JamRF: Performance Analysis, Evaluation, and Implementation of RF Jamming over Wi-Fi

Abubakar S. Ali 1, Michael Baddeley 1, Lina Bariah 2, Martin Andreoni 1, Willian T. Lunardi 1, Jean-Pierre Giacalone 1, and Sami Muhaidat 1

1Affiliation not available
2Technology Innovation Institute

October 30, 2023

Abstract

Jamming attacks significantly degrade the performance of wireless communication systems and can lead to significant overhead in terms of re-transmissions and increased power consumption. Although different jamming techniques are discussed in the literature, numerous open-source implementations have used expensive equipment in the range of thousands of dollars with the exception of a few. These implementations have also tended to be partial band, and do not cover the whole available bandwidth of the system under attack. In this work, we demonstrate that flexible, reliable, and low priced software-defined radio (SDR) jamming is feasible by designing and implementing different types of jammers against IEEE 802.11n networks. First, to demonstrate the optimal jamming waveform, we present an analytical bit error rate expression of the system under attack by employing two common jamming waveforms: Gaussian noise and digitally modulated. Then, we validate this analysis through simulations using the MATLAB WLAN toolbox. Afterwards, we implement JamRF, a toolkit that employs a low-cost SDR to implement numerous types of jammers to validate the analysis. Obtained results showed that, to jam the whole 2.4GHz spectrum, a stateful-reactive jammer employing random channel hopping jamming strategy, achieves a packet loss ratio above 90%.
JamRF: Performance Analysis, Evaluation, and Implementation of RF Jamming over Wi-Fi

Abubakar S. Ali, Student Member, IEEE, Michael Baddeley, Member, IEEE, Lina Bariah, Senior Member, IEEE, Martin Andreoni Lopez, Member, IEEE, Willian T. Lunardi, Member, IEEE, Jean-Pierre Giacalone, and Sami Muhaidat, Senior Member, IEEE

Abstract—Jamming attacks significantly degrade the performance of wireless communication systems and can lead to significant overhead in terms of re-transmissions and increased power consumption. Although different jamming techniques are discussed in the literature, numerous open-source implementations have used expensive equipment in the range of thousands of dollars with the exception of a few. These implementations have also tended to be partial band, and do not cover the whole available bandwidth of the system under attack. In this work, we demonstrate that flexible, reliable, and low priced software-defined radio (SDR) jamming is feasible by designing and implementing different types of jammers against IEEE 802.11n networks. First, to demonstrate the optimal jamming waveform, we present an analytical bit error rate expression of the system under attack by employing two common jamming waveforms: Gaussian noise and digitally modulated. Then, we validate this analysis through simulations using the MATLAB WLAN toolbox. Afterwards, we implement JamRF, a toolkit that employs a low-cost SDR to implement numerous types of jammers to validate the analysis. Obtained results showed that, to jam the whole 2.4GHz spectrum, a stateful-reactive jammer employing random channel hopping jamming strategy, achieves a packet loss ratio above 90%.

Index Terms—Bit error rate (BER), IEEE 802.11n, Jamming, Software defined radio (SDR), Wi-Fi

I. INTRODUCTION

The broadcast nature of wireless channels renders transmitted wireless signals vulnerable to external interference, as well as potential malicious jamming attacks. Adversarial users are generally categorized into passive eavesdroppers, that try to intercept transmitted signals and extract information without being detected, and active jammers, that aim to degrade signals quality, and hence, prevent the recipient from receiving the required transmitted information. These security threats have been deemed as a critical concern due to the increasing reliance on wireless services [1]. A swarm of Unmanned Aerial Vehicles (UAVs), for example, commonly employ off-the-shelf infrastructure-less wireless communication (such as 802.11s in mesh mode) which can be significantly affected by external threats [2].

Furthermore, with the recent advances in low-cost SDR technologies, it has become remarkably easy to launch jamming attacks on wireless networks, and off-the-shelf devices such as a USRP [3], HackRF [4], or BladeRF [5] have introduced a low-barrier to entry. These devices are powerful, flexible, and can be tuned to cover a wide range of radio frequency (RF), costing between hundreds to a few thousand dollars. On the other hand, SDRs, such as rtl-SDR [6] and Airspy [7], can be obtained with more affordable prices, with some limitations on the operating frequency. Military and commercial jamming devices [8-10] can be employed to launch attacks on various types of wireless networks. These however, are very expensive and are less flexible compared to SDRs.

Within this context, different types of jamming strategies have been proposed in the literature, in order to significantly deteriorate the performance of a particular wireless communication system. This has further motivated the renewed research on RF jamming mitigation schemes, with the aim to study different kinds of jamming strategies, and hence, mitigate their effects. To the best of the authors’ knowledge, there is no prior work that provides both extensive analysis, simulation study and real-world implementation of different types of jamming attacks on Wi-Fi systems using SDR.

Therefore, in this work we study the performance of a WLAN IEEE 802.11n communication networks in the presence of jamming. Furthermore, we provide an implementation of different types of jammers on a HackRF. Specifically, the main contributions of this work are: i) Presenting the Bit Error Rate (BER) performance analysis for the IEEE 802.11n communication system in the presence of jammers and under the assumption of Gaussian noise and digitally modulated (QPSK) waveforms; ii) Validation of the analysis through MATLAB simulation, evaluating the impact of these jamming waveforms (Gaussian noise and QPSK) on the performance of IEEE 802.11n communications; iii) The development and implementation of ‘JamRF’, a jamming toolkit for the HackRF SDR; and iv) Investigating the impact of the considered different jamming techniques on IEEE 802.11n communications through practical experimentation within an RF isolation chamber.

This rest of the paper is organized as follows. Background and related works is presented in Sec. II. We introduce the employed system model in Sec. III. In Sec. IV we present

1Available at https://github.com/tiiuae/sdr-jammer/HackRF

https://github.com/tiiuae/sdr-jammer/simulation
the performance analysis of the victim system under jamming attack. Simulation results are presented and discussed in Sec. VI. Section VII presents the experiments and the discussions of the obtained results. Finally, the paper is concluded in Sec. VII.

Table I presents a comparison of the features and prices of several common wide-band commercial SDRs. The table highlights the SDRs, their tune low and high values, receive bandwidth, ADC resolution, transmission mode, and price.

Generally speaking, jammers can be classified into five types based on their capability to sense the wireless medium, react, and maintain a state that dictates their future actions as presented in Fig. 1.

Proactive jammers are also known as channel-oblivious jammers, in which a malicious node transmits jamming signals whether there is a channel activity or not. The aim of this jammer is to put all nodes in the network that intend to transmit over the jammed channel, into a non-operating mode [30]. This type of jammer is relatively easy to implement [20]. Proactive jammers are memoryless due to the fact that they are channel-oblivious.

Reactive jammers are also known as channel-aware jammers, in which a malicious node sends an interfering radio signal when it detects legitimate packets transmitted over the air [19]. Reactive jamming attacks are widely regarded as an energy-efficient attack strategy since the jammer is active only when there are data transmissions in the network. Reactive jamming attacks, however, require tight timing constraints (e.g., < 1 OFDM symbols, 4 µs) for real-world system implementation, as it needs to switch from listening mode to transmitting mode quickly [20]. In practice, a jammer may be triggered by either channel energy-sensing or part of a legitimate packet’s detection (e.g., preamble detection). Prasad and Thuente [13] implemented a reactive jamming attack in legacy Wi-Fi networks using the energy detection capability of cognitive radio devices. In [14, 15], the authors studied a reactive jamming attack where a jammer sends a jamming signal after detecting the preamble of the transmitted Wi-Fi packets. By doing so, the jammer is capable of effectively attacking Wi-Fi packet payloads. A stateful reactive jammer is the most sophisticated type, due to its capability to maintain a state that dictates its future actions [17].

Constant jammers are also known as single-band jammers, in which the jammer may target the entire or a fraction of a channel bandwidth occupied by legitimate users [30, 32]. Such a jammer continually emits radio signals on the wireless medium. The signals can consist of a completely random sequence of bits or regular packets. Karhima et al. [11] analyzed the performance of legacy Wi-Fi communications under broadband and partial-band constant jamming attacks through theoretical exploration and experimental measurement [11].

Deceptive jammer is a type of jammer similar in operation to the constant jammer. However, here, the malicious jamming device sends meaningful radio signals to a Wi-Fi access point or legitimate Wi-Fi client devices, with the aim of wasting the

| SDR            | Tune Low (MHz) | Tune High (MHz) | RX Bandwidth (MHz) | ADC Resolution (Bits) | Transmission Mode           | Price (USD) |
|----------------|----------------|-----------------|--------------------|-----------------------|-----------------------------|--------------|
| RTL-SDR R820T | 24             | 1766            | 3.2/2.56           | Stable                | No                          | 20           |
| Airspy R2      | 24             | 1800            | 0.192              | 16                    | No                          | 200          |
| HackRF One     | 30             | 6000            | 20                 | 8                     | Half Duplex                 | 300          |
| BladeRF xA4    | 300            | 6000            | 40                 | 12                    | Full Duplex                 | 1000         |
| USRP B200      | 70             | 6000            | 56                 | 12                    | Full Duplex                 | 1200         |

Fig. 1: Classification of Jammers in Wireless Networks.
TABLE II: Comparison of JamRF with prior works

| Ref. | Jamming System/Testbed | Victim System | Strategy | Jamming Signal | Channel Awareness | Frequency Band | Memory State | Transmission |
|------|-----------------------|---------------|----------|----------------|-------------------|----------------|--------------|--------------|
| [11] | Lecroy LW420 + HP 8780A | WLAN | IEEE 802.11b/g | Constant | Random bits | Proactive | Single-band | Memoryless | Continuous |
| [12] | Soekris net4826 + Intel-2915 | WLAN | IEEE 802.11a/g | Deceptive | Packets | Proactive | Single-band | Memoryless | Continuous |
| [13] | Simulation with OPNET | WLAN | IEEE 802.11a/g | Constant | Packets | Proactive/ Reactive | Single-band | Memoryless | Continuous/ Periodic |
| [14] | USRP-B200 + XCVR2450 | WLAN | IEEE 802.11g | Constant | Random bits | Reactive | Single-band | Memoryless | Continuous |
| [15] | USRP B200 + XCVR2450 | WLAN | IEEE 802.11g | Constant | Random bits | Reactive | Single-band | Memoryless | Continuous |
| [16] | USRP B200 | WLAN I | IEEE 802.15.4 | Deceptive | Packets | Proactive | Single-band | Memoryless | Continuous |
| [17] | USRP2 | WLAN | IEEE 802.11i | Constant | Packets | Proactive/ Reactive | single-band | Memoryless/ Stateful | Continuous/ Periodic |
| [18] | Simulation with OPNET | WLAN | IEEE 802.11g | Sweeping | Packets | Proactive | multi-band | Memoryless | Continuous |
| [19] | Simulation with OPNET | WLAN | IEEE 802.11n | Constant | Packets | Reactive | single-band | Memoryless | Continuous |
| [20] | USRP2 + Spartan-3 FPGA | WLAN | IEEE 802.15.4 | Constant | Random bits | Reactive | single-band | Memoryless | Continuous |
| [21] | Agilent M9330A | WLAN | IEEE 802.11n | Constant | Random bits | Proactive | single-band | Memoryless | Continuous |

**Network resources and preventing legitimate users from channel access.** Broustis et al. [12] implemented a deceptive jamming attack using a commercial Wi-Fi card. Also, Gvozdenovic et al. [16] proposed a deceptive jamming attack on Wi-Fi networks called truncate after preamble (TaP) jamming and evaluated its performance on a USRP testbed.

**Frequency Sweeping jammer** are multi-band jamming attacks proposed to get around the constraints posed by constant jammers ability to only jam a single-band, such that a jammer can quickly switch to different channels [30, 32]. In [18], the authors analyzed Wi-Fi networks’ performance under frequency-sweeping jamming attacks on 2.4 GHz, where there are only 3 non-overlapping 20 MHz channels, and demonstrated the negative impact of jamming on the performance of a WLAN system.

**Random channel hopping jammer** is similar to the sweeping jammer in its operation. In this jammer, however, the channel to jam is chosen randomly. This random behavior increases the detection difficulty when compared to the sweeping jammer.

**Periodic jammer** refers to the type of jammer that emits signals for random periods whilst sleeping the rest of the time. This type of jamming attacks allows the jammer to save more energy compared to a continuous jamming attack by continuously switching between two states: a sleep phase and a jamming phase. However, it is less effective compared to continuous jamming attacks [30]. Bayraktaroglu et al. [17] investigated the impact of periodic jamming attacks on Wi-Fi networks, realizing that periodic, memoryless jamming is the least effective type of jamming attacks.

**Single and Multi band jammers** as discussed, there are multiple channels available for Wi-Fi communications on ISM bands. A single-band jammer only jams a single channel at a given time. For instance, a low-cost jammer, is constrained by its hardware circuit (e.g., very high ADC sampling rate and broadband power amplifier) to attack a large number of channels simultaneously. On the other hand, a multi-band jammer can jam multiple channels at the same time [32].

Table [II] compares different types of JamRF and summarizes the earlier presented discussion.

![Fig. 2: The underlying system model.](image)
The signal model for a QAM waveform is expressed as

\[ r(t) = x_i(t) + n(t) + j(t); \quad i = 1, 2, \cdots, M; \quad 0 \leq t \leq T_s. \tag{1} \]

The transmitted symbol \( x_i(t) \) can be represented in terms of orthonormal basis functions as

\[ x_i(t) = \sum_{k=1}^{N} x_{ik}\psi_k(t); \quad i = 1, 2, \cdots, M; \quad k = 1, 2, \tag{2} \]

where \( \psi_k \) is the \( k \)th basis function, while \( x_{ik} \) can be given as

\[ x_{ik} = \int_{0}^{T} x_i(t)\psi_k(t)dt. \tag{3} \]

The signal model for a QAM waveform is expressed as

\[ x_i(t) = a_{m_{11}}(t)\cos(2\pi f_{c}t + \alpha) + a_{m_{21}}(t)\sin(2\pi f_{c}t + \alpha), \tag{4} \]

where \( \alpha \) is an arbitrary yet fixed phase and \( f_{c} \) denotes the center frequency of the transmit signal. Also, the signal components can be expressed as

\[ x_{11} = A_{m_{11}}, \quad x_{12} = A_{m_{21}}, \quad A = a\sqrt{\frac{T}{2}}, \tag{5} \]

where \( m = 1, 2, \cdots, M \), \( A_{m_{11}} \) and \( A_{m_{21}} \) are the information-bearing signal amplitudes of the quadrature carriers. Hence, the signal model can be rewritten as

\[ x_i(t) = A_{m_{11}}(t)\psi_1(t) + A_{m_{21}}(t)\psi_2(t), \tag{6} \]

where

\[ \psi_1(t) = \frac{\cos(2\pi f_{c}t + \alpha)}{\sqrt{Ts/2}}; \quad \psi_2(t) = \frac{\sin(2\pi f_{c}t + \alpha)}{\sqrt{Ts/2}}. \tag{7} \]

Moreover, assuming that \( x_i(t), j(t), \) and \( n(t) \) are statistically independent of each other, with respective power levels \( P_T, P_J, \) and \( \sigma^2, \) the signal to noise ratio (SNR) can thus be expressed as \( SNR = \frac{P_T}{\sigma^2}. \) Similarly, the jamming to noise ratio (JNR) can be expressed as \( JNR = \frac{P_J}{\sigma^2}. \) Hence, based on the free space path loss model, the jamming to signal ratio can be denoted as

\[ JSR = \frac{ERP_J G_J d_T^2}{ERP_T G_T d_J^2}. \tag{8} \]

where \( G_T \) and \( G_J \) are the transmitter and jammer antenna gains respectively, and \( ERP_T \) and \( ERP_J \) are the effective radiated powers of the transmitter and jammer respectively expressed in dB as:

\[ ERP_T = P_T + G_T - 32.44 - 20\log(f_T), \]
\[ ERP_J = P_J + G_J - 32.44 - 20\log(f_J), \tag{9} \]

where \( f_T \) and \( f_J \) are the frequencies of the transmitter and jammer respectively.

**IV. PERFORMANCE ANALYSIS**

Advanced communication technology stems from spread spectrum, error correction coding, and waveform modulation techniques [33]. Utilizing, time, frequency, and coding schemes, communication efficiency, design flexibility, and immunity to jamming attacks in communication systems are enhanced [34]. In this section, we will demonstrate the system performance experienced under different jamming attacks in AWGN channels.

The average error probability of \( M \)-QAM with signal model given in [4] in AWGN channel is given by [34]

\[ P_e = 4 \left( 1 - \frac{1}{\sqrt{M}} \right) Q \left( \sqrt{\frac{3\log_2 M E_b}{M-1 N_o}} \right) \times \left( 1 - \frac{1}{\sqrt{M}} \right) Q \left( \sqrt{\frac{3\log_2 M E_b}{M-1 N_o}} \right), \tag{10} \]

where \( E_b \) represents the average bit energy, and \( Q(\cdot) \) is defined as

\[ Q(z) = \frac{1}{\sqrt{2\pi}} \int_{z}^{\infty} e^{-t^2} dt. \tag{11} \]

For a gray-encoded WLAN IEEE 802.11n with MCS = 4, the average bit error rate in AWGN in the absence or jamming of interference is approximated as [35]

\[ P_{e,16QAM} = \frac{3}{8} \text{erfc} \left( \sqrt{\frac{2 E_b}{5 N_o}} \right). \tag{12} \]

where \( \text{erfc}(\cdot) \), is the complementary error function defined as

\[ \text{erfc}(z) = 1 - \frac{2}{\sqrt{\pi}} \int_{0}^{z} e^{-t^2} dt. \tag{13} \]

A jamming waveform can be generated either in the form of a tone signal, a Gaussian noise, or a digitally modulated signal to disrupt the communication between a transmitter and a receiver. Here, we carry out the performance analysis of the considered IEEE 802.11n system, and we assume that the receiver is unaware of the presence of the jamming signal.

**A. Gaussian Noise Jamming Waveform**

For noise jamming, the jamming carrier signal is modulated with a random noise waveform with the aim of disrupting the communication, by injecting noise into the system. The bandwidth of the signal can be as wide as the entire spectrum width used by the IEEE 802.11n system or much narrower, occupying only a single channel. The noise is generally assumed to be Gaussian for theoretical analysis, however, theoretical Gaussian noise has an infinite frequency extent. In situations where the filtering effects are important, colored Gaussian noise is the appropriate type to use [35].

Here, we assume that at time \( t, x_m(t) \) is transmitted, and a colored Gaussian noise jammer is attacking the IEEE 802.11n system. Hence, the received signal can be expressed as

\[ r(t) = \sum_{k=1}^{2} x_{mk}\psi_k(t) + n(t) + j(t), \tag{14} \]

such that

\[ r_k = x_{mk} + N_k + j_k; \quad k = 1, 2. \tag{15} \]
where

\[ N_k = \int_0^T n(t)\psi_k(t)dt; \quad j_k = \int_0^T j(t)\psi_k(t)dt; \quad k = 1, 2. \]  

(16)

This shows that \( r_k \) is a Gaussian random variable, with mean value equals to \( \mathbb{E} \{ r_k | x_m(t) \} = x_{mk}; \quad k = 1, 2. \) \( \text{(17)} \)

Therefore, (17) can be expanded as

\[ \mathbb{E} \{ (r_1 - x_{m1})(r_2 - x_{m2}) | x_m(t) \} = \mathbb{E} \{ (n_1 + j_1)(n_2 + j_2) \}. \]  

(18)

As indicated earlier, the noise and jamming signals are independent, and hence, \( r_1 \) and \( r_2 \) are independent random variables, with variance equals to

\[ \text{var} \{ r_k | x_m(t) \} = \frac{N_0}{2} + \int_0^T K_j(t - \tau)\psi_k(t)\psi_k(\tau)dtd\tau, \]  

(19)

where \( K_j(\cdot) \) is the jammer auto-correlation function. The joint probability density function (PDF) of \( r_1 \) and \( r_2 \) can be expressed as

\[ f_{r_1, r_2 | x_m(t)}(R_1, R_2) = \frac{1}{2\sqrt{\pi}\sigma^2}\exp\left(-\frac{(R_1 - x_{m1})^2}{2\sigma^2}\right) \times \exp\left(-\frac{(R_2 - x_{m2})^2}{2\sigma^2}\right). \]  

(20)

If the symbol \( x_m(t) \) is transmitted, the probability that the receiver decodes it correctly \( P_r(C | m) \) is given as \( 36 \)

\[ P_r(C | m) = \int_{L_{m1}^1}^{L_{m1}^2} \int_{L_{m2}^1}^{L_{m2}^2} f_{r_1, r_2 | x_m(t)}(R_1, R_2)dR_1dR_2, \]  

(22)

where the integration limits in (22) are dependent on the particular transmitted signal. Hence (22) becomes

\[ P_r(C | m) = \int_{h_{m1}}^{h_{m2}} \int_{g_{m1}}^{g_{m2}} \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{(z)^2}{2}\right) \int_{h_{ml}}^{h_{m2}} \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{(w)^2}{2}\right) dw dz, \]  

(23)

where

\[ h_{ml} = \frac{L_{m2}^1 - x_{m2}}{\sigma}; \quad h_{ml} = \frac{L_{m2}^2 - x_{m2}}{\sigma}; \]  

\[ g_{ml} = \frac{L_{m1}^1 - x_{m1}}{\sigma}; \quad g_{ml} = \frac{L_{m1}^2 - x_{m1}}{\sigma}; \]  

(24)

Following \( 36 \) to evaluate (23) based on (24), the average probability of error \( P_e \) of 16-QAM signal in an AWGN channel in the presence of Gaussian noise jamming waveform \( j(t) \) is given by:

\[ P_e = 1 - \frac{1}{4}\left\{ \text{erf}(d)^2 + 2\text{erf}(d)\left[ 1 - 2\text{erfc}(d) \right] \right\} + \left[ 1 - 2\text{erfc}(d) \right]^2, \]  

(25)

where \( d \) is a constant defined as

\[ d = \left[ \frac{\text{SNR}}{1 + \text{SNR} \cdot \text{JSR}} \right]^{\frac{1}{2}}. \]  

(26)

\subsection*{B. QPSK modulated Jamming Waveform}

It was shown in \( 37 \) that QPSK modulated waveform is the optimal digitally modulated waveform for jamming an M-QAM system. From a practical standpoint, digitally modulated signal is a more realistic choice to perform denial of service attacks \( 38 \). Here, a perfect channel estimation is assumed such that the jamming signal perfectly synchronized with the WLAN IEEE 802.11n signal in both time and phase. The signal model representation of an M-PSK modulated jamming signal is denoted as

\[ j(t) = \sqrt{\frac{P_j}{2}} \cos \left( \frac{2\pi}{M} (m - 1) \right) \psi_1(t) + \sqrt{\frac{P_j}{2}} \sin \left( \frac{2\pi}{M} (m - 1) \right) \psi_2(t), \]  

(27)

It was shown in \( 37 \) that, in the presence of any jamming signal \( j \), the average probability of error \( P_e \) of an M-QAM signal in an AWGN channel is given by

\[ P_e (j, \text{SNR}, \text{JNR}) \approx \frac{1}{2} \left( 1 - \frac{1}{\sqrt{\text{JNR}}} \right) \left[ \text{erfc} \left( \sqrt{\text{SNR} \cdot d_{\text{min}}} + \sqrt{\text{JNR} \cdot d_{\text{min}}} \right) \right] \]  

(28)

where \( j = \mathcal{R} \cdot \{ \mathcal{N}_j \} \) or \( j = \mathcal{I} \cdot \{ \mathcal{N}_j \} \), and \( d_{\text{min}} \) denotes the minimum distance of the M-QAM modulation scheme.

The jammer intends to maximize (28) by transmitting a sequence of symbols \( j \) which are chosen based on the operating SNR and JNR. Let the signal level be \( a = |j| \) with energy denoted as \( E(a^2) \leq 1/2 \) and PDF \( f_A \). In the following, we aim to find the optimum distribution to model \( a \) at the jammer, in order to maximize the probability of error. The optimization problem can hence be formulated as

\[ \max_{f_A} \int_a P_a(a, \text{SNR}, \text{JNR}) f_A da; \quad \text{s.t.} \quad E(a^2) \leq \frac{1}{2} \]  

\[ \equiv \max_A \mathbb{E} \{ P_e (a, \text{SNR}, \text{JNR}) \}; \quad \text{s.t.} \quad E(a^2) \leq \frac{1}{2} \]  

(29)

Considering that the jamming signal has at most two signal levels \( a_1 \) and \( a_2 \) \( 37 \), the pdf of the jamming signal along any signalling dimension can be expressed as

\[ f_A(a) = \lambda \delta (a - a_1) + (1 - \lambda) \delta (a - a_2); \quad \lambda \in [0, 1] \]  

\[ \lambda a_1^2 + (1 - \lambda) a_2^2 \leq \frac{1}{2} \]  

(30)

where \( \lambda \) and \((1 - \lambda)\) denote the probabilities that the jammer sends signals with levels \( a_1 \) and \( a_2 \), respectively and \( \delta (a) \) is the Dirac-delta function. Hence, based on (30), the overall \( P_e \) along any signalling dimension can be generalized to

\[ P_e (\lambda, a_1, a_2, \text{SNR}, \text{JNR}) \approx \frac{1}{2} \left( 1 - \frac{1}{\sqrt{\text{JNR}}} \right) \left[ \lambda \Gamma_1 + (1 - \lambda) \Gamma_2 \right], \]  

(31)

where \( \Gamma_1 \) and \( \Gamma_2 \) are expressed as

\[ \Gamma_1 = \text{erfc} \left( \sqrt{\text{SNR} \cdot d_{\text{min}}} + \sqrt{\text{JNR} \cdot a_1} \right) \]  

(32)
$$\Gamma_2 = \text{erfc}\left(\sqrt{\text{SNR}}\sqrt{d_{\text{min}}^2 + \text{JNR}\alpha_2}\right) + \text{erfc}\left(\sqrt{\text{SNR}}\sqrt{d_{\text{min}}^2 - \text{JNR}\alpha_2}\right).$$

For a QPSK jamming signal when the IEEE 802.11n signal uses $M$-QAM, it was shown that

$$\sqrt{\text{SNR}}\frac{d_{\text{min}}^2}{2} < \sqrt{\text{JNR}} \cdot \tanh\left[2\sqrt{\text{SNR}}\frac{d_{\text{min}}^2}{2} \text{ JNR}\right].$$

From (34), it can be noted that when $\text{SNR}\frac{d_{\text{min}}^2}{2} > 1$, $\tanh\left[2\sqrt{\text{SNR}}\frac{d_{\text{min}}^2}{2} \text{ JNR}\right] \approx 1$. Thus, it can be deduced that $\text{SNR}\frac{d_{\text{min}}^2}{2} \ll \text{JNR}$. Based on this, it was shown in [21] that for the case of using QPSK as a jamming signal with an $M$-QAM signal, (31) can be simplified as

$$P_e = \frac{1}{2} \left(1 - \frac{1}{\sqrt{M}}\right) \left[\text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\text{min}}^2}{2} + \sqrt{\text{p} \text{ JNR}}\right) + \text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\text{min}}^2}{2} - \sqrt{\text{JNR}}\right)\right].$$

Therefore, for WLAN IEEE 802.11n signal employing MCS = 4, $d_{\text{min}} = 2$, and JNR = $2 \ast \text{JSR} \ast \text{SNR}$, the average probability of error $P_e$ in the presence of QPSK modulated jamming waveform $j(t)$ is obtained as

$$P_e = \frac{3}{8} \left[\text{erfc}\left(\sqrt{\text{SNR}}(1 + \sqrt{\text{JSR}})\right) + \text{erfc}\left(\sqrt{\text{SNR}}(1 - \sqrt{\text{JSR}})\right)\right].$$

A. Numerical Results for AWGN Channel Scenario

In Sec. [V], the BER performance of the underlying system model under Gaussian noise and QPSK jamming waveforms were obtained as in (25) and (36) respectively. Fig. 3 demonstrates the impact of Gaussian noise jamming signal on the BER performance of the IEEE 802.11n system under study. It is observed that at JSR = $-100$ dB, the jammer has a negligible effect on the system performance. However, as the JSR increases to 0 dB, the performance is severely degraded where a BER $> 0.1$ is experienced over all SNR values.

Similarly, Fig. 4 shows that the QPSK modulated jamming waveform has a destructive impact on the considered system. From the figure, it can be noticed that for JSR $> 0$ dB, a BER $> 0.1$ is achieved. It can be further observed from Figs. 3 and 4 that, the impact of QPSK jamming is less than that of Gaussian noise jamming. Also, it can be observed that for both Gaussian noise and QPSK modulated jamming signals, the system performance is significantly degraded for all SNR values when JSR $> 0$ dB. This indicates that both two waveforms are able to completely corrupt all transmitted packets when JSR $\geq 0$ dB, regardless of the SNR value.

B. Simulation Results for Realistic Channel Scenario

In this subsection, we investigate and compare the performance of the considered jamming waveforms under a realistic channel model, and compare their performance with a baseline single-tone signal. The signal model representation of the single-tone jamming waveform is expressed as:

$$j(t) = \sqrt{2P_j\sin(2\pi f_j t + \theta_j)},$$

where $f_j$ is the jamming tone frequency, and $\theta_j$ is the random jammer phase. All the simulations were performed by employing the wlanHTConfig and wlanTGnChannel system objects of the MATLAB WLAN toolbox. Unless otherwise stated, adopted simulation parameters are presented in Table III.

Fig. 5 shows that the Gaussian noise jamming waveform has a destructive impact on the considered system. We find that for JSR $> 0$ dB, the BER $> 0.1$ is achieved. This agree with the analysis results obtained for the AWGN scenario. However, it
TABLE III: Simulation Parameters

| Parameter          | Value          | Parameter          | Value          |
|--------------------|----------------|--------------------|----------------|
| Channel Bandwidth  | 20 MHz         | Sample rate        | 20 MHz         |
| Number of Tx antennas | 1             | $d_{TR}$           | 10 m           |
| Number of Rx antennas | 1             | $d_{JR}$           | 5 m            |
| Number of J antennas | 1             | Carrier freq       | 2412 MHz       |
| PSDU length        | 1024 Bytes     | Delay profile      | Model-A        |
| Spatial mapping scheme | Direct        | Power line freq    | 60 Hz          |
| MCS                | 4              | Large-sale fading  | None           |
| Guard interval duration | Long          | Fluorescent effect | 1              |
| Channel coding     | BCC            | Channel filtering  | 1              |

should be noted that even at lower $-10 < JSR < 0$ dB, BER $> 0.1$ is still experienced due to the fact that, the simulation tries to model a realistic communication channel and not an AWGN channel.

Similarly, Fig. 6 demonstrates that QPSK modulated waveform jammer also cause degrading effect on the victim system which is also in agreement with the analysis results. This indicates that both two waveforms are able to completely corrupt all transmitted packets when JSR $\geq 0$dB. Overall, the simulation results further demonstrate that the Gaussian noise is a more effective jamming waveform to attack IEEE 802.11n victim system with MCS = 4 compared to digitally modulated waveforms.

![Fig. 5: The BER of IEEE 802.11n victim system in the presence Gaussian noise waveform with varying JSR.](image)

![Fig. 6: The BER of IEEE 802.11n victim system in the presence QPSK modulated waveform with varying JSR.](image)

![Fig. 7: The BER of IEEE 802.11n victim system in the presence of jamming signals.](image)

VI. EXPERIMENTAL RESULTS

We implement JamRF, a jamming framework based on GNU Radio interfaced with HackRF SDR, and make this available to the community [3] as a platform for further research. The experimental setup depicted in Fig. 8 is employed to measure the impact of RF jamming on the victim IEEE 802.11n system. Focusing on distributed ad-hoc networks, we consider the Better Approach to Mobile Ad Hoc Networking Advanced (BATMAN-Adv) [39] as a routing protocol instead of Hybrid Wireless Mesh Protocol (HWMP) of IEEE 802.11s standard. The specific implemented jammers are summarized in Table IV

**Constant jammer.** JamRF implements a constant signal that jams a 20 MHz band centered at a center frequency $f_c$.

**Sweeping jammer.** Since the HackRF has a maximum bandwidth of 20 MHz, it cannot be used to emit jamming signals that can disrupt the whole frequency spectrum of Wi-Fi. Therefore, we implement a sweep signal that sweeps 20 MHz band centered at a center frequency $f_c$. This allows the blockage of all transmissions within 20 MHz of the center frequency. The center frequency is shifted every few seconds to sweep over the whole frequency spectrum. For instance, in a 2.4 GHz

[https://github.com/tiiuae/sdr-jammer/HackRF](https://github.com/tiiuae/sdr-jammer/HackRF)
Wi-Fi with 14 channels, the jammer sequentially hops from one channel to the next sequentially.

**Random channel hopping jammer.** This is implemented similar to the sweeping jammer. However, the center frequency is randomly shifted every few seconds over the whole Wi-Fi frequency spectrum. For instance, in a 2.4 GHz Wi-Fi with 14 channels, the jammer continuously hops from one channel to the next in a random manner.

**Reactive jammer.** Frequency sweeping and random channel hopping jamming strategies can also be employed to jam a channel reactively. In the case of reactive jamming, a sensing mechanism is required to detect channel activity. JamRF, implements an energy detection technique to detect channel activity. During the sensing, the HackRF is employed as a receiver and is interfaced with GNU radio software to interpret the incoming IQ samples. The power of the received IQ samples can be expressed as

$$P = \frac{1}{2N} \sum_{i=0}^{N} |x(i)|^2$$  \hspace{1cm} (38)

where \(N\) is the number of obtained IQ samples, and \(x(i)\) are the received IQ samples. Channel is active when \(P\) is greater than or equal to a fixed threshold of 0.002 and channel is inactive when \(P\) is less than the threshold.

Moreover, we enable the reactive jammer to remember the state (active or idle) of the current channel. If the current channel is active, the jammer senses the current channel again after the elapse of the jamming duration before moving to the next channel.

**Periodic jammer.** Furthermore, we aim to save energy during jamming duration by continuously switching between two states: sleep phase and jamming phase. In JamRF, a predetermined duty cycle is set at the onset to determine the duration of each of the two phases.

### A. Experimental Setup

The project requires both hardware and software tools. These are presented in Table V and VI respectively. Unless otherwise stated, are summarized in Table VII.

**TABLE IV: Implemented jammers and features in JamRF.**

| Jammer                  | Proactive | Reactive | Periodic | Multi-band | Memory |
|-------------------------|-----------|----------|----------|------------|--------|
| Constant                | ✓         |          | ✓        |            |        |
| Sweeping                | ✓         | ✓        | ✓        | ✓          | ✓      |
| Hopping                 | ✓         | ✓        | ✓        | ✓          | ✓      |

**TABLE V: Experimental testbed hardware specifications**

| Component                          | Version/model                                      |
|------------------------------------|---------------------------------------------------|
| Jammer radio host                  | Lenovo ThinkPad X1 Extreme Gen 3                   |
| Host device                        | Raspberry Pi 4                                     |
| Jammer radio                       | HackRF One                                         |
| Sender and receiver interface      | wab-r508n Dongle                                   |
| SME Cables                         | Tonearm series 300                                 |
| Spectrum Analyzer                  | Tektronix RSA306B                                  |
| Component                          | Version/model                                      |
| Host device                        | Raspberry Pi 4                                     |
| Jammer radio                       | HackRF One                                         |
| Spectrum Analyzer                  | Tektronix RSA306B                                  |

Table VII presents the obtained measurement for the CPU consumption for jamming and sensing on the Raspberry Pi 4 (Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz, 8GB LPDDR4-3200 SDRAM), and a laptop (Intel i9-10885H CPU @ 2.40GHz, 32GB SDRAM).

It can be seen from Table VII that single-tone waveform jammers consumed the least CPU resources compared with the Gaussian noise and QPSK modulated waveforms. Among the two analyzed waveforms, the Gaussian noise consumes fewer resources in the order of 10% compared with the QPSK waveform. It can also be observed that the sensing operation consumes approximately 6 times fewer resources than jamming.
If the transmission frequency is known, a simple constant jammer can be employed to determine the optimal jamming waveform. The packet receive ratio (PRR) with the varying jammer transmit power is measured as shown in Fig. [10]. It is observed that to reach a PRR < 0.1 we need a jamming transmit power of 6dBm, 4dBm and 2dBm for the single-tone, QPSK modulated and Gaussian noise waveforms respectively. This shows that the Gaussian noise waveform requires less power to achieve significant performance degradation on the IEEE 802.11n system compared to both single-tone and QPSK modulated waveforms. This confirms both the analysis and simulation results presented earlier in Secs. III and V.

However, when the transmission frequency is unknown, a constant jammer cannot be employed. Therefore, other jamming strategies are employed that can jam multiple bands. This promotes the need to determine how much of the band these jamming strategies should employ to optimally jam the entire target spectrum. To that extent, a frequency sweeping jammer is deployed with varying distance between adjacent channels and the PRR in order to quantify the optimal distance between adjacent channels. We set the jamming duration per channel to $t_{jam} = 5s$ and vary the distance between adjacent channels. For instance, using a distance between adjacent channels of 5MHz, it will take $5 \times 14 = 70s$ to sweep the whole 2.4GHz spectrum. However for 20MHz distance between channels, it will take about $5 \times 4 = 20s$ to sweep over the whole spectrum.

In Fig. [11] it is observed that PRR decreases with increasing distance between adjacent channels.

The optimal distance between adjacent channels for the HackRF with 20MHz transmit bandwidth is observed to be 20 MHz. Also, for this value, Gaussian noise waveform exhibits the best performance by making the victim system to only achieve a PRR of about 45%.

In Fig. [12] the performance of the proactive jammer is compared with that of reactive jammer when the jamming duration $t_{jam}$ is varied with Gaussian noise jamming waveform. It is observed that both frequency sweeping and random channel hopping proactive jammers have relatively similar performance. Furthermore, at lower jamming duration, proactive jammers outperform the sweeping reactive jammer. This is due to the additional time the reactive jammer takes to sense the channels, which is aligned with the timing constraints discussed earlier. For instance, at $t_{jam} = 5s$, frequency sweeping reactive jammer caused the PRR of the IEEE 802.11n system to be $\approx 70\%$, whereas the corresponding proactive jammer resulted in PRR $\approx 50\%$. However, at higher jamming durations, both sweeping and random channel hopping reactive jammers outperform the corresponding proactive jammers. For $t_{jam} = 20s$, frequency sweeping and random channel hopping reactive jammers resulted in a PRR of about 38% and 32%, respectively. Whereas the corresponding proactive jammers resulted in a PRR of about 51% and 56%, respectively.

The performance of a reactive jammer with and without memory is demonstrated in Fig. [13]. It is observed that, at all jamming durations, the stateful reactive jammer outperforms the memoryless reactive jammer. At $t_{jam} = 20s$, frequency sweeping and channel hopping memoryless reactive jammers resulted in PRR of about 39% and 37% respectively. Whereas the corresponding frequency sweeping and channel hopping stateful reactive jammers resulted in PRR of about 18% and 9% respectively. Overall, the best implemented jammer is the random channel hopping stateful reactive jammer that resulted in a very low PRR of about 9%.

### VII. Conclusions

In this paper, we present the error rate performance analysis of WLAN IEEE 802.11n wireless communication systems in the presence of jammer employing different types of jamming waveform. Simulations and practical experiments were carried out to demonstrate the impact of jamming on the victim system. Furthermore, practical experimentation was performed on IEEE 802.11n links in an isolation chamber, using a HackRF SDR as the jamming device. To this end, we have developed JamRF, a jamming ‘toolbox’ with multiple implemented jammer types, and make this available to the research community.
TABLE X: CPU consumption for jamming and sensing

| Operation   | Waveform          | Laptop (%) | Pi 4 (%) |
|-------------|-------------------|------------|----------|
| Jamming     | Gaussian noise    | 104.7      | 121.2    |
|             | Single-tone       | 56         | 103.3    |
|             | QPSK modulated    | 115.9      | 149.3    |
| Sensing     | -                 | 13.6       | 22.4     |

Fig. 10: Impact of jamming waveforms on the underlying IEEE 802.11n system.

It was observed that the obtained analytical and simulation results, as well as the experimental results, demonstrated system performance degradation under jamming attacks. The simulation results agree with the analytical results in terms of determining the effective jamming waveform. Furthermore, although the simulation results depict a 100% PER when QPSK modulated and Gaussian noise waveforms are employed, the experimental results demonstrate a packet loss ratio \((1 – \text{PRR})\) of about 80% for both QPSK modulated and Gaussian noise waveforms under constant jamming attack. The 20% difference between simulation and experimental results is due to the \(t_{\text{boot}} = 450\text{ms}\) HackRF time constraint in a proactive jammer. This indicates that, when the traffic flow and jamming operations are executed at the same time, a certain amount of traffic will pass through before the jamming kicks in after 450ms. This demonstrates that the major drawback of using low-cost SDRs (such as the HackRF) to implement these jamming techniques is the hardware time constraints. To mitigate this, we added channel awareness feature to further enhance the performance of the reactive jammer by about 10%.

We additionally show that the effective jamming waveform to attack IEEE 802.11n system is Gaussian noise. The Gaussian noise is shown to consume fewer CPU resources compared to QPSK and at the same time achieves 100% PER. Furthermore, in order to jam the full spectrum, a stateful random channel hopping reactive jammer outperforms other types of jammers. Overall, the obtained results indicate that, despite the flexibility and affordability of SDRs, they are still wanting when compared to high grade military jammers. The limitations of these SDRs can be exploited in designing relatively easy anti-jamming strategies to mitigate the effects of these type of jammers.

Accordingly, as a future work, we will implement anti-jamming strategies to mitigate the effects of the implemented jammers in an IEEE 802.11n victim system. We will exploit the limitations posed by the hardware time constraints of the SDRs in order to design an efficient anti-jamming strategy.

REFERENCES

[1] H. Pirayesh and H. Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey,” arXiv preprint arXiv:2101.00292, pp. 1–39, 2021. [Online]. Available: http://arxiv.org/abs/2101.00292

[2] M. Andreoni Lopez, M. Baddeley, W. T. Lunardi, A. Pandey, and J.-P. Giacalone, “Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities,” in Proc. 17th Int. Conf. Distrib. Comput. Sens. Syst. (DCOSS), 2021, pp. 319–326.

[3] Ettus Research LLC, “Universal software radio peripheral (USRP),” ettus.com. [Online]. Available: http://www.ettus.com (accessed Jun. 20, 2022).

[4] M. Ossmann, “HackRF One,” greatscottgadgets.com. [Online]. Available: https://greatscottgadgets.com/hackrf/ (accessed Jun. 20, 2022).

[5] Nuand, “BladeRF 2.0,” nuand.com. [Online]. Available: https://www.nuand.com/bladerf-2-0-micro (accessed Jun. 20, 2022).
Fig. 13: Jamming Performance of stateful reactive jammers versus jamming duration.

[6] RTL-SDR, “Blog R820T RTL2832U,” rtl-sdr.com. https://www.rtl-sdr.com/ (accessed Jun. 20, 2022).

[7] Airspy, “Airspy R2,” airspy.com. https://airspy.com/ (accessed Jun. 20, 2022).

[8] Perfect Jammer, “EO-08-007 Jammer,” perfectjammer.com. https://perfectjammer.com/wireless-wifi-blueooth-jammers.html (accessed Jun. 20, 2022).

[9] ———, “TX-100 Jammer,” perfectjammer.com. https://www.perfectjammer.com/5g-cellphone-signal-jammers.html (accessed Jun. 20, 2022).

[10] ———, “M16-5G M16-A M16-B Jammer,” perfectjammer.com. https://www.perfectjammer.com/desktop-16-antennas-cellphone-5g-jammers.html (accessed Jun. 20, 2022).

[11] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, “Ieee 802.11 b/g wlan tolerance to jamming,” in Proc. IEEE Military Commun. Conf. (MILCOM), vol. 3. IEEE, 2004, pp. 1364–1370.

[12] I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, “Fiji: Fighting implicit jamming in 802.11 wlans,” in Proc. Int. Conf. Priv. Secur. Mob. Syst. Springer, 2009, pp. 21–40.

[13] S. Prasad and D. J. Thuente, “Jamming attacks in 802.11 g—a cognitive radio based approach,” in Proc. IEEE Military Commun. Conf. (MILCOM). IEEE, 2011, pp. 1219–1224.

[14] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, “Mimo-based jamming resilient communication in wireless networks,” in Proc. IEEE Conf. Comput. Commun. (INFOCOM). IEEE, 2014, pp. 2697–2706.

[15] ———, “Jamming resilient communication using mimo interference cancellation,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 7, pp. 1486–1499, 2016.

[16] S. Gvozdenovic, J. K. Becker, J. Mikulskis, and D. Starobinski, “Truncate after preamble: Phy-based starvation attacks on iot networks,” in Proc. 13th ACM Conf. Secur. Priv. Wirel. Mob. Netw. ACM, 2020, pp. 89–98.

[17] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, “Performance of iee 802.11 under jamming,” Mob. Netw. Appl., vol. 18, no. 5, pp. 678–696, 2013.

[18] S. Bandaru, “Investigating the effect of jamming attacks on wireless lans,” Int. J. Comput. Appl. Technol., vol. 99, no. 14, pp. 5–9, 2014.

[19] Y. Cai, K. Pelechrinis, X. Wang, P. Krishnamurthy, and Y. Mo, “Joint reactive jammer detection and localization in an enterprise wifi network,” Comput. Netw., vol. 57, no. 18, pp. 3799–3811, 2013.

[20] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, “Short paper: Reactive jamming in wireless networks: How realistic is the threat?” in Proc. 4th ACM Conf. Wirel. Netw. Secur. (WiSec), 2011, pp. 47–52.

[21] E. M. Shaheen, “Performance of mimo ieee802. 11n wlan in presence of qpsk jammer with inphase/quadrature origin offsets,” Wirel. Pers. Commun., vol. 113, no. 1, pp. 555–574, 2020.

[22] E. M. Shaheen and M. El-Tanany, “The impact of narrowband interference on the performance of UWB systems in the IEEE802. 15.3 a channel models,” in Proc. Can. Conf. Electr. Comput. Eng. (CCECE). IEEE, 2010, pp. 1–6.

[23] M. K. Bek, E. M. Shaheen, and S. A. Elgamel, “Analysis of the global position system acquisition process in the presence of interference,” IET Radar Sonar Navig., vol. 10, no. 5, pp. 850–861, 2016.

[24] Y. Fan, X. Liao, and A. V. Vasilakos, “Physical layer security based on interference alignment in k-user MIMO wiretap channels,” IEEE Access, vol. 5, pp. 5747–5759, 2017.

[25] S. Jia, J. Zhang, H. Zhao, and R. Zhang, “Relay selection for improved security in cognitive relay networks with jamming,” IEEE Commun. Lett., vol. 6, no. 5, pp. 662–665, 2017.

[26] H. Wang, Y.-D. Yao, R. Wang, and L. Shen, “Coordinated jamming and communications in an MC-CDMA system,” IEEE Trans. Aerosp. Electron. Syst., vol. 51, no. 4, pp. 3151–3160, 2015.

[27] V. Kristem, A. F. Molisch, and L. Christen, “Jammer sensing and performance analysis of MC-CDMA ultrawideband systems in the presence of a wideband jammer,” IEEE Trans. Wireless Commun., vol. 17, no. 6, pp. 3807–3821, 2018.

[28] J. Gao, S. A. Vorobyov, H. Jiang, and H. V. Poor, “Worst-case jamming on MIMO gaussian channels,” IEEE Trans. Signal Process., vol. 63, no. 21, pp. 5821–5836, 2015.

[29] M. Vanhoef and F. Piessens, “Advanced Wi-Fi attacks using commodity hardware,” in Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC), 2014, pp. 256–265.

[30] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014.

[31] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, “Phy-layer resiliency in ofdm communications: A tutorial,” IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 292–314, 2014.

[32] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy,
“Denial of service attacks in wireless networks: The case of jammers,” IEEE Commun. Surveys Tuts., vol. 13, no. 2, pp. 245–257, 2010.

[33] M. Viswanathan, Wireless Communication Systems in Matlab, 2nd ed. Gaussian Waves, 2014. [Online]. Available: https://www.gaussianwaves.com/2014/07/power-delay-profile/

[34] J. G. Proakis and M. Salehi, Digital Communications, 5th ed. The McGraw-Hill Companies, 2008.

[35] R. Poisel, Modern Communications Jamming: Principles and Techniques. Artech House, Inc., 2011. [Online]. Available: http://books.google.com/books?id=cty3iV1vkNAC&amp;pgis=1

[36] D. C. Bukofzer, “Performance of receivers in digital radio applications operating in the presence of noise and jamming,” in Proc. IEEE Military Commun. Conf. (MILCOM), vol. 3. IEEE, 1986, pp. 39–51.

[37] S. Amuru and R. M. Buehrer, “Optimal jamming against digital modulation,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2212–2224, 2015.

[38] ——, “Optimal jamming strategies in digital communications - Impact of modulation,” Proc. IEEE Glob. Commun. Conf. (GLOBECOM), pp. 1619–1624, 2014.

[39] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, “Better approach to mobile ad-hoc networking (batman),” IETF draft, pp. 1–24, 01 2008.