \frac{1}{2}\left[\mathrm{Q}\left(\sqrt{2(1-m)^2\frac{\mathcal{E}_b}{N_0}}\right) + \mathrm{Q}\left(\sqrt{2(1+m)^2\frac{\mathcal{E}_b}{N_0}}\right)\right]. \tag{17}$$

Fig. 3 depicts the probability of d-bit error at the intended receiver for $m = 0.1$, 0.2, and 0.3. As expected, the larger the modulation index, the higher the probability of d-bit error. When compared to the unwatermarked OFDM signal, watermarking increases the probability of d-bit error by about 1-3 dB depending on the modulation index. This is a measurable but small impact on the intended wireless system, and designers must evaluate if this is an acceptable cost to incur to be able to operate on the band that is primarily allocated to passive reception.

IV. Experiments

To demonstrate low power pseudonym detection and to validate the analysis of Section III, a set of experiments are conducted on the Platform for Open Wireless Data-driven Experimental Research (POWDER) [13], an openly-accessible wireless testbed. For this experiment, we use PhantomNet [15], part of the POWDER testbed. It has software defined radio (SDR) devices connected via cables to an RF attenuator matrix. As a result, we can fully control the interference power and signal power at the passive receiver.

The experimental setup is as follows: two Universal Software Radio Peripheral (USRP-B210) devices [16], are used as a pseudonymetry transmitter and passive receiver. The transmitter and receiver devices are connected to the RF attenuator matrix, creating a controlled experimental environment. We operate in the Citizens Broadband Radio Service (CBRS) band, which is within the range of operations of the B210. The transmitter sends 1 MHz bandwidth OFDM signals at 3.655 GHz with subcarrier spacing of 15 kHz. Transmit gain settings in the range 20 dB to 35 dB with 1 dB increase are used to watermarked OFDM packets. At the SDR transmitter device, we use a Python program to generate the complex-valued watermarked OFDM packet samples.

At the receiver, complex baseband samples are collected using an SDR device operating in receive-only mode. We use a sampling rate of 2 MHz and a constant receiver gain setting of 50 dB. Transmitter gains corresponding to each $\frac{\mathcal{E}_b}{N_0}$ at the receiver are determined empirically. At each transmitter gain, samples are collected and $\frac{\mathcal{E}_b}{N_0}$ is determined as [17],

$$\frac{S}{N} = \frac{\mathcal{E}_b}{N_0}\frac{f_b}{B}, \tag{18}$$

where B is the channel bandwidth, f_b is the channel data rate, and S and N are the observed signal and noise powers, respectively. We calculate the average noise power for each transmitter gain by stopping the transmission, gathering IQ samples at the receiver, and calculating the average power. When the transmitter is turned on, the signal power is calculated as the average received power minus average noise power.

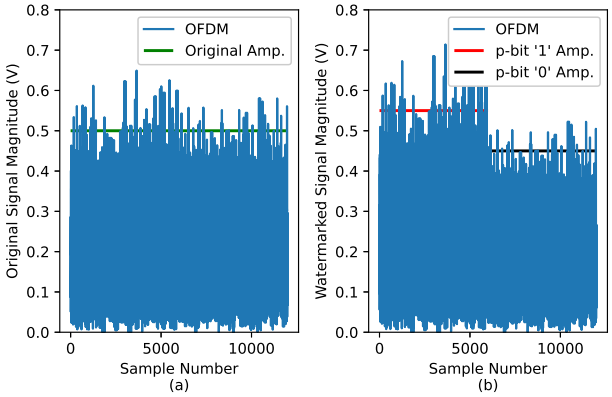

Fig. 4. Amplitudes of the OFDM signal before and after watermarking. (a) The 12000 OFDM samples' original amplitudes; (b) the new amplitudes of the OFDM signals after watermarking.

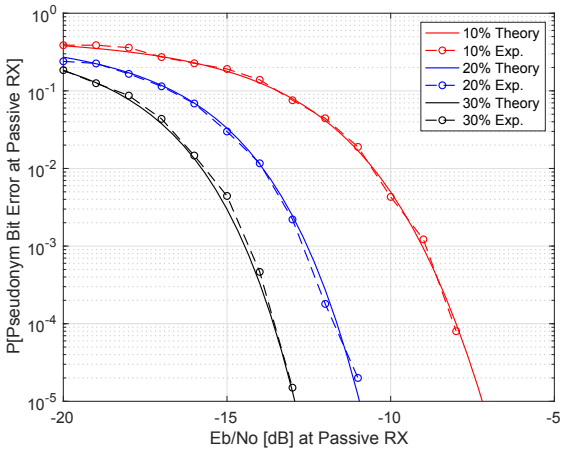

Fig. 5. Probability of p-bit error vs. $\frac{\mathcal{E}_b}{N_0}$ at the passive RX. Theory vs. Experimental results for three values of m.

The spectral efficiency, $\frac{f_b}{B}$, of our PAM example system is 2. For each $\frac{\mathcal{E}_b}{N_0}$ value calculated at the receiver, the procedure is repeated.

A. Pseudonym Transmission

In pseudonymetry, each pseudonym bit is transmitted as a watermark spread over N OFDM samples. We use a QPSK modulated OFDM signal as the host signal. Watermarked OFDM signals are generated in Python for three different modulation indices: m = 0.1, 0.2 and 0.3. Modulation indices show how much amplitude change we make to the host signal. When m = 0.1, for instance, if the first p-bit is '0', we transmit the first N samples at amplitudes 0.9 times the original host signal amplitudes, and when it is '1', we transmit the first N samples at amplitudes 1.1 times the original amplitudes. Depending on our pseudonym bit sequence, the resulting waveform is the original OFDM signal with slightly different amplitudes spanning windows of N samples.

The norm of the watermarked OFDM signals before and after watermarking is illustrated in Fig. 4. Plots are for m = 0.1 and $N = 6000$. The samples in the first window (0–6000) represent p-bit '1' and are transmitted at larger amplitudes than the initial amplitudes displayed in (a), as illustrated in (b). While the samples in the second window (6001–12000) represent p-bit '0' and are sent at lower amplitudes. The process is repeated for each pseudonym bit in the watermark.

B. Pseudonym Detection

Multiple IQ samples are collected using a dedicated receive-only device. Then, post-processing technique [12] is used to detect pseudonyms in these complex samples. The number of p-bits observed to calculate the probability of p-bit error is a function of the theoretical bit error rate and the confidence level [18]. At each $\frac{\mathcal{E}_b}{N_0}$, we use our theoretical p-bit error rate and a confidence level of 99% to determine the minimum number of p-bits needed to estimate the probability of p-bit error. However, for higher p-bit error rates at $\frac{\mathcal{E}_b}{N_0}$ in the range from -20 dB to -16 dB, we transmit higher number of p-bits than the empirical values stated in [18].

Here we compare our heuristic approach to the Expectation Maximization (EM) Algorithm [19] and the ideal threshold estimation.

Expectation Maximization Algorithm for Threshold Estimation: We use the EM algorithm to estimate the means and variances of the average powers, Z, for p-bit '0' and '1', as described in (8). We compute the average power for all p-bits, $\{Z\}$, and we use them as data points in a one-dimensional Gaussian mixture model with two components. Then, the Bayes' Law is used to calculate the threshold [20].

Ideal Threshold: Our heuristic threshold is contrasted with an ideal threshold. The procedure for determining the ideal threshold is as follows: at each $\frac{\mathcal{E}_b}{N_0}$, we compute the average p-bit power for each p-bit '0' and '1' observed at the receiver. Then using the transmitted p-bit sequence, we calculate the statistical mean and variance for the average p-bit power levels associated with p-bit '0' and '1'. Finally, using the Bayes's Law, we determine the ideal threshold. We call it ideal or ground truth because we use the knowledge of the transmitted p-bit sequences to calculate the ideal threshold. We use this ideal threshold for comparison purposes only.

C. Experimental Results and Discussion

Here we consider pseudonym detection performance at the passive receiver. Fig. 5 shows that the experimental probability of p-bit error agrees fairly well with the probability of error in the theoretical analysis. In these experimental results, we use heuristic approach to compute the threshold.

The ability to detect pseudonyms at extremely low SNR is a unique feature in pseudonymetry. Data bit demodulation is impractical when $\frac{\mathcal{E}_b}{N_0}$ is low, say 5 dB, but as seen in Fig. 5, pseudonym bit demodulation at $\frac{\mathcal{E}_b}{N_0} = -15$ dB is possible, primarily because of the design of the watermarking method.

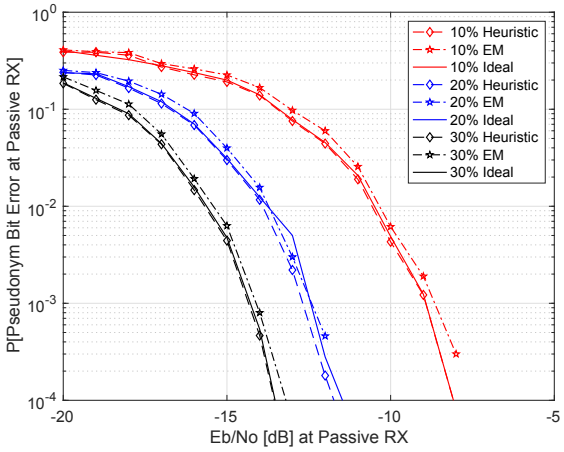

Fig. 6. Probability of p-bit error vs. $\frac{\mathcal{E}_b}{N_0}$ for the heuristic, EM and ideal threshold estimation techniques.

We calculate the probability of p-bit error at each $\frac{\mathcal{E}_b}{N_0}$ using the ideal threshold and thresholds obtained using heuristic and EM techniques. Fig. 6 shows the probability of p-bit error for the three thresholds for pseudonym length of $K = 64$. Clearly, the heuristic approach has the best error performance. This is because our heuristic approach disregards extreme values when estimating the threshold.

V. Conclusion

Pseudonymetry is a cooperative spectrum sharing protocol for the coexistence of passive receivers and active wireless transmitters. Pseudonymetry uses RF signal watermarking and a database feedback loop to stop an offending transmission whenever measurable interference is detected at the passive receiver. In this paper, we study watermarking of OFDM signals in the secondary signals. We analyze an amplitude modulation based watermarking scheme to embed low-rate pseudonym bits on top of the secondary OFDM signal. Through mathematical analysis and experiment, we show that watermark detection is possible at low $\frac{\mathcal{E}_b}{N_0}$ values, e.g., -10 dB with a modulation index, m = 0.1. This enables identification of the active transmitter at the $\frac{\mathcal{E}_b}{N_0}$ at which the OFDM data samples themselves cannot be demodulated. We show that, depending on the modulation index, watermarking causes $1-3$ dB performance degradation on OFDM data demodulation. We provide a practical pseudonym receiver implementation, which we implement in an SDR experiment, and show that its performance is nearly identical to the optimal receiver and very close to our analytical performance formulation.

In short, this paper advances our capability to implement and design pseudonymetry for OFDM signals. Future work will study the design and implementation of further aspects of the pseudonymetry system, including: cost implications at primary and secondary users, database and latency, integration into other sharing architectures like CBRS or automated frequency coordination (AFC), and security and privacy implications. Our goal is to provide a pseudonymetry system integration into an emerging wireless communication protocol.

References

[1] M. Zheleva, C. R. Anderson, M. Aksoy, J. T. Johnson, H. Affinnih, and C. G. DePree, "Radio dynamic zones: Motivations, challenges, and opportunities to catalyze spectrum coexistence," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 156–162, 2023.

[2] K. J. Martin, "In the matter of unlicensed operation in the TV broadcast bands, additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band. Second memorandum opinion and order," November 2008, US FCC ET Docket No. 04-186, ET Docket No. 02-380.

[3] M. J. Marcus, "Cognitive radio under conservative regulatory environments: Lessons learned and near term options," in *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN)*, April 2010, pp. 1–5.

[4] A. Clegg, "Spectrum data," in *WSRD Workshop: Making Data Available for National Spectrum Management*, Boulder, Colorado, May 2023, (Panel presentation in Session 3: Spectrum Data Collection). [Online]. Available: https://www.nist.gov/news-events/events/2023/05/wsrd-workshop-making-data-available-national-spectrum-management

[5] J. Marsh, "AT&T statement on FCC order to allow unlicensed devices in 6 GHz band," April 2020, press release, AT&T Executive Vice President of Regulatory & State External Affairs. [Online]. Available: https://www.attconnects.com/att-statement-on-fcc-order-to-allow-unlicensed-devices-in-6-ghz-band/

[6] J. Lowenthal, C. Walker, and P. Benvenuti, *Dark and Quiet Skies II Working Group Reports*. Astronomy: Faculty Publications, Smith College, Northampton, MA, 2022.

[7] National Research Council, *Spectrum Management for Science in the 21st Century*. National Academies Press, 2010.

[8] G. Cloud, "Citizens broadband radio service device overview," 2024, accessed 29 Mar. 2024. [Online]. Available: https://cloud.google.com/spectrum-access-system/docs/cbsd/overview

[9] M. G. Weldegebriel, J. Wang, N. Zhang, and N. Patwari, "Pseudonymetry: Precise, private closed loop control for spectrum reuse with passive receivers," in *2022 IEEE International Conference on RFID (RFID)*, 2022, pp. 91–96.

[10] Y. Zhang, Y. Chen, W. Yang, Y. Cai, G. Hu, and X. Qiao, "Secure transmission method of spectrum watermark for fine-grained spectrum management," *IEEE Access*, vol. 8, pp. 52 221–52 231, 2020.

[11] M. Gautier and D. Noguet, "Signal detection using watermark insertion," in *2013 IEEE 77th Vehicular Technology Conference*, pp. 1–5.

[12] M. Weldegebriel and N. Patwari, "Pseudonymetry receiver," 2024. [Online]. Available: https://github.com/Meles-Weldegebriel/Watermarking-of-OFDM-for-Pseudonymetry

[13] J. Breen, A. Buffmire, J. Duerig, K. Dutt, E. Eide, M. Hibler, D. Johnson, S. K. Kasera, E. Lewis, D. M. A. Orange, N. Patwari, D. Reading, R. Ricci, D. Schurig, L. B. Stoller, J. V. der Merwe, K. Webb, and G. Wong, "Powder: Platform for open wireless data-driven experimental research," in *in Proc. 14th Intl. Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH)*, Sep. 2020.

[14] A. Papoulis and S. Unnikrishna Pillai, *Probability, Random Variables and Stochastic Processes*. McGraw-Hill, 2002.

[15] PhantomNet. (February 2023) Phantomnet mobile testbed. [Online]. Available: https://phantomnet.org/

[16] (February 2023) Ettus Research USRP Products. [Online]. Available: https://www.ettus.com/all-products/ub210-kit/

[17] R. Wolff, "Noise; SNR and Eb/N0," Montana State University: Fall 2011 Lecture by Richard Wolff. [Online]. Available: https://www.montana.edu/aolson/ee447/EB\%20and\%20NO.pdf/

[18] D. Mitić, A. Lebl, and Z. Markov, "Calculating the required number of bits in the function of confidence level and error probability estimation," *Serbian Journal of Electrical Engineering*, vol. 9, pp. 361–375, 2012.

[19] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[20] A. Arnaout, B. Esmael, R. K. Fruhwirth, and G. Thonhauser, "Automatic threshold tracking of sensor data using expectation maximization algorithm," in *2011 11th International Conference on Hybrid Intelligent Systems (HIS)*, 2011, pp. 551–554.