Hiding Data in Plain Sight: Undetectable Wireless Communications Through Pseudo-Noise Asymmetric Shift Keying

Salvatore D'Oro*, Francesco Restuccia*, and Tommaso Melodia*
*Department of Electrical and Computer Engineering, Northeastern University, Boston, USA,
Email: {s.doro, f.restuccia, t.melodia}@northeastern.edu.

***Abstract*—Undetectable wireless transmissions are fundamental to avoid eavesdroppers or censorship by authoritarian governments. To address this issue, wireless steganography "hides" covert information inside primary information by slightly modifying the transmitted waveform such that primary information will still be decodable, while covert information will be seen as noise by agnostic receivers. Since the addition of covert information inevitably decreases the SNR of the primary transmission, a key challenge in wireless steganography is to mathematically analyze and optimize the impact of the covert channel on the primary channel as a function of different channel conditions. Another core issue is to make sure that the covert channel is almost undetectable by eavesdroppers. Existing approaches are protocol-specific and thus their performance cannot be assessed and optimized in general scenarios. To address this research gap, we notice that existing wireless technologies rely on phase-keying modulations (*e.g.*, BPSK, QPSK) that in most cases do not use the channel up to its Shannon capacity. Therefore, the residual capacity can be leveraged to implement a wireless system based on a pseudo-noise asymmetric shift keying (PN-ASK) modulation, where covert symbols are mapped by shifting the amplitude of primary symbols. This way, covert information will be undetectable, since a receiver expecting phase-modulated symbols will see their shift in amplitude as an effect of channel/path loss degradation. Through rigorous mathematical analysis, we first investigate the SER of PN-ASK as a function of the channel; then, we find the optimal PN-ASK parameters that optimize primary and covert throughput under different channel condition. We evaluate the throughput performance and undetectability of PN-ASK through extensive simulations and on an experimental testbed based on USRP N210 software-defined radios. Results indicate that PN-ASK improves the throughput by more than 8x with respect to prior art. Finally, we demonstrate through experiments that PN-ASK is able to transmit covert data on top of IEEE 802.11g frames, which are correctly decoded by an off-the-shelf laptop WiFi card without any hardware modifications.**

***Index Terms*—Steganography, Wireless Communications, Undetectability.**

I. Introduction

Establishing undetectable wireless communications is of paramount importance not only in military and tactical settings; but also when the freedom and security of individuals is undermined by censorship or malicious entities. Since radio waveforms are broadcast and cannot be hidden, a fundamental issue is *how to conceal a wireless transmission behind another.* To this end, *steganography* (from the Greek word $\sigma\tau\epsilon\gamma\alpha\nu\acute{o}\varsigma$, meaning "covered, concealed, or protected") allows to "hide" covert information behind intelligible (also called *primary*) data [1], such that the covert information is disguised as noise to receivers oblivious to the covert data exchange [2].

The application of steganographic techniques to wireless communications has received significant attention over the last years [3–10]. Among others, prior work creates covert channels by encoding information on top of the training sequences of WiFi [11], the cyclic prefix of WiFi OFDM symbols [4], errors introduced in the Bluetooth direct-sequence spread spectrum [9], and a "dirty" WiFi QPSK constellation [3]. However, existing approaches present a number of core limitations, which are discussed in details in Section II. Most importantly, since any steganographic technique will necessarily decrease the signal-to-noise ratio (SNR) of the primary channel, we need to thoroughly investigate and optimize through rigorous mathematical analysis the primary and covert symbol error rate (SER) as a function of the wireless channel. However, prior approaches are tied to specific wireless technologies (*i.e.*, WiFi and Bluetooth), thus their performance cannot be analyzed in general scenarios.

In this paper, we approach the problem in a different way by making the following core observation. Most of the modern wireless communication standards use phase-shifting modulations that do not fully utilize the wireless channel up to its Shannon capacity. For example, BPSK and QPSK utilize only a very limited portion of the I/Q constellation plane, since information is encoded only on top of the symbols' phase. Traditionally, this critical aspect has been leveraged to increase system throughput by encoding information also on the symbol amplitude, *e.g.*, as in asymmetric shift keying (ASK) [12]. Conversely, we leverage the additional channel capacity to implement a covert channel where information is encoded by changing the *amplitude* of the primary symbols while keeping their *phase* intact.

Fig. 1 shows an example of our pseudo-noise asymmetrical shift keying (PN-ASK). More in detail, PN-ASK maps each covert symbol to a radius length of an M-PSK constellation diagram. Thus, if we define n_c as the number of bits per covert symbol, it follows that $M_c = 2^{n_c}$ will be the number of possible covert symbols, *i.e.*, the number of radii that can be used to map a different covert symbol. Fig. 1.(b) and Fig. 1.(b)

This paper has been accepted for publication in IEEE INFOCOM 2019.

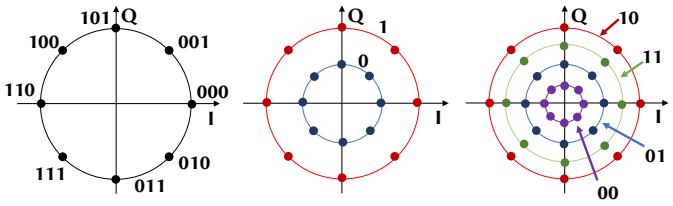

Fig. 1. (a) Constellation diagram for 8-PSK; Constellation diagram for PN-ASK on top of 8-PSK (b) with $M_c = 2$; (c) with $M_c = 4$.

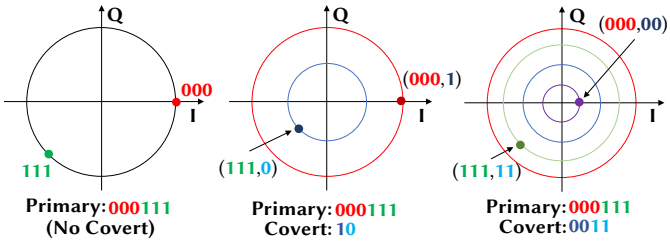

Fig. 2. (a) Transmitted symbols over a 8-PSK constellation; Transmitted symbols over PN-ASK when (b) $M_c = 2$; (c) $M_c = 4$.

show respectively the PN-ASK constellation for $M_c = 2$ and $M_c = 4$, as well as the related bit-to-symbol encoding. For example, the inner and outer radii in Fig. 1.(b) encode a covert "0" and "1" with a primary respectively, while the outer radius in Fig. 1.(c) encodes a covert "10".

To make an example, let us consider a primary bit sequence $B_P =$ "000111" to be transmitted over 8-PSK. If no covert communications are needed, the bit sequence would be transmitted by generating two different symbols as shown in Fig. 2.(a). Now, let us assume that the transmitter wants to use PN-ASK to embed covert data in the ongoing primary communication. Let us consider the case where $M_c = 2$, *i.e.*, one bit is transmitted through each covert channel utilization, and the covert bit sequence is $B_C =$ "10". Thus, the embedding of B_C in B_P would produce the two symbols in the center of Fig. 2. That is, the symbol $(000, 1)$ lies over the external radius of the constellation. Instead, the symbol $(111, 0)$ is transmitted by using the inner radius. When $M_c = 4$, the constellation shown in Fig. 1.(c) can be used. Thus, to embed the covert bit sequence $B_C = \{0, 0, 1, 1\}$ in B_P, the two symbols $(000, 00)$ and $(111, 11)$ shown in Fig. 2.(c) are generated and sent.

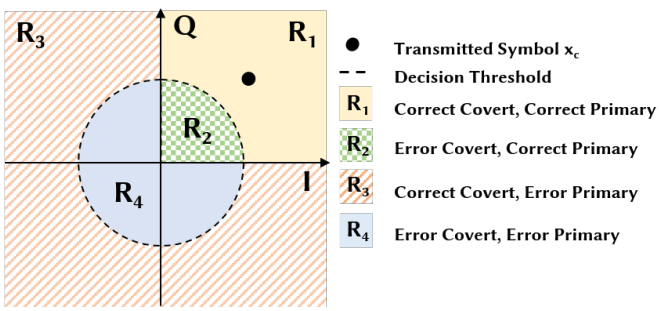

Fig. 3. Primary/Covert Demodulation Errors in PN-ASK.

We point out that the performance of PN-ASK cannot be analyzed by considering a simple ASK scheme [12]. This PN-ASK implements two different communication streams (i.e., primary and covert), thus the same channel may influence the covert and primary symbol error rate (SER) in very different ways. Indeed, Fig. 3 shows an example where we consider a symbol in the top-right quadrant being transmitted. The covert symbol is correctly demodulated when it is received inside R_1 (yellow shaded) or R_3 (orange shaded). However, while in R_1 both primary and covert demodulations are successful, in R_3 an error is generated in the primary channel. Instead, if the symbol is received in R_2 or R_4, an error is generated in the covert channel. However, when in R_2, the primary symbol is correctly demodulated. If the symbol is in R_4, both primary and covert symbol are not correctly demodulated.

In addition to proposing a covert wireless communication scheme using PN-ASK, we answer the following questions:

Q1: Since the introduction of a covert channel will necessarily increase the primary channel's SER, what is the set of PN-ASK parameters that will yield a desired minimum primary SER assuming a given channel distribution?

Q2: It is straightforward to notice that PN-ASK will generate a constellation pattern that slightly differs from the original primary constellation. Thus, can we assess the undetectability of the covert transmission as function of different PN-ASK parameters?

Q3: Can we demonstrate that a practical covert wireless communication system can use PN-ASK as modulation scheme? Moreover, is PN-ASK general enough to be applied to existing standard wireless technologies such as WiFi?

We address these questions by making the following core contributions:

- Through rigorous mathematical analysis, in Section IV we derive closed-form formulas to predict PN-ASK's SER on both primary and covert symbols as a function of AWGN noise (Section IV-A) and fading level (Section IV-B) experienced at the receiver, as well PN-ASK's energy per bit (Section IV-C) and maximum rate achievable (Section IV-D);
- We implement and evaluate the performance on PN-ASK through extensive simulations and on a testbed composed by two USRP N210 software-defined radios in two different scenarios, and compare PN-ASK's performance with prior work [3]. Simulation results confirm that (i) our analytical model is significantly accurate in predicting PN-ASK's performance (Section V-A); and (ii) PN-ASK can trade off performance for undetectability by changing its parameters (Section V-B). Experimental results indicate that *PN-ASK* achieves 8x throughput than prior work [3] (Section V-E);
- We demonstrate through experiments with an off-the-shelf WiFi card that PN-ASK-based transmissions can be created on top of standard-compliant IEEE 802.11 frames without modifying the receiver's WiFi card firmware/hardware (Section VI). We believe that this is a unique contribution of this paper that might open new directions in covert wireless communications.

II. Related Work

The application of steganography to design covert wireless communication systems has received some attention over the

last few years [13–17]. However, only few works have focused on the design of general-purpose, efficient and undetectable covert wireless communication systems.

Classen *et al.* analyze in [11] different covert channels over IEEE 802.11 networks, and show that it is feasible to transmit covert information on top of "redundant" information such as the short and long training sequences. Similarly, the authors of [4], [6] and [7] encode covert information by leveraging, respectively, the cyclic prefix of OFDM symbols, the OFDM frame padding mechanisms and the redundancy introduced by error correction coding. Direct sequence spread spectrum (DSSS) steganography over IEEE 802.15.4 communications has been investigated in [9], where covert information is effectively transmitted by intentionally generating errors in the DSSS sequence. On the other hand, the evaluation is only theoretical and no experiments on a practical testbed were conducted. Power allocation over a set of subcarriers is used in [10] to transmit covert data over AWGN channels. However, the authors conclude that such an approach achieves zero-rate transmission when a large number of subcarriers is considered.

The core limitation of the above-mentioned work is that it is tailored to specific protocols (*i.e.*, WiFi, Bluetooth), thus it is hardly generalizable and cannot be mathematically analyzed and optimized. In this paper, we follow a different approach and do *not* encode covert information on protocol-specific features. On the contrary, we leverage an approach only the *data subcarriers* involved in the primary data transmission, so as to (i) improve throughput (since more subcarriers are used), and (ii) to not disrupt critical information such as synchronization symbols and cyclic prefixes.

The closest work to ours is [3], where covert information is modulated onto WiFi QPSK primary symbol so that the symbols are seen as a "dirty" QPSK modulation at the receiver's side (see Fig. 12). However, some design choices in [3] make the proposed scheme less than fully general. First, the covert constellations will overlap in case of higher-order modulations (*e.g.*, 16-QPSK), which inevitably results in throughput loss in both primary and covert channels. Conversely, we encode covert information by *decreasing the amplitude* of a primary symbol, which does not cause overlap in higher-order modulations. Furthermore, the authors do not offer any mathematical analysis of the proposed scheme. Finally, we show through experiments in Section V-E that PN-ASK achieves 8x throughput of [3] under the same conditions.

To the best of our knowledge, ours is the first paper that proposes a covert wireless communication system that is (i) high-throughput and energy-efficient; (ii) extremely flexible (*i.e.*, to the level of subcarrier allocation); (iii) may be applied on top of wireless standards such as WiFi without any hardware modification.

III. Covert Communications Through PN-ASK

The core idea behind our pseudo-noise asymmetric shift keying (PN-ASK) modulation scheme is that in M-PSK systems, symbols are equally distributed over the unit circle and the information is encoded only in the phase rotation of each symbol, while the amplitude is always constant and, in general,

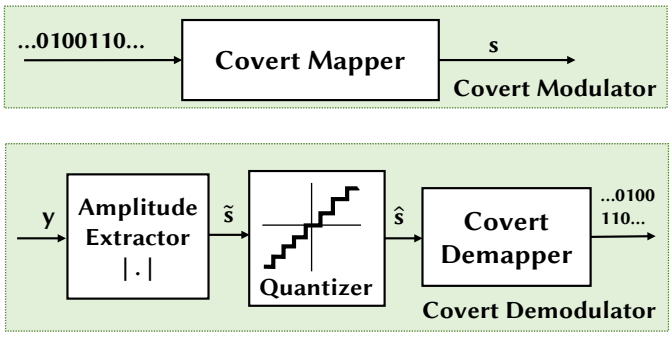

Fig. 4. Covert modulator and demodulator design.

unitary. Accordingly, any variation in the amplitude of M-PSK modulated symbols leaves the information encoded in each M-PSK symbol intact. The core idea of this paper is to leverage this peculiar feature of M-PSK modulated signals to establish a covert channel that encodes hidden data in the *variation of amplitude of the transmitted M-PSK symbols*, *i.e.,* the radius of the M-PSK constellation diagram.

Fig. 4 shows a modulator/demodulator design based on PN-ASK, which consists of a mapper that translates sequences of M_c consecutive bits to their corresponding covert symbol s. The mapping is performed with a *coding map*, where a bit combination is associated to one symbol. We define the covert coding map as follows. Let d be the *amplitude variation* imposed by the covert modulation. For a given index $i \in [1, M_c]$, and a value d, the corresponding i-th element $k(i)$ of the covert coding map can be defined as

$$k(i) = 1 - (i-1) \cdot d, \; 1 \leq i \leq M_c. \tag{1}$$

where the condition $d \leq 1/(M_c - 1)$ must always be satisfied to guarantee $k(i) \geq 0$.

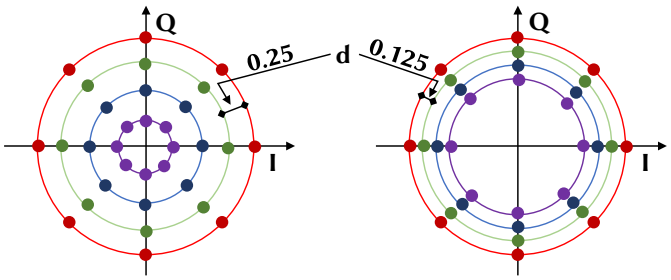

Fig. 5. Covert constellation diagram for 8-PSK with different values of d (Left: $d = 0.25$, Right: $d = 0.125$).

Fig. 5 depicts the impact of different values of d on the PN-ASK constellation diagram. From (1), the covert coding map $\mathcal{S}_c$ is defined as $\mathcal{S}_c = \{k(i)\}_{i=1}^{M_c}$. Note that when no covert information is transmitted, *i.e.*, $n_c = 0$, we have $M_c = 2^0 = 1$ and $\mathcal{S}_c = \{1\}$. Accordingly, in this case only primary data is transmitted and all transmissions are performed over the unitary circle.

At the demodulator side, the received baseband signal y is processed by an *amplitude extractor* block that computes $\tilde{s} = |y|$. Then, the obtained sample $\tilde{s}$ is dispatched to a *quantizer* having M_c levels. Each quantization level is used to

map samples to their nearest symbol in $\mathcal{S}_c$. This is achieved by defining $M_c - 1$ decision thresholds, which will generate M_c decision regions. Without loss of generality, we assume that all covert symbols in $\mathcal{S}_c$ are equally likely to be transmitted. In such case, it is easy to show that the optimal decision thresholds are

$$\tau(i) = \frac{k(i) + k(i+1)}{2} \tag{2}$$

where $k(i)$ is defined in (1). After quantization, the output $\hat{s}$ of estimated symbols is then converted to the corresponding bit sequence by using the same coding map $\mathcal{S}_c$ used at the transmitter's side.

A. Increasing PN-ASK's Undetectability

The main concern when implementing a covert wireless communication scheme is to ensure undetectability of covert information. Although a very generic, information-theoretical definition of steganographic undetectability has been proposed by Cachin in [18], the formal definition of what "undetectable" means in the context of steganographic wireless communications is still a (very challenging) open research problem, which we leave for future work.

Indeed, differently from traditional applications such as image steganography [19], *the wireless channel modifies significantly the information transmitted*, *which not only impacts the primary and covert information* (as analyzed in Section IV), *but also the undetectability of the scheme itself*. Furthermore, a receiver eavesdropping the channel for covert communication may (i) observe the transmission for an arbitrary amount of time; and (ii) use different measurements to determine whether covert information is being transmitted, which further complicates the analysis.

From a practical standpoint, we make the observation that a significantly noisy channel will make the steganographic transmission more undetectable (however, to the detriment of performance). Therefore, we can introduce artificial "noise" in the transmitted symbols, so as to further confuse an eavesdropper. An easy way to introduce noise is to transmit the i-th PN-ASK symbol not exactly at distance $k(i)$ but with a random displacement $D \in \mathbb{R}$ such that $k(i) + D \in (\max\{0, \tau(i)\}, \max\{\tau(i-1), 2k(i) - \tau(i)\})$ with $i = 1, \ldots, M_c$. We will show in Section V-B that this simple addition to PN-ASK increases the resilience to eavesdroppers.

IV. PN-ASK Symbol Error Rate Analysis

Let us define the number of coding symbols for the two channels as $M = 2^{n_P}$ and $M_c = 2^{n_c}$, respectively, where n_p and n_c are the number of bits per symbol in the covert and primary channels, respectively. We define the respective coding maps as $\mathcal{S}_p$ and $\mathcal{S}_c$.

A. Additive white Gaussian noise (AWGN) Channel

Let us now consider an AWGN channel. The received signal is thus $y = x_c + n = x \cdot s + n$, where $x \in \mathcal{S}_p$ is the primary transmitted signal, $s \in \mathcal{S}_c$ is the covert signal and n represents the AWGN introduced by the channel. We assume that n is modeled as a circular symmetric complex Gaussian random variable with variance σ_N^2, *i.e.*, $n \sim \mathcal{CN}(0, \sigma_n^2)$. Let us first consider the simple case of $n_c = 1$ and fixed distance d between symbols. From (1), it follows that the coding map is $\mathcal{S}_c = \{1, 1-d\}$, with decision threshold $\tau = \{(2-d)/2\}$. As explained earlier, the covert demodulator first computes $\tilde{s} = |y|$ upon reception of signal y. Then, $\tilde{s}$ is quantized to obtain the quantized symbol $\hat{s}$. An error is generated when the quantized symbol $\hat{s}$ is different from the transmitted symbol s, *i.e.*, the symbol error probability (SER) is:

$$P_c^{\text{AWGN}} = \sum_{s \in \mathcal{S}_c} \Pr\{\hat{s} \neq s | s \text{ sent}\} \Pr\{s \text{ sent}\} \tag{3}$$

Without loss of generality, we assume that $k = 1 - d$ and that all symbols are equally likely to occur. In other words, $\Pr\{s \text{ sent}\} = 1/M_c$ for all $s \in \mathcal{S}_c$, and (3) can be rewritten as

$$P_c^{\text{AWGN}} = \frac{1}{M_c} \left(\Pr\{\hat{s} \neq 1 | 1 \text{ sent}\} + \Pr\{\hat{s} \neq k | k \text{ sent}\} \right) \tag{4}$$

We now derive the two probabilities in (4). We note that a symbol error is generated when $\tilde{s} = |y|$ is not in the proper decision region. Thus,

$$\Pr\{\hat{s} \neq 1 | 1 \text{ sent}\} = \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \leq \tau^2 | 1 \text{ sent}\} \tag{5}$$

$$\Pr\{\hat{s} \neq k | k \text{ sent}\} = 1 - \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \leq \tau^2 | k \text{ sent}\} \tag{6}$$

The above equation is explained as follows. Under the AWGN assumption, when $s = 1$ the quantities $\Re\{y\}$ and $\Im\{y\}$ can be modeled as two independent normal random variables (r.v.) with distributions respectively equal to $\mathcal{N}(x_Q, \sigma_n^2)$ and $\mathcal{N}(x_I, \sigma_n^2)$, where x_Q and x_I represents the quadrature (Q) and in-phase (I) components. Thus, (5) can be rewritten as

$$\Pr\{\hat{s} \neq 1 | 1 \text{ sent}\} = \Pr\left\{ z_1 \leq \frac{\tau^2}{\sigma_N^2} \middle| 1 \text{ sent} \right\} \tag{7}$$

with $z_1 \sim \chi^2(2, x_Q^2/\sigma_N^2 + x_I^2/\sigma_N^2)$ being a non-central Chi-squared r.v. with 2 degrees of freedom and non-centrality parameter equal to $x_Q^2/\sigma_N^2 + x_I^2/\sigma_N^2$.

Recall that the noise spectral density of the channel can be obtained as $N_0 = 2\sigma_N^2$, and $x_Q^2 + x_I^2 = E_S$ holds for PSK signals, thus $z_1 \sim \chi^2(2, 2E_S/N_0)$.

Similarly, if $s = k$, the M-PSK signal is multiplied by $1 - d$ and $\Re\{y\} \sim \mathcal{N}(x_Q \cdot k, \sigma_n^2)$ and $\Im\{y\} \sim \mathcal{N}(x_I \cdot k, \sigma_n^2)$. Thus, (6) can be reformulated as

$$\Pr\{\hat{s} \neq k | k \text{ sent}\} = 1 - \Pr\left\{ z_k \leq \frac{\tau^2}{\sigma_N^2} \middle| k \text{ sent} \right\} \tag{9}$$

with $z_k \sim \chi^2(2, 2k^2 E_S/N_0)$. The Cumulative Distribution Function (CDF) of a non-central chi-squared r.v. z with k degrees of freedom and non-centrality parameter λ is $F_Z^{(k,\lambda)}(t) =$

$$P_c^{\text{AWGN}}\left(\frac{E_S}{N_0}\right) = \frac{1}{M_c}\Bigg\{1- Q_1\left(\sqrt{\frac{2E_S}{N_0}}, \sqrt{\frac{2\tau^2(1)}{N_0}}\right) + Q_1\left(\sqrt{\frac{2k^2(M_c)E_S}{N_0}}, \sqrt{\frac{2\tau^2(M_c-1)}{N_0}}\right) + \sum_{i=2}^{M_c-1}\left[1 - Q_1\left(\sqrt{\frac{2k^2(i)E_S}{N_0}}, \sqrt{\frac{2\tau^2(i)}{N_0}}\right) + Q_1\left(\sqrt{\frac{2k(i)^2E_S}{N_0}}, \sqrt{\frac{2\tau^2(i-1)}{N_0}}\right)\right]\Bigg\} \tag{8}$$

$1 - Q_{\frac{k}{2}}(\sqrt{\lambda}, \sqrt{(}t))$, where $Q_N(\alpha, \beta)$ is the generalized Marcum Q-function [20]. It follows that the SER in (3) can be defined as

$$P_c^{\text{AWGN}} = \frac{1}{M_c}\left(1-Q_1\left(\sqrt{\frac{2E_S}{N_0}}, \sqrt{\frac{2\tau^2}{N_0}}\right) + Q_1\left(\sqrt{\frac{2k^2E_S}{N_0}}, \sqrt{\frac{2\tau^2}{N_0}}\right)\right) \tag{10}$$

Now we derive the SER for the more general case where $n_c \geq 1$. From (1) and (2), in this case we have $\mathcal{S}_c = \{k(i)\}_{i=1}^{M_c}$ and $\tau(i) = {}^{[k(i)+k(i+1)]}/_2$. Thus,

$$P_c^{\text{AWGN}} = \frac{1}{M_c}\left[1 - Q_1\left(\sqrt{\frac{2E_S}{N_0}}, \sqrt{\frac{2\tau^2(1)}{N_0}}\right) + Q_1\left(\sqrt{\frac{2k^2(M_c)E_S}{N_0}}, \sqrt{\frac{2\tau^2(M_c-1)}{N_0}}\right)\right] + \frac{1}{M_c}\sum_{i=2}^{M_c-1}\Pr\{\hat{s} \neq k(i) | k(i) \text{ sent}\} \tag{11}$$

When $i \neq 1$ and $i \neq M_c$,

$$\begin{aligned}\Pr\{\hat{s} \neq k(i) | k(i) \text{ sent}\} &= \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \leq \tau^2(i) | k(i) \text{ sent}\} \\ &+ \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \geq \tau^2(i-1) | k(i) \text{ sent}\} \\ &= \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \leq \tau^2(i) | k(i) \text{ sent}\} \\ &+ 1 - \Pr\{\Re\{y\}^2 + \Im\{y\}^2 \leq \tau^2(i-1) | k(i) \text{ sent}\}\end{aligned} \tag{12}$$

Similarly to (7) and (9), (12) can be computed as

$$\Pr\{\hat{s} \neq k(i) | k(i) \text{ sent}\} = 1 - Q_1\left(\sqrt{\frac{2k^2(i)E_S}{N_0}}, \sqrt{\frac{2\tau^2(i)}{N_0}}\right) + Q_1\left(\sqrt{\frac{2k(i)^2E_S}{N_0}}, \sqrt{\frac{2\tau^2(i-1)}{N_0}}\right) \tag{13}$$

The primary SER can be computed as follows [20]:

$$P_p^{\text{AWGN}} = \frac{1}{M_c}\sum_{i=1}^{M_c} P_{\text{MPSK}}^{\text{AWGN}}\left(\frac{k^2(i) \cdot E_S}{N_0}\right) \tag{14}$$

where $P_{\text{MPSK}}^{\text{AWGN}}(\cdot)$ is the SER of a traditional M-PSK modulated signal under the AWGN regime.

B. Fading over AWGN Channel

Let us now extend the results derived in Section IV-A to the more general case where fading is considered. In the fading regime, the received signal can be expressed as $y = h \cdot x_c + n = h \cdot x \cdot s + n$, where h is a complex channel gain coefficient that models the fading introduced by channel distortions with probability density function (p.d.f.) $f_h(x)$, $x \in \mathcal{S}_p$, $s \in \mathcal{S}_c$ and $n \sim \mathcal{CN}(0, \sigma_n^2)$. Recall that the SNR per symbol in the fading regime is $\gamma_S^{(\text{FADING})} = |h|^2 E_S/N_0$ [20]. Thus, we have that the SER of both covert and primary channels under the fading regime can be computed as [20]

$$P^{\text{FADING}} = \int_0^{+\infty} P^{\text{AWGN}}\left(\frac{E_S}{N_0}z\right) f_{|h|^2}(z)dz \tag{15}$$

where and $f_{|h|^2}(\cdot)$ is the p.d.f. of the r.v. $|h|^2$ that represents the squared amplitude of the r.v. h and $P^{\text{AWGN}}(\cdot)$ is defined in (11) and (14) for covert and primary channels, respectively. Note that (15) is general and holds for any p.d.f. $f_{|h|^2}(\cdot)$. It is easy to extend (15) to include the additional random noise D as discussed in Section III-A.

C. Energy Per Symbol

The average energy per symbol under PN-ASK can be computed as

$$E_S^c = \sum_{s \in \mathcal{S}_c} \|x \cdot s\|^2 \cdot \Pr\{s \text{ sent}\} \tag{16}$$

Recall that all symbols on the primary channel lies on the unit circle of the constellation diagram, thus $\|x\|^2 = E_s$ for any $x \in \mathcal{S}_p$. Furthermore, since $\|s \cdot x\| = s\|x\|$ and all symbols in $\mathcal{S}_c$ are equiprobable, (16) can be rewritten as

$$E_S^c = \frac{1}{M_c}\sum_{i=1}^{M_c} k^2(i)\|x\|^2 = \frac{E_S}{M_c}\sum_{i=1}^{M_c} k^2(i) \tag{17}$$

Since $k(i) \leq 1$ for all $i = 1, 2, \ldots, M_c$, we have that $E_S^c \leq E_S$. That is, the covert modulation produces a reduction in the energy per symbol of the transmitted symbol. Furthermore, the energy per symbol decreases as the number n_c of covert bits transmitted over the steganographic channel increases.

On the one hand, this latter result shows that the superimposition of covert data reduces the energy consumption of the system. Furthermore, by increasing the amount of covert bits, the symbol rate increases as well. However, on the other hand, a reduction in the energy per symbol causes a reduction in the SNR of the received primary signal, which eventually results in the generation of errors, and thus a reduction in the achieved symbol rate on the primary channel.

D. PN-ASK Rate Optimization

From the previous discussions, it follows that PN-ASK can transmit up to $\log_2(M)+\log_2(M_c)$ bits per symbol. In the case of multiple carrier wireless communications, $N \cdot (\log_2(M) + \log_2(M_c))$ bits can be transmitted over the channel at each wireless transmission, where N is the number of subcarriers used in the system. Theoretically, the achievable bit rate of the proposed steganographic system is thus equal to

$$R = \frac{N}{T_s}\left[\log_2(M_c)(1-\mathrm{BER}_c) + \log_2(M)(1-\mathrm{BER}_p)\right], \tag{18}$$

where N is the number of subcarriers used for data transmission, T_s is the symbol period, and BER_c, BER_p represent the bit error rate (BER) of the covert and primary channels, respectively.

Both BER_c and BER_p can be derived by using the SER expressions we have derived in Section IV. Unfortunately, the relationship between BER and SER strongly depends on the actual bit coding used for data transmission. As an example, when Grey coding is used to map bit sequences to symbols, we have that $\mathrm{BER} \approx \mathrm{SER}/n$, where n is the number of bit per symbol. However this approximation is not tight for small values of the ratio E_s/N_0, which makes it hard to find closed form expressions for the BER of both primary and covert channels. For this reason, we will only focus on the SER of PN-ASK, while we will consider the computation of the BER as out of the scope of this paper.

The primary and covert symbol rates R_p and R_c (equations not shown here due to space constraints) not only depend on the ratio E_s/N_0, but also on the configuration of both primary and covert modulation schemes. Thus, to maximize the performance of the system, we define the following optimization problem.

$$\underset{M,M_c,d}{\text{maximize}}\ \beta \cdot R_p\left(\frac{E_S}{N_0}\right) + (1-\beta)\cdot R_c\left(\frac{E_S}{N_0}\right) \tag{19}$$

$$\text{subject to} \qquad d < \frac{1}{M_c - 1}. \tag{20}$$

where $\beta \in [0,1]$ trades off primary for covert symbol rates, and (20) ensures that all covert symbols in $\mathcal{S}_c$ are positive, *i.e.*, $k(i) > 0$ for all $i = 1, 2, \ldots, M_c$.

TABLE I
OPTIMUM PN-ASK SETTING

$\frac{E_s}{N_0}$	$\beta = 0.1$			$\beta = 0.5$			$\beta = 0.9$		
	M	M_c	d	M	M_c	d	M	M_c	d
0dB	4	4	0.2333	4	4	0.0333	4	4	0.0333
15dB	8	8	0.1286	8	8	0.1000	8	8	0.0143

Table I reports the solution of Problem 19 for different values of β and E_s/N_0. The obtained results clearly show that poor channel conditions require low values of M and M_c. Conversely, high values of E_S/N_0 produce higher SNR levels, which ultimately makes it possible to support higher-order modulations, i.e., higher values of M and M_c. Table I also shows that when we primarily focus on the maximization of the covert channel (*i.e.*, $\beta = 0.1$), the distance d increases. This confirms the theoretical analysis of Section IV. On the other hand, when higher values of β are considered, the distance d decreases to accommodate higher SNR values on the primary channel.

V. PN-ASK EVALUATION

In this section, we report the results obtained by our simulation study of PN-ASK over AWGN, Rayleigh, Rice, and log-normal channels [21], which is aimed at validating the mathematical model proposed in Section IV.

A. PN-ASK Model Validation and SER Performance

Fig. 6 compares the symbol error rate (SER) derived in (11) and (15) (shown as lines) with the SER obtained by simulation experiments (shown as point markers), as a function of the E_s/N_0 ratio. In our simulations, we fixed the energy per symbol to $E_s = 1$J and varied N_0. Results were averaged over $10,000$ independent runs.

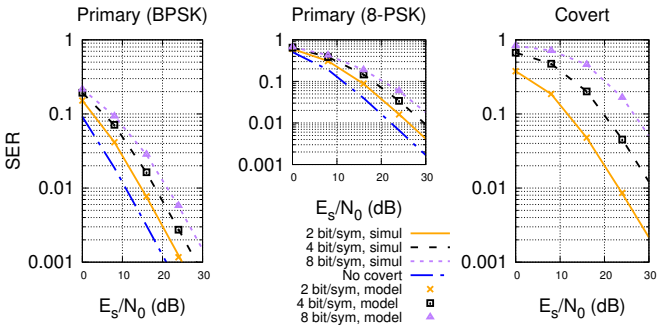

Fig. 6. SER as a function of E_s/N_0.

Fig. 6 shows that our mathematical formulation is accurate as lines and markers perfectly match. Furthermore, as already mentioned in Section IV, we conclude that the introduction of covert data reduces the SNR of the received signal on the primary channel, ultimately causing an increased SER on the primary channel. Also, the SER always increases as the number M_c of covert symbols increases. This is because the distance between each symbol in $\mathcal{S}_c$ decreases as M_s and the probability to incorrectly demodulate symbols increase.

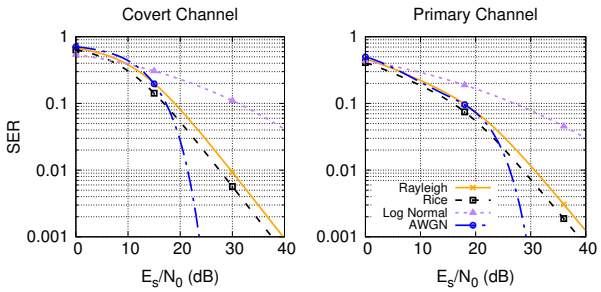

Fig. 7. Symbol Error Rate as a function of the E_s/N_0 ratio for different fading scenarios.

Fig. 7 evaluates PN-ASK under different fading distributions, where we consider respectively 2 and 4 bit/symbol for primary and covert transmissions. The results show that the SER always decreases when large values of the ratio E_s/N_0 are considered.

Furthermore, Fig. 7 shows that the best performance is achieved when no fading is considered and only AWGN noise affects ongoing communications. On the contrary, fading produces lower SNR values, which eventually results in high values of the SER.

B. PN-ASK Undetectability Analysis

A key advantage of PN-ASK is its capability to trade off covert throughput for additional undetectability. As explained in Section III, PN-ASK achieves this goal by reducing the distance d between the covert symbols, "camouflaging" the covert transmission as fading and noise.

To thoroughly evaluate this crucial aspect, the bottom side of Fig. 8 shows the related primary/covert symbol rate as function of E_s/N_0 and d. In these experiments, we considered a Rayleigh fading channel with $\sigma_h = 1$ and a symbol time of $T_s = 4\mu s$. The symbol rate is computed through our mathematical model by $1/T_s \cdot (1 - SER)$. For simplicity, we consider that 2 covert symbols are being sent (*i.e.*, $M_c = 2$), which implies that the optimal threshold is set to $1 - d/2$. To produce additional pseudo-noise, the transmitter introduces a displacements D whose absolute value is uniformly distributed in $(0, \min\{1-d, d/2\})$ as explained in Section III-A.

From Fig. 8, we notice that the primary symbol rate increases as d decreases. On the contrary, the covert symbol rate increases as higher values of d are considered. This results is reasonable as when d is large, *i.e.*, $d = 0.7$, symbols are closer to the origin and are more likely to change decision region in phase-keyed modulations, thus generating errors on the primary channel. On the other hand, as soon as the distance becomes smaller, *i.e.*, $d = 0.2$, symbols become closer with each other and the covert receiver can decode less covert symbols correctly, hence the decreased symbol rate on the covert channel.

The impact of the distance d on the undetectability of the PN-ASK scheme is shown in the top side of Fig. 8, where we show the pdf of the amplitude of the received (equalized) symbols, as well as their scatterplot, for different values of d (respectively 0.7, 0.4, and 0.2). *As we can see, as d decreases the PN-ASK symbols become less evident as they "camouflage" themselves more and more as a traditional 8-PSK transmission with additional fading.*

C. Experimental Evaluation

We evaluate the performance of PN-ASK on two practical testbeds deployed in an office setting (*i.e.*, in the presence of severe multipath and interference) and in an open hall space (*i.e.*, less multipath and interference but further distance between radios). We also experimentally compare the performance of PN-ASK with the state-of-the-art work on "dirty constellations" in [3], henceforth referred to as DTY-PSK. We also evaluate the undetectability of PN-ASK.

Fig. 9 shows our *Office* and *Hall* testbeds, which consist of two off-the-shelf USRP N210 [22] deployed at about 180cm and 50 m distance from each other, respectively. Both USRPs were equipped with (i) one CBX RF transceiver with frequency band from 1.2 GHz to 6 GHz and 40 MHz instantaneous bandwidth ; and (ii) two VERT2450 dual-band vertical antennas able to transmit in the ranges 2.4 to 2.48 GHz and 4.9 to 5.9 GHz.

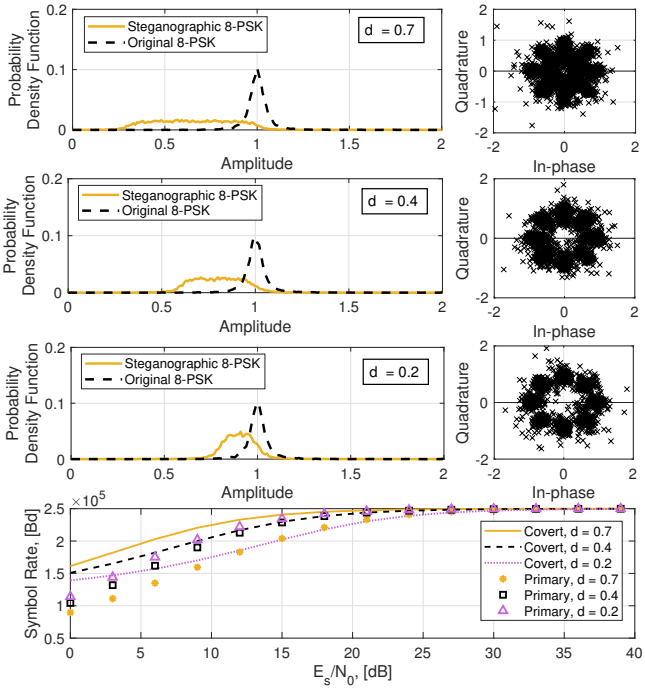

Fig. 8. Probability Density Function, Constellation Scatterplot, and Symbol Rate of PN-ASK with different values of d (0.7, 0.4, and 0.2).

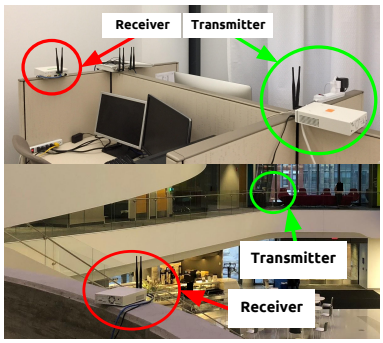

Fig. 9. *Office* and *Hall* Experimental Setups.

The *Office* setting was chosen since transmissions were affected by not only severe multipath caused by nearby walls and other obstacles, but also by interference caused by several nearby devices transmitting on the industrial, scientific and medical (ISM) band such as WiFi and Bluetooth. These aspects make this setup ideal to evaluate the performance of PN-ASK under challenging channel conditions. The *Hall* setting was chosen to evaluate the performance on a scenario with less interference but with radios communicating over a longer distance.

To experience different channel conditions, we varied the sampling rate of the USRP devices; also, to introduce interference from other ISM technologies, we fixed the center frequency to 2.432 GHz, corresponding to channel 5 of WiFi. Since WiFi channels are spaced 5 MHz apart with a bandwidth of approximately 22MHz [23], PN-ASK transmissions received interference from WiFi channels 3 to 6. Please also note that our current implementation does not support CSMA/CA and

acknowledgments, thus packet collisions are more likely to occur.

As far as the PHY layer is concerned, we implemented an OFDM system with the same parameters (*i.e.*, pilot carriers, symbols, FFT size, etc) used by WiFi. In particular, our OFDM subframes are long $N = 64$ symbols, of which $N_o = 48$ are data, $N_p = 4$ are pilots, and $N_g = 12$ are guard symbols; pilot symbols are (1, 1, 1, -1,) and are placed at subcarriers indexed at (-21, -7, +7, +21) [24]. If not otherwise specified, the experiments were performed with sampling rate of 0.5 MS/s. To guarantee reliability, we fixed the modulations used for the headers to BPSK in case of primary packets and PN-ASK with 1 bit/sample and $d = 0.5$ for covert packets – if not specified otherwise, this is also the modulation for the covert and primary payloads. In our experiments, covert and primary applications continuously stream UDP packets encapsulating bytes read from two different files of approximately 1 MB each. Payload size (included CRC) for both primary and covert PHY packets was fixed to 96 bytes (*i.e.*, two OFDM subframes).

D. Throughput Study

Fig. 10 depicts the throughput (expressed in bit/s) experienced by both primary and covert channels, as a function of the sampling rate (expressed in MS/s) for different modulation values, in both the *Office* and *Hall* scenarios. The results in Fig. 10 indicate that PN-ASK is able to encode covert information without compromising the primary communication channel. They also conclude that PN-ASK is able to achieve high-throughput covert communication, as it is able to deliver a throughput of about 1.5 Mbit/s on both primary and covert channels and both settings, despite (i) the adverse channel conditions; (ii) the lack of CSMA/CA mechanism; (iii) the loss in performance due to the usage of USRPs (*i.e.*, most of the DSP implemented in software rather than in hardware); and (iv) the distance between transmitter and receiver in the *Hall* setting.

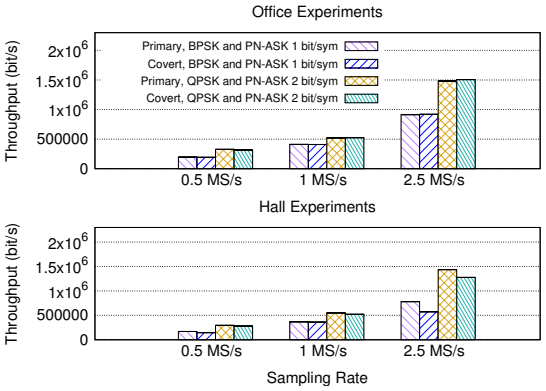

Fig. 10. PN-ASK, Throughput vs. Sampling Rate.

E. Comparison Study

Fig. 11 shows the experimental comparison between DTY-PSK and PN-ASK. In a nutshell, the rationale behind DTY-PSK is to encode covert symbols on top of four QPSK constellations, each having origin where traditional QPSK symbols are usually placed, so that the received constellation in interpreted as a "dirty" QPSK by the receiver. To place the covert symbols, we used the same parameters as in [3]. Fig. 11 indicates that PN-ASK exhibits a 6.28x and 8.37x throughput increase with respect to DTY-PSK in the *Office* and *Hall* setups, respectively. This is because (i) DTY-PSK symbols are placed very closely to each other (see Fig. 12); and (ii) they are affected by both amplitude *and* phase distortion, the DTY-PSK covert channel exhibits low throughput. Conversely, PN-ASK symbols are not affected by phase distortion but only by amplitude, which significantly increases throughput.

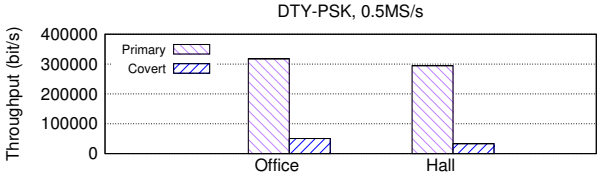

Fig. 11. DTY-PSK, Throughput vs. Scenario.

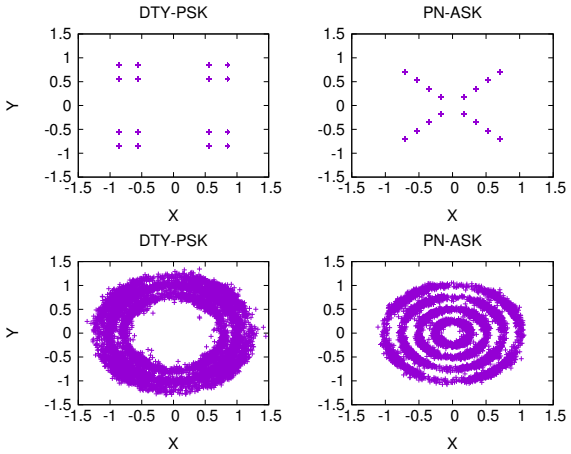

Fig. 12. Transmitted and Received Symbols, PN-ASK 2 bit/sym vs DTY-PSK, *Hall* setup, 0.5 MS/s.

VI. PN-ASK over WiFi

To demonstrate the applicability of PN-ASK to widely-used wireless technologies, we have implemented an additional version of *PN-ASK*, named *PN-ASK-WiFi*, that establishes PN-ASK-based covert communications on top of standard IEEE 802.11 frames. We have also shot a video demonstration (demo) of our system, which is available upon request and was not included here for the sake of anonymity. *PN-ASK-WiFi* was implemented by leveraging free-software PHY-layer Gnuradio libraries of IEEE 802.11 [25]. In our experiments, the standard receiver was a Dell XPS laptop running Ubuntu 17.10 and equipped with an off-the-shelf Intel Dual-Band Wireless-AC 7265NGW wireless card [26]. On the transmitter's side, we have implemented a primary application broadcasting a WiFi frame every 5 milliseconds for 5 minutes, with source and destination MAC addresses *23:23:23:23:23:23* and *42:42:42:42:42:42*. The frame's payload has been set to the string `This is a message on the primary channel!`, whereas MAC addresses are *25:25:25:25:25:25*

and *43:43:43:43:43:43*, respectively, with payload set to the string `This is a covert message!`.

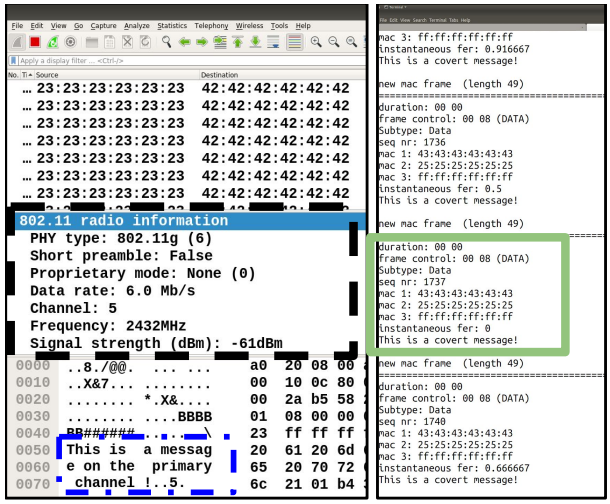

Fig. 13. (left) Wireshark screenshot on the WiFi-equipped laptop; (right) Decoded covert WiFi frames.

Our PN-ASK-WiFi system sends WiFi frames without the need to associate with an access point (AP). For this reason, we have used the `airmon-ng` and `iwconfig` tools to put the WiFi card in monitor mode and thus receive any IEEE 802.11 frame transmitted on a given channel. Similar to the previous experiments, WiFi frames are transmitted on channel 5 (2.432 GHz). However, to be WiFi-compatible, in these experiments the bandwidth has been set to 20 MHz. To visualize the WiFi frames received on channel 5 by the laptop, we have used the widely used `Wireshark` tool. Covert frames are instead received by an iMac desktop equipped with an USRP N210. The left side of Fig. 13 shows a screenshot of the Wireshark capture. As it can be observed, primary frames are received correctly by the laptop's WiFi card, whose hardware and software was not modified in any shape or form.

VII. Conclusions

This work has presented a novel pseudo-noise amplitude shift keying (PN-ASK) modulation scheme to implement covert wireless communication systems. First, we have provided a real-world OFDM-based implementation of PN-ASK, and mathematically analyzed the symbol error rate (SER) of PN-ASK. Then, we have evaluated PN-ASK on USRP N210 software radios, and shown that PN-ASK achieves a throughput of about $1.5\ \mathrm{Mbit/s}$ on both covert and primary data streams, on a channel only $2.5\ \mathrm{MHz}$ wide and in the presence of severe interference from nearby ISM band transmissions, and that PN-ASK increases the covert throughput by more than 8x with respect to the state of the art. Furthermore, results have shown that PN-ASK is almost undetectable. Finally, we have demonstrated that PN-ASK can be used to transmit covert data on top of standard IEEE 802.11 frames, which are correctly decoded by the WiFi card without any hardware modifications.

References

[1] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.

[2] D. Kahn, "The history of steganography," in *Proc. of Springer Intl. Workshop on Information Hiding*, 1996.

[3] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Proc. of Springer Intl. Workshop on Information Hiding (IH)*, 2012.

[4] S. Grabski and K. Szczypiorski, "Steganography in OFDM symbols of fast IEEE 802.11 n networks," in *Proc. of IEEE Security and Privacy Workshops (SPW)*, 2013.

[5] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "A timing channel-based MAC protocol for energy-efficient nanonetworks," *Nano Communication Networks*, vol. 6, no. 2, pp. 39 – 50, 2015.

[6] K. Szczypiorski and W. Mazurczyk, "Hiding data in ofdm symbols of IEEE 802.11 networks," in *Proc. of IEEE Intl. Conf. on Multimedia Information Networking and Security (MINES)*. IEEE, 2010.

[7] T. Kho, "Steganography in the 802.15.4 physical layer," *Technical Report*, 2007.

[8] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: A game-theoretic analysis," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, 2015.

[9] E. Zielinska and K. Szczypiorski, "Direct sequence spread spectrum steganographic scheme for IEEE 802.15.4," in *Proc. of IEEE Intl. Conf. on Multimedia Information Networking and Security (MINES)*, 2011.

[10] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.

[11] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for WiFi systems," in *Proc. of IEEE Conf. on Communications and Network Security (CNS)*, 2015.

[12] H. Méric, "Approaching the gaussian channel capacity with apsk constellations," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1125–1128, 2015.

[13] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," *Communications of the ACM*, vol. 57, no. 3, pp. 86–95, 2014.

[14] S. Wendzel, W. Mazurczyk, L. Caviglione, and M. Meier, "Hidden and uncontrolled–on the emergence of network steganographic threats," in *Proc. of Springer Information Security Solutions Europe Conf. – Securing Electronic Business Processes (ISSE)*, 2014.

[15] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225–229, 2014.

[16] D. Martins and H. Guyennet, "Steganography in MAC layers of 802.15.4 protocol for securing wireless sensor networks," in *Proc. of IEEE Intl. Conf. on Multimedia Information Networking and Security (MINES)*, 2010.

[17] C. Krätzer, J. Dittmann, A. Lang, and T. Kühne, "WLAN steganography: a first practical review," in *Proc. of ACM Workshop on Multimedia and Security (MMSec)*, 2006.

[18] C. Cachin, "An information-theoretic model for steganography," in *Proc. of Springer Intl. Workshop on Information Hiding (IH)*, 1998.

[19] J. Fridrich, T. Pevnỳ, and J. Kodovskỳ, "Statistically undetectable JPEG steganography: dead ends challenges, and opportunities," in *Proc. of ACM Workshop on Multimedia & Security (MMSec)*. ACM, 2007.

[20] J. Proakis and M. Salehi, *Digital Communications*, ser. McGraw-Hill International Edition. McGraw-Hill, 2008.

[21] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.

[22] Ettus Research (A National Instrument Company), "USRP N210," https://www.ettus.com/product/details/UN210-KIT, 2018.

[23] Tektronix, "Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements," 2018. [Online]. Available: https://tinyurl.com/TektronixWiFi

[24] IEEE, "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - redline," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) - Redline*, pp. 1–5229, March 2012.

[25] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An IEEE 802.11a/G/P OFDM Receiver for GNU Radio," in *Proc. of ACM Workshop on Software Radio Implementation Forum (SRIF)*, 2013.

[26] Intel Corporation, "Intel Dual Band Wireless-AC 7265 Network Card," 2018. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/dual-band-wireless-ac-7265-brief.pdf