A Wireless Security Threat Arising from the Contamination of Transmission Pulse Shape

Sameer Raju Dhole, Maryam Farahnak-Ghazani, and Aria Nosratinia
Electrical and Computer Engineering Department, University of Texas at Dallas, USA
{sameer.dhole, maryam.farahnak, aria}@utdallas.edu

***Abstract*—We unveil a new hardware security threat that leaks unauthorized information from a wireless node by subtle manipulation of its pulse-shaping filter. We denote it as *Pulse-Shaping Trojan.* The leaked information is carried through a small variation to the envelope of the transmitted waveform, created by the pulse-shaping filter at the transmitter. The contamination of transmitter hardware can occur at many points in the IC fabrication supply chain; this is a well-recognized and realistic threat. We show that the pulse-shaping Trojan can be designed to have little to no impact on legitimate communication, including in the spectral mask as well as the bit-error rate of legitimate communication. Thus, it will be much more difficult to detect than earlier hardware Trojan threats. We explore the bitrate and bit-error rate of the information leaked by this Trojan, showing that this new threat is capable of effectively exfiltrating unauthorized information.**

***Index Terms*—Hardware Trojans, Covert Channel, Wireless Security**

I. Introduction

In an era characterized by the widespread use of smart devices and interconnected networks, the reliance on Integrated Circuits (ICs) has grown significantly. With this dependence, the vulnerabilities in the IC supply chain have become increasingly prominent. The introduction of Trojans at any point in this supply chain poses a substantial threat, emphasizing the need to investigate and comprehend these malicious entities. Hardware Trojans represent deliberate and malicious modifications within an IC intending to disrupt its proper operation or covertly extract sensitive information. These Trojans raise particularly grave concerns in the context of wireless networks, where they have the potential to compromise the security of any wireless standard.

While numerous hardware Trojan attacks and countermeasures have been documented in the literature [1]–[7], the majority of these studies have focused on digital circuits. However, in the ever-evolving technology landscape, there's a growing interest in investigating hardware Trojan threats within wireless networks, especially those employing basic wireless connections [8]–[12]. This emerging interest is primarily because wireless networks operate over open channels, eliminating the need for direct physical contact with the components. Moreover, emerging adversarial attacks that secretly extract data through side channels are becoming increasingly prevalent in recent literature [13], [14].

Due to conservative design principles that prioritize cost reduction and increased production, many real-world wireless devices operate well below their maximum potential. This creates a gap between the typical operating conditions and the maximum potential boundaries, which can be exploited by Trojans. For instance, [10] and [11] have investigated the variations in transmission power characteristics to develop amplitude-modulating wireless hardware Trojans. Similarly, [12] modifies the constellation of the transmitted symbols to carry out covert communication, while conforming to Error Vector Magnitude (EVM) guidelines.

This paper unveils a new security threat arising from the contamination of a wireless node. The new hardware Trojan manipulates the pulse-shaping filter that is present in every wireless transmitter.[1] In the sequel, we show that the pulse-shaping filter can be manipulated such that the transmission continues to satisfy all specifications including the EVM and spectral mask while leaking information covertly to a rogue receiver. The new threat has key distinctions compared with earlier discoveries such as the amplitude-modulating Trojan [10], [11] and dirty modulation [12]. Unlike the Trojans [10]–[12] in which the rogue information rides on top of the legitimate signal, the pulse-shaping Trojan carries the rogue information in a subspace approximately *orthogonal* to the legitimate signal. Therefore, it is invisible in the legitimate signal path at any point after the matched filter, where almost all of the decision-making and gathering of statistics in a receiver takes place. This is unprecedented in earlier threat discoveries, meaning that the operation of the new Trojan is far more covert compared with previously identified threats. Consequently, this Trojan is much more difficult to detect using metrics calculated on the legitimate signal path.

The paper is organized as follows: Section II introduces the legitimate system model. The details of the Rogue model, and the construction of the rogue pulse shape, are covered in Sections III and IV, respectively. Section V showcases simulations. Finally, in Section VI, we present concluding remarks.

II. System Model

Fig. 1 illustrates the system model used in this study. The model depicted in this figure represents the baseband equivalent model for a legitimate communication between the

This work was supported in part by the NSF grant 2148211.

[1] corresponding to the time inverse of the matched filter at the receivers

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622168

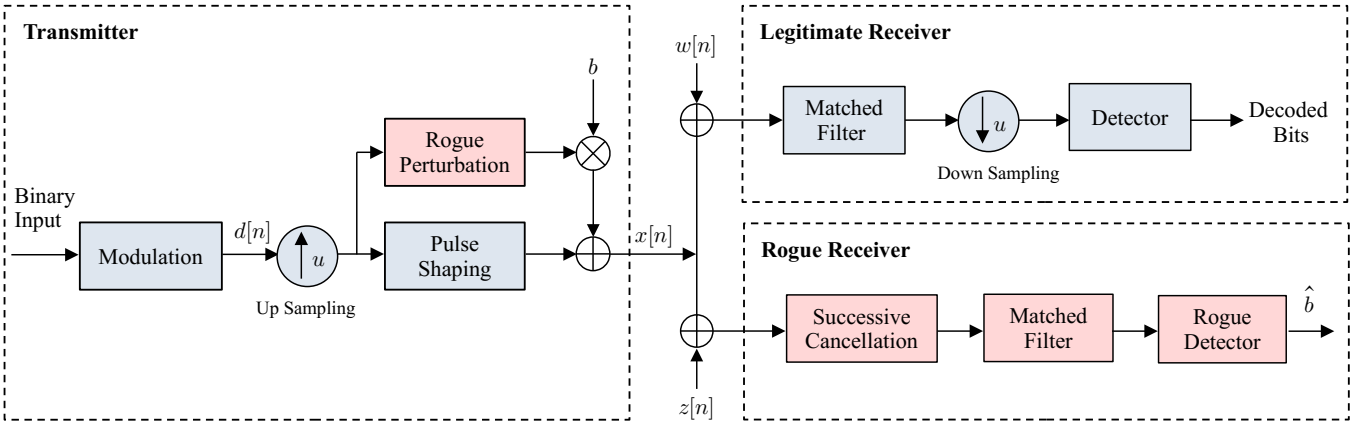


Fig. 1: System model.

transmitter and the receiver (Legitimate Receiver). This model includes standard components typical of digital communication systems. One of the key aspects of this model is the pulse-shaping filter applied to the modulated symbols. This paper focuses on a novel hardware Trojan threat that covertly targets this pulse-shaping process. Operating without the transmitter's knowledge, the Trojan's main objective is to leak specific data to a rogue receiver.

As shown in Fig. 1, within the transmitter, the modulated data symbols undergo up-sampling and pass through a pulse-shaping filter before being sent into the channel. Therefore, the original transmitted signal from the Tx, denoted by $x[n], n \in \mathbb{Z}$, can be characterized as

$$x[n] = p[n] \circledast d\left[\frac{n}{u}\right] = \sum_{k=0}^{\infty} p[n-ku]d\left[k\right], \tag{1}$$

where $p[n]$ represents the pulse-shaping filter, $d[n]$ is the modulated data symbol at the time instance n, and u is the up-sampling factor. The pulse-shaping filters are intentionally designed to be symmetric i.e., $p[n] = p[-n]$, ensuring a linear phase response.

Typically, in digital communication systems, pulse shaping is realized using Finite Impulse Response (FIR) filters [15], with the coefficients denoted by vector $\mathbf{p} = [p_1, ..., p_L]^{\mathrm{T}} \in \mathbb{R}^{L\times 1}$. The pulse-shaping filter introduces a delay in the system, which represents the amount of time it takes for the pulse-shaping filter to generate an output after receiving an input. According to the pulse-shaping filter size, the filter delay is equivalent to $L-1$ time intervals. We employ the matrix construction of the up-sampling and convolution operations in (1) for finite sequences, taking into account the filter delay and eliminating the first $L-1$ output samples. We then re-index them to obtain the output vector $\mathbf{x} \in \mathbb{R}^{M\times 1}$ as follows:

$$\mathbf{x} = \mathbf{PUd}, \tag{2}$$

where, $\mathbf{d} = [d_1, ..., d_N]^{\mathrm{T}} \in \mathbb{R}^{N\times 1}$ is the finite length vector of data symbols, $\mathbf{U} \in \mathbb{R}^{M\times N}$ is the up-sampling matrix with up-sampling factor u, i.e., $u = \frac{M}{N}$. The (i,j)-th element of the matrix $\mathbf{U}$ is given by $\{\mathbf{U}\}_{i,j} = \delta[(i-1) - u(j-1)], i \in \{1, ..., M\}, j \in \{1, ..., N\}$. The up-sampling matrix can be represented as follows:

$$\mathbf{U} = \begin{bmatrix} 1 & & \mathbf{0}_{N-1} \\ & \mathbf{0}_{(u-1)\times N} & \\ 0 & 1 & \mathbf{0}_{N-2} \\ & \mathbf{0}_{(u-1)\times N} & \\ \mathbf{0}_2 & 1 & \mathbf{0}_{N-3} \\ \vdots & \vdots & \vdots \end{bmatrix}. \tag{3}$$

Moreover, $\mathbf{P} \in \mathbb{R}^{M\times M}$ is a Toeplitz matrix utilized for constructing the convolution operation for the pulse-shaping filter, which can be characterized as follows:

$$\mathbf{P} = \begin{bmatrix} p_L & p_{L-1} & \cdots & p_1 & 0 & \cdots & 0 & 0 \\ 0 & p_L & \cdots & p_2 & p_1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & p_L & p_{L-1} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & p_L \end{bmatrix}. \tag{4}$$

A. Legitimate Receiver

The transmitted signal traverses an AWGN channel to reach the legitimate receiver. Therefore, the received signal at the legitimate receiver, denoted by $\mathbf{r} \in \mathbb{R}^{M\times 1}$ is as follows:

$$\mathbf{r} = \mathbf{x} + \mathbf{w}, \tag{5}$$

where $\mathbf{w} \in \mathbb{R}^{M\times 1}$ represents the channel noise. The elements of the noise vector follow an i.i.d Gaussian distribution with variance σ^2, i.e., $\mathbf{w} \sim \mathcal{N}(0, \sigma^2\mathbf{I}_M)$. At the legitimate receiver, match filtering is performed using the time-reversed transmitter pulse shape. However, since the pulse-shaping filter is symmetric, this time-reversed version remains identical to the pulse shape used at the transmitter. Subsequently, the signal undergoes down-sampling to yield the estimated symbols. These estimated symbols are then passed through a detector to obtain the binary bits.

Using the matrix formulation of the filters, the estimated symbol vector at the transmitter, denoted by $\hat{\mathbf{d}} \in \mathbb{R}^{N\times 1}$, is obtained as follows:

$$\widehat{\mathbf{d}} = \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{r}, \tag{6}$$

where $\mathbf{U}^{\mathrm{T}} \in \mathbb{R}^{N\times M}$ is the down-sampling matrix. Using (2) and (5), the estimated data symbols can be simplified as

$$\hat{\mathbf{d}} = \mathbf{U}^{\mathrm{T}}\mathbf{P}(\mathbf{x}+\mathbf{w}) = \mathbf{U}^{\mathrm{T}}\mathbf{P}^2\mathbf{U}\mathbf{d} + \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{w}. \tag{7}$$

To obtain the SNR at the receiver, let $\mathbf{s} = \mathbf{U}^{\mathrm{T}}\mathbf{P}^2\mathbf{U}\mathbf{d}$ denote the signal component and $\mathbf{n} = \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{w}$ denote the noise component. Hence, the SNR per symbol at the legitimate receiver can be obtained using the following equation:

$$\mathrm{SNR} = \frac{\mathbb{E}\left[\mathbf{s}^{\mathrm{T}}\mathbf{s}\right]}{\mathbb{E}\left[\mathbf{n}^{\mathrm{T}}\mathbf{n}\right]}. \tag{8}$$

By simplifying this equation, we get

$$\mathrm{SNR} = \frac{E_{\mathrm{s}}}{\sigma^2}, \tag{9}$$

where $E_{\mathrm{s}} = \mathbb{E}[\|\mathbf{d}\|_2^2]$ is the average energy per symbol.

III. Pulse-Shaping Trojan

The pulse-shaping Trojan introduced in this paper adds a perturbation to the pulse-shaping filter at the transmitter. Specifically, within the pulse shaping block in Fig. 1, we introduce two new elements in addition to $\mathbf{p}$: the rogue perturbation, denoted by the vector $\mathbf{q} \in \mathbb{R}^{L\times 1}$, and a switching action dictated by $b \in \{0,1\}$. b represents rogue bits, signifying the information the Trojan aims to transmit from the system to the rogue receiver covertly. Hence, the vector $\mathbf{q}$ is added to the pulse-shaping vector $\mathbf{p}$ based on the rogue bits. When $b = 1$, the pulse shaping of $\mathbf{p}+\mathbf{q}$ is applied to the sequence of length N of legitimate symbols. Conversely, when $b = 0$, we resort to the standard pulse shaping operation. Importantly, it should be noted that the rate of legitimate data symbols is N times greater than the rate of the rogue data bits. Consequently, the transmitted signal in (2) is modified by the Trojan as follows:

$$\widetilde{\mathbf{x}} = (\mathbf{P}+b\mathbf{Q})\mathbf{U}\mathbf{d}, \tag{10}$$

where $\mathbf{Q} \in \mathbb{R}^{M\times M}$ is a Toeplitz matrix similar to $\mathbf{P}$ in (4), which contains the elements of vector $\mathbf{q}$ in its rows.

A. Legitimate Receiver

The received signal at the legitimate receiver in the presence of the Trojan is obtained as:

$$\widetilde{\mathbf{r}} = \widetilde{\mathbf{x}} + \mathbf{w} = (\mathbf{P}+b\mathbf{Q})\mathbf{U}\mathbf{d} + \mathbf{w}. \tag{11}$$

The Trojan influences the performance of the legitimate receiver, as it performs match filtering with $\mathbf{p}$ and not $\mathbf{p}+\mathbf{q}$. Hence, the following estimated symbols are obtained in the presence of the Trojan:

$$\widehat{\mathbf{d}} = \mathbf{U}^{\mathrm{T}}\mathbf{P}\widetilde{\mathbf{r}} = \mathbf{U}^{\mathrm{T}}\mathbf{P}^2\mathbf{U}\mathbf{d} + \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{w} + \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{Q}\mathbf{U}\mathbf{d}. \tag{12}$$

To obtain the SNR at the receiver, similar to (7), let $\mathbf{s} = \mathbf{U}^{\mathrm{T}}\mathbf{P}^2\mathbf{U}\mathbf{d}$ and $\mathbf{n} = \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{w}$. However, unlike before, there is an interference term $\mathbf{i} = \mathbf{U}^{\mathrm{T}}\mathbf{P}\mathbf{Q}\mathbf{U}\mathbf{d}$, leading to the SINR formula:

$$\mathrm{SINR} = \frac{\mathbb{E}\left[\mathbf{s}^{\mathrm{T}}\mathbf{s}\right]}{\mathbb{E}\left[\mathbf{n}^{\mathrm{T}}\mathbf{n}\right] + \mathbb{E}\left[\mathbf{i}^{\mathrm{T}}\mathbf{i}\right] + \mathbb{E}\left[\mathbf{i}^{\mathrm{T}}\mathbf{n}\right] + \mathbb{E}\left[\mathbf{n}^{\mathrm{T}}\mathbf{i}\right]}.$$

Since $\mathbf{d}$ and $\mathbf{w}$ are independent, we have $\mathbb{E}\left[\mathbf{i}^{\mathrm{T}}\mathbf{n}\right] = \mathbb{E}\left[\mathbf{n}^{\mathrm{T}}\mathbf{i}\right] = 0$. Thus, the above equation simplifies to

$$\mathrm{SINR} = \frac{E_{\mathrm{s}}}{\sigma^2 + E_{\mathrm{s}}(\|\mathbf{p}\circledast\mathbf{q}\|_2^2)}, \tag{13}$$

where $\mathbf{p}\circledast\mathbf{q}$ is the convolution of the legitimate pulse and perturbation vectors.

B. Rogue Receiver

At the rogue receiver, we are interested in decoding rogue bit $b \in [0,1]$. The following signal is obtained at the rogue receiver after passing through the channel:

$$\mathbf{r}_{\mathrm{g}} = \widetilde{\mathbf{x}} + \mathbf{z} = \mathbf{P}\mathbf{U}\mathbf{d} + b\mathbf{Q}\mathbf{U}\mathbf{d} + \mathbf{z}, \tag{14}$$

where $\mathbf{z}$ is the AWGN noise vector with variance σ^2. For the detection of the rogue bit, we need to have the legitimate data symbols $\mathbf{d}$. The rogue receiver can decode the legitimate symbols similar to the legitimate receiver in section III-A. Here, we assume there is no error in this detection. In Section V, we investigate the effect of the detection error of the legitimate data symbols on the performance of the rogue receiver. Knowing $\mathbf{d}$, we can eliminate the first term in (14), referred to as successive cancellation in Fig. 1. Thus, we obtain

$$\overline{\mathbf{r}}_{\mathrm{g}} = b\mathbf{s}_{\mathrm{g}} + \mathbf{z}, \tag{15}$$

where $\mathbf{s}_{\mathrm{g}} = [s_1, ..., s_M]^{\mathrm{T}}$ is defined as $\mathbf{s}_{\mathrm{g}} = \mathbf{Q}\mathbf{U}\mathbf{d}$. By employing the Maximum Likelihood (ML) detection at the receiver, we have:

$$p(\overline{\mathbf{r}}_{\mathrm{g}}|b=1) \underset{b=0}{\overset{b=1}{\gtrless}} p(\overline{\mathbf{r}}_{\mathrm{g}}|b=0). \tag{16}$$

Knowing the legitimate data symbols and conditioned on the rogue bits, the elements of $\overline{\mathbf{r}}_{\mathrm{g}} = [r_1, ..., r_M]^{\mathrm{t}}$ are independent and have Gaussian distribution with mean 0 for $b = 0$ and mean $\mu_i = s_i, i = 1, ..., M$ for $b = 1$. Hence, (16) reduces to

$$\exp\left(\frac{1}{2}\sum_{i=1}^{M}\left(\frac{r_i-\mu_i}{\sigma}\right)^2\right) \underset{b=1}{\overset{b=0}{\gtrless}} \exp\left(\frac{1}{2}\sum_{i=1}^{M}\left(\frac{r_i}{\sigma}\right)^2\right). \tag{17}$$

After simplification, we get

$$\mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\overline{\mathbf{r}}_{\mathrm{g}} \underset{b=0}{\overset{b=1}{\gtrless}} \frac{1}{2}\|\mathbf{s}_{\mathrm{g}}\|_2^2. \tag{18}$$

Hence, the rogue matched filter is obtained as $\mathbf{s}_{\mathrm{g}} = \mathbf{Q}\mathbf{U}\mathbf{d}$. This implies that the legitimate symbols $\mathbf{d}$ are required for both successive cancellation and matched filtering. After matching, we have

$$\mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\overline{\mathbf{r}}_{\mathrm{g}} = b\mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\mathbf{s}_{\mathrm{g}} + \mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\mathbf{z}. \tag{19}$$

Hence, the SNR per rogue bit b is obtained as

$$\mathrm{SNR}_{\mathrm{rog}} = \frac{\mathbb{E}\left[\left(\mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\mathbf{s}_{\mathrm{g}}\right)^2\right]}{\mathbb{E}\left[\left(\mathbf{s}_{\mathrm{g}}^{\mathrm{T}}\mathbf{z}\right)^2\right]}, \tag{20}$$

which leads to

$$\mathrm{SNR}_{\mathrm{rog}} = N\|\mathbf{q}\|_2^2\,\mathrm{SNR}\,. \tag{21}$$

This shows that $\mathrm{SNR}_{\mathrm{rog}}$ depends on the SNR of the legitimate data symbols and the number of legitimate data symbols used for sending the rogue bit, i.e., N.

IV. Rogue Pulse Design

The rogue perturbation $\mathbf{q}$ needs to be designed to meet several criteria. The main objective is to maximize the SINR of the Legitimate Receiver in (13) while also maximizing the SNR of the rogue bit in (21). The optimization problem below details the objective function and the constraints utilized to generate $\mathbf{q}$:

$$\min_{\mathbf{q}} \quad \|\mathbf{p} \circledast \mathbf{q}\|_2^2 \tag{22}$$

$$\text{s.t.} \quad (\mathbf{p}+\mathbf{q})^t \mathbf{f}\left(\omega_i\right)\mathbf{f}\left(\omega_i\right)^t(\mathbf{p}+\mathbf{q}) \le v\left(\omega_i\right), \tag{23}$$

$$\|\mathbf{q}\| \ge \sqrt{\frac{\mathrm{SNR}_{\mathrm{rog}}}{N \times \mathrm{SNR}}}, \tag{24}$$

$$\|\mathbf{p}+\mathbf{q}\|_2^2 < \|\mathbf{p}\|_2^2 + \alpha, \tag{25}$$

$$q[j] = q[L-j-1] \quad \forall \quad 0 \le j < L. \tag{26}$$

The objective function in (22) aims to minimize the impact of the rogue pulse shape on legitimate transmission, as it contributes to the interference term in (13). Ideally, this minimization would result in orthogonality between $\mathbf{p}$ and $\mathbf{q}$, which also leads to orthogonality in the frequency domain. However, achieving such orthogonality in the frequency domain may lead to a frequency response for $\mathbf{p}+\mathbf{q}$ that exceeds the spectral mask constraints imposed by communication standards (e.g., IEEE 802.11, 3GPP). Thus, to prevent spectral leakage, we introduce the constraint in (23), which enforces an upper limit on the power spectral density of the pulse shape, which is discussed in [15]. In this equation, $\mathbf{f}(w_i)$ represents the Fourier transform vector at frequency w_i, where $[\mathbf{f}\left(\omega_i\right)]_n = e^{j\omega_i n}$, and v signifies the spectral mask constraint. In Section V, we provide a demonstration of this concept using an example spectral mask specified in IEEE 802.11b.

There is also a requirement to maintain a minimum amount of energy for $\mathbf{q}$, as enforced by the constraint in (24), derived from (21). However, it is essential to prevent the energy of the rogue pulse from increasing excessively compared to the energy of the original pulse shape $\mathbf{p}$. This control is achieved through the constraint (25), where α is a small positive scalar. Moreover, the constraint (26) is employed to ensure the symmetry of the optimization result, resulting in a linear phase response for the filter.

As (24) represents a non-convex constraint, it renders the overall problem non-convex. Consequently, we require solvers tailored for non-convex problems. In Section V, we utilize the Sequential Least Squares Quadratic Programming (SLSQP) method to solve this optimization problem. SLSQP is specifically designed to address non-linear constrained optimization problems and is particularly effective when dealing with smooth functions.

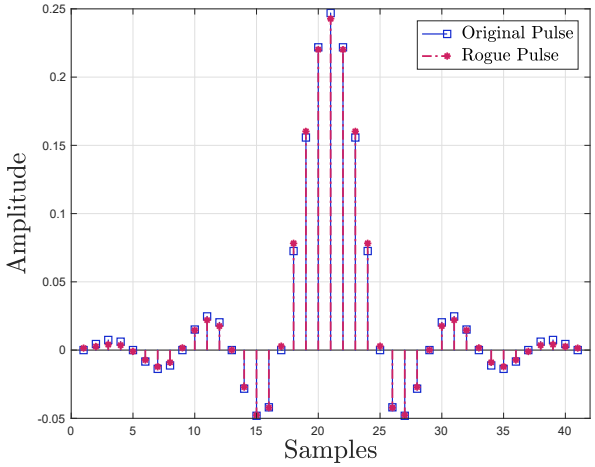


Fig. 2: Impulse response of the original pulse $\mathbf{p}$ and rogue pulse $\mathbf{p}+\mathbf{q}$.

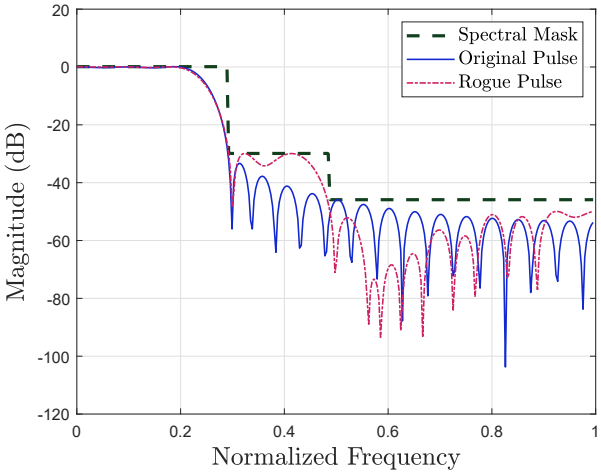


Fig. 3: FFT of the original pulse $\mathbf{p}$ and rogue pulse $\mathbf{p}+\mathbf{q}$.

V. Simulation Results

A. Optimization Results

For our experimental simulations, we adopted a pulse-shaping filter, $\mathbf{p}$, in accordance with the IEEE 802.11b standard [16]. This filter is generated using a root-raised cosine (RRC) with a span of 10 symbols, a roll-off factor of 0.2, and an up-sampling factor of $u = 4$. Hence, the pulse-shaping vector length is $K = (\text{span} \times u) + 1 = 41$. Building upon our discussion in Section IV, the The SLSQP method was employed to address the optimization challenge. As we utilize BPSK modulation for these experiments, $\sigma^2 = \mathrm{No}, E_{\mathrm{s}} = E_{\mathrm{b}}$, where No is the power spectral density of the signal, and E_{b} is the energy per bit. We set $\alpha = 0.05$. We set the SNR for legitimate transmission at 10 dB, since according to [17], the

TABLE I: Optimization Results

Metric	Value
Objective Function (22)	9.7033527×10^{-5}
$\|\mathbf{q}\|_2^2$	2.4849557×10^{-4}
$\|\mathbf{p}\|_2^2$	$2.31688827 \times 10^{-1}$
$\|\mathbf{p}+\mathbf{q}\|_2^2$	$2.31688923 \times 10^{-1}$

throughput saturates for most modes of IEEE 802.11b after reaching 10 dB SNR. We set the number of encoding symbols, N, to 5000. Based on a Bit Error Rate (BER) of 10^{-3} for On-Off Keying (OOK) modulation, we designated the rogue SNR, SNR_{rog}, to be 10.94 dB [18].

Table 1 summarizes the results of the optimization. As we can see, the objective function achieves an extremely low value, while maintaining a relatively higher energy in the perturbation $\|\mathbf{q}\|$. The optimization also ensures that the energy of the rogue pulse, $\|\mathbf{p}+\mathbf{q}\|$, is not too different compared to $\|\mathbf{p}\|$. This is also seen via Fig. 2, where the coefficients of the rogue pulse are nearly identical to the original. Additionally, as seen in Fig. 3, the rogue tends to increase its frequency components past 0.6, in an attempt to be orthogonal to $\mathbf{p}$, however, the Spectral Mask constraint prevents it from doing so.

B. Impact on Legitimate Transmission

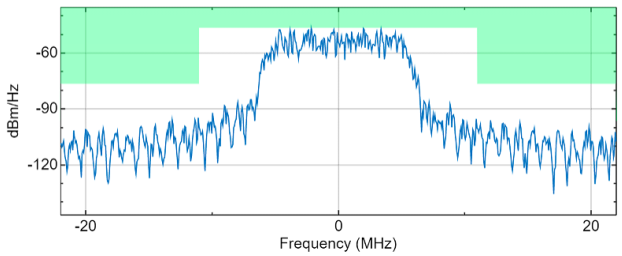
The original pulse $\mathbf{p}$ complies with the IEEE 802.11b standards, as confirmed by the spectral mask verification presented in Fig. 4a. In this illustration, the curve depicts the power spectral density of the transmitted signal $\mathbf{x}$, and the shaded region denotes the spectral mask boundary. Notably, the power spectral density does not fully occupy the available region within the spectral mask. This vacant space allows for the introduction of a rogue perturbation, $\mathbf{q}$, resulting in the rogue pulse $\mathbf{p}+\mathbf{q}$. As shown in Fig. 4b, this constructed rogue pulse remains within the acceptable spectral mask limits, emphasizing its capability to operate covertly without triggering detection mechanisms.

To evaluate the effect on the legitimate transmission, we referred to the parameters discussed in (13). Our simulations covered 5×10^6, randomly generated, uncoded BPSK modulated signals transmitted across an AWGN channel. We conducted these simulations for both scenarios: rogue bit $b = 1$ and $b = 0$ i.e. pulse shapes $\mathbf{p}$ and $\mathbf{p}+\mathbf{q}$, respectively. As illustrated in Fig. 5, there is no visible disparity in the BER between the two scenarios.

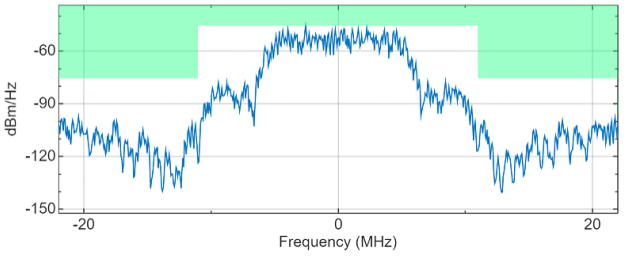
C. Efficacy of Covert Communication

The efficacy of covert communication was evaluated by calculating the bit error rate (BER) subject to Additive White Gaussian Noise. This was performed for 10,000 randomly generated bits. The y-axis denotes the BER, while the x-axis denotes the SNR for the legitimate symbols.

At the rogue detector, before detecting the rogue bits, the legitimate symbols are detected, similar to the approach discussed in Section III-A. Then using the detected legitimate symbols, the rogue bits are detected using (18). As observed



(a)



(b)

Fig. 4: Power spectral density of transmitted signal $\mathbf{x}$ alongside the IEEE 802.11b spectral mask using (a) the original pulse $\mathbf{p}$ (b) the rogue pulse $\mathbf{p}+\mathbf{q}$.

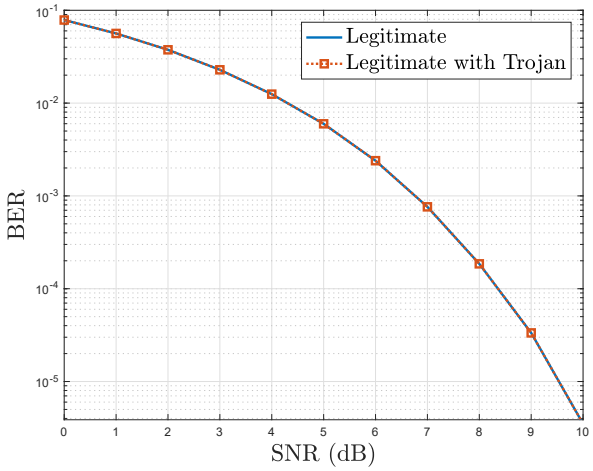


Fig. 5: Impact of rogue on BER for legitimate bits.

in Fig. 6, the BER for the rogue detection is relatively high between 5-7 dB SNRs. This is primarily due to the high detection error in the decoding of the legitimate symbols at lower SNRs for the rogue detection. However, at 11 dB, there is a sharp drop for the rogue detection. This drop is a result of the minimum energy constraint in (25) in our design of $\mathbf{q}$, where we set the SNR_{rog} value $\approx$ 11 dB corresponding to a Rogue BER $\leq 10^{-3}$.

VI. Conclusions

In this paper, we introduced the Pulse-Shaping Trojan, a new hardware security threat that discreetly leaks unauthorized information by manipulating a wireless transmitter's pulse-shaping filter. This threat poses a unique challenge due to its minimal impact on legitimate communication, making it

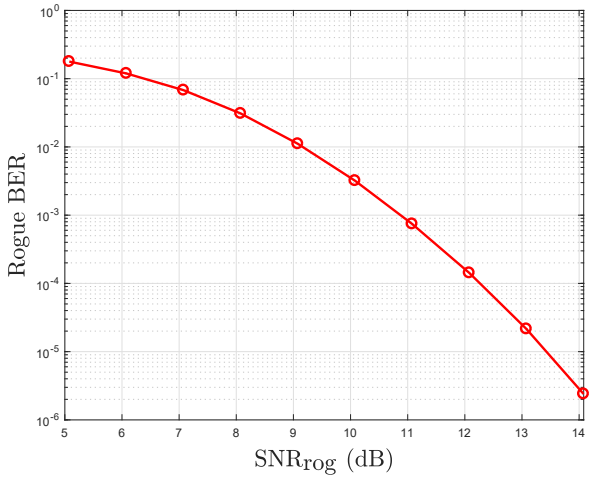


Fig. 6: BER for rogue bits.

challenging to detect. Our findings demonstrated the Pulse-Shaping Trojan's capacity to exfiltrate unauthorized data effectively. As such, it underscores the importance of robust security measures to protect wireless communication systems from this newly discovered threat.

REFERENCES

[1] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons learned after one decade of research," *ACM Trans. on Design Automation of Electronic Sys. (TODAES)*, vol. 22, no. 1, pp. 1–23, 2016.

[2] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[3] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, pp. 10–25, 2010.

[4] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[5] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting," in *Proc. of the 51st Annual Design Automation Conf.*, 2014, pp. 1–6.

[6] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious off-chip leakage enabled by side-channels," in *Proc. of the 2009 Int. Conf. on computer-aided design*, 2009, pp. 117–122.

[7] K. S. Subraman, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "Demonstrating and mitigating the risk of an FEC-based hardware Trojan in wireless networks," *IEEE Trans. on Information Forensics and Security*, vol. 14, no. 10, pp. 2720–2734, 2019.

[8] N. Kiyavash, F. Koushanfar, T. P. Coleman, and M. Rodrigues, "A timing channel spyware for the CSMA/CA protocol," *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 3, pp. 477–487, 2013.

[9] D. Chang, B. Bakkaloglu, and S. Ozev, "Enabling unauthorized RF transmission below noise floor with no detectable impact on primary communication performance," in *2015 IEEE 33rd VLSI Test Symposium (VTS)*. IEEE, 2015, pp. 1–4.

[10] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, "Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs," *IEEE Trans. on Very Large Scale Integration (VLSI) Sys.*, vol. 25, no. 4, pp. 1506–1519, 2016.

[11] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-modulating analog/RF hardware Trojans in wireless networks: Risks and remedies," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 3497–3510, 2020.

[12] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Information Hiding: 14th Int. Conf., IH 2012, Berkeley, CA, USA, May 15-18, 2012, Revised Selected Papers 14*. Springer, 2013, pp. 160–175.

[13] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," in *Proc. of the 2018 ACM SIGSAC Conf. on Computer and Comm. Security*, 2018, pp. 163–177.

[14] G. Goller and G. Sigl, "Side channel attacks on smartphones and embedded devices using standard radio equipment," in *Int. Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2015, pp. 255–270.

[15] T. N. Davidson, "Enriching the art of FIR filter design via convex optimization," *IEEE signal processing magazine*, vol. 27, no. 3, pp. 89–101, 2010.

[16] "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," *ANSI/IEEE Std 802.11, 1999 Edition (R2003)*, pp. i–513, 2003.

[17] I. Haratcherev, K. Langendoen, R. Lagendijk, and H. Sips, "Hybrid rate control for IEEE 802.11," in *Proc. of the second Int. workshop on Mobility management & wireless access protocols*, 2004, pp. 10–18.

[18] B. Sklar, *Digital Communications: Fundamentals and Applications*. USA: Prentice-Hall, Inc., 1988.