IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 November 2022, accepted 9 December 2022, date of publication 20 December 2022,
date of current version 28 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3230895

RESEARCH ARTICLE

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

ABUBAKAR S. ALI[1], (Graduate Student Member, IEEE), MICHAEL BADDELEY[2], (Member, IEEE), LINA BARIAH[1,2], (Senior Member, IEEE), MARTIN ANDREONI LOPEZ[2], (Member, IEEE), WILLIAN TESSARO LUNARDI[2], (Member, IEEE), JEAN-PIERRE GIACALONE[2], (Member, IEEE), AND SAMI MUHAIDAT[1], (Senior Member, IEEE)

[1]KU Center for Cyber-Physical Systems, Khalifa University, Abu Dhabi, United Arab Emirates
[2]Technology Innovation Institute (TII), Abu Dhabi, United Arab Emirates

Corresponding author: Abubakar S. Ali (asali@ieee.org)

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 in an additive white Gaussian noise channel to obtain a lower bound performance. Then, we validated the finding obtained by the analysis via realistic end-to-end 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 further validate the analysis and simulation findings. The obtained results demonstrated that the Gaussian noise waveform outperformed the digitally modulated waveforms. Furthermore, in terms of jamming attack strategies, experimental results showed that to jam the whole 2.4GHz spectrum, a stateful-reactive jammer employing a 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 signal quality and hence prevent the recipient from receiving the required transmitted information. These security threats have been deemed 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

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaofan He.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

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. Furthermore, both rtl-SDR and Airspy operate only as receivers. Military and commercial jamming devices [8], [9], [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 makes it imperative for wireless network security researchers to study these jamming strategies and implement them in order to mitigate their effects. To the best of the authors' knowledge, there is no prior work that provides both extensive analysis, a 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 WLAN IEEE 802.11n communication networks in the presence of jamming. Furthermore, we provide an implementation of different types of jammers on a HackRF.[1] 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 that can jam both 2.4GHz and 5GHz bands; 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 the performance analysis of the victim system under jamming attack. Simulation results are presented and discussed in Sec. V. Sec. VI presents the experiments and the discussions of the obtained results. Finally, the paper is concluded in Sec. VII.

II. BACKGROUND AND RELATED WORKS

Jamming techniques have been covered in the earlier literature, where the physical layer jammer is modeled as single or multi-tone [22], [23], [24], [25], [26]. Alternatively, jamming attacks are sometimes modeled as partial-band or broadband additive white Gaussian noise (AWGN) [24].

[1] Available at https://github.com/tiiuae/jamrf

Jia et al. [25] introduced a cognitive radio network where a secondary transmitter communicates with a secondary receiver via multiple cognitive relays. One of the cognitive relays is employed for transmission, while the remaining relays cooperate in jamming multiple eavesdroppers. A coordinated jamming and communications technique, based on a linear minimum mean square error multi-user detection–based algorithm, was proposed in [26] with the aim to achieve simultaneous friendly jamming and reliable communication. In [27], the performance analysis of ultra-wideband systems employing a multi-carrier code division multiple access scheme in the presence of wideband jammer was presented. Optimal jamming over an AWGN channel was investigated in [28], where the optimal jamming signal for various digital amplitude-phase-modulated constellations was derived. It was assumed that the modulation of the legitimate receiver was known by the jammer. Chirp modulated waveforms fall under the category of narrow-band interference and have been used as in-car jammers. A survey of in-car jammers was conducted in [29], with a few having a continuous wave signal and the majority having a chirp signal of varying complexity. The authors proposed mathematical models of the surveyed in-car jammers as well as a novel mitigation scheme.

Owing to the advances in SDR, one can easily program a small, low-cost USB dongle device to jam a 20 MHz bandwidth below 6 GHz with up to 100 mW transmission power [30]. Such a USB dongle is sufficient to disrupt Wi-Fi services in home or office scenarios. Other off-the-shelf SDR devices such as the HackRF [4], USRP [3] and BladeRF [5] are even more powerful and flexible. These SDRs are presented in Table 1 and can be used to implement different types of generic jammers.

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 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 [31]. These types of jammers are 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

TABLE 1. Comparisons of common Wide-band Commercial SDRs.

SDR	Tune Low (MHz)	Tune High (MHz)	RX Bandwidth (MHz)	ADC Resolution (Bits)	Transmission	Price ($USD)
RTL-SDR R820T	24	1766	3.2/2.56 Stable	8	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

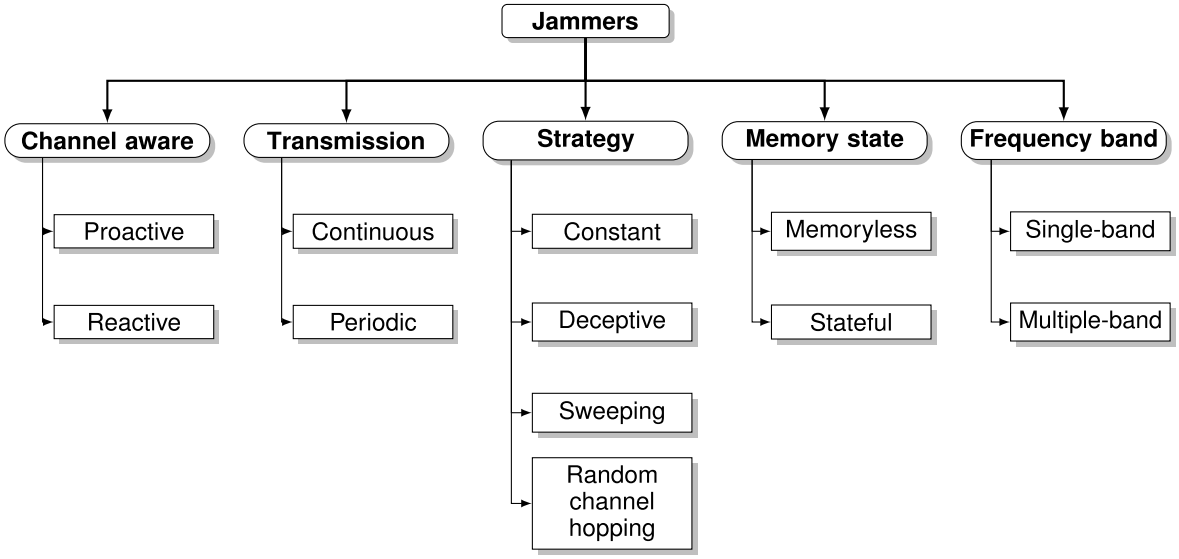

FIGURE 1. Classification of jammers in wireless networks.

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] and [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 the channel bandwidth occupied by legitimate users [31], [32], [33]. 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 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. The authors of [34] devised a revolutionary deception jamming technique that conceals the real target and presents the adversary radar with a number of phony targets at various arbitrary ranges in the same general direction. The technique was intended to counteract the hazards and efficacy of the hostile radar, ensuring the safe entry of the actual aircraft inside enemy territory.

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 [31], [33]. In [18], the authors analyzed Wi-Fi networks' performance under frequency-sweeping jamming attacks on 2.4 GHz, where there are only three 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.

TABLE 2. 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 IEEE802.11g	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	LAN IEEE802.11	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
JamRF	HackRF One	WLAN IEEE 802.11a/b/g/n	Constant/ Sweeping/ Hopping	Random bits	Proactive/ Reactive	single-band/ multi-band	Memoryless/ Stateful	Continuous/ Periodic

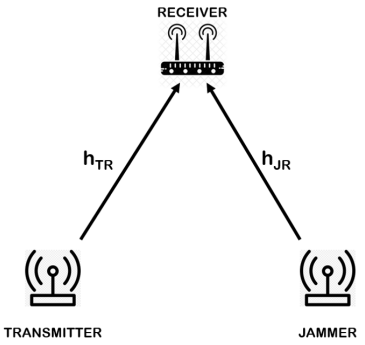

FIGURE 2. Underlying system model.

Periodic jammer refers to the type of jammer that emits signals for random periods while sleeping the rest of the time. This type of jamming attack 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 [31]. 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 attack.

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 [33].

Table 2 compares different types of JamRF and summarizes the earlier presented discussion.

III. SYSTEM MODEL

In order to investigate the BER performance of a wireless system in the presence of a jamming attack and while considering the IEEE 802.11n standard, in this section we introduce the considered jamming scenario. As illustrated in Fig. 2, the considered system model comprises a single transmitter communicating with a legitimate receiver and a jammer. Without loss of generality, we employ a modulation and coding scheme (MCS) of 4, which implies a single-antenna Wi-Fi transmitter emitting a 16-QAM digitally modulated signal. The receiver is equipped with a single antenna to detect the digitally modulated transmitted signal.

The baseband equivalent waveform of the transmitted signal is represented as $x(t) = \sum_{m=-\infty}^{\infty} \sqrt{P_T} x_m g(t - mT)$, where m is the modulation index, P_T is the average transmit power, $g(t)$ is the real valued pulse shape and T is the symbol interval.

At the same time, an SDR-based jammer aims to corrupt the received signal at the receiver. The baseband equivalence of the jamming signal is represented as $j(t) = \sum_{m=-\infty}^{\infty} \sqrt{P_J} j_m g(t - mT)$, where P_J is the average jammer transmit power while j_m denotes the transmitted jamming symbols. It is assumed that at time t a symbol $x_i(t)$; $i = 1, 2, \cdots, M$ where M is the modulation order, is transmitted over the interval $0 \leq t \leq T$. The noise is modeled as AWGN, with power spectral density (PSD) of $N_0/2$. Thus,

the received signal $r(t)$ at the receiver can be expressed as

$$r(t) = x_i(t) + n(t) + j(t);\ i = 1, 2, \cdots, M;\ 0 \le t \le T_s. \tag{1}$$

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

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

where ψ_k is the kth 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

$$x_i(t) = a_{m1i}(t)\cos(2\pi f_c t + \alpha) + a_{m2i}(t)\sin(2\pi f_c t + \alpha), \tag{4}$$

where α 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

$$\begin{aligned} x_{i1} &= A_{m1i}, \\ x_{i2} &= A_{m2i}, \\ A &= a\sqrt{\frac{T}{2}}, \end{aligned} \tag{5}$$

where $m = 1, 2, \cdots, M$, A_{m1i} and A_{m2i} are the information-bearing signal amplitudes of the quadrature carriers. Hence, the signal model can be rewritten as

$$x_i(t) = A_{m1i}(t)\psi_1(t) + A_{m2i}(t)\psi_2(t), \tag{6}$$

where

$$\psi_1(t) = \frac{\cos(2\pi f_c t + \alpha)}{\sqrt{T_s/2}};\ \psi_2(t) = \frac{\sin(2\pi f_c t + \alpha)}{\sqrt{T_s/2}}. \tag{7}$$

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

$$\text{JSR} = \frac{\text{ERP}_J G_J d_T^2}{\text{ERP}_T G_T d_J^2}, \tag{8}$$

where G_J and G_T are the transmitter and jammer antenna gains respectively, d_T and d_J are the distances between the transmitter to receiver, and jammer to receiver respectively, and ERP_T and ERP_J are the effective radiated powers of the transmitter and jammer respectively, expressed in dB as:

$$\begin{aligned} \text{ERP}_T &= P_T + G_T - 32.44 - 20\log(f_T), \\ \text{ERP}_J &= P_J + G_J - 32.44 - 20\log(f_J), \end{aligned} \tag{9}$$

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 [35]. Utilizing, time, frequency, and coding schemes, communication efficiency, design flexibility, and immunity to jamming attacks in communication systems are enhanced [36]. In this section, we will demonstrate the system performance 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 [36]

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

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 of jamming or interference is approximated as [37]

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

where erfc(·), 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 assume that the receiver is unaware of the presence of the jamming signal.

A. GAUSSIAN NOISE JAMMING WAVEFORM

For noise jamming, the jamming signal is modulated with a random noise waveform with the aim of disrupting communication by injecting Gaussian 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 [37].

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 the equivalent discrete-time baseband received signal is expressed as

$$r_k = x_{mk} + N_k + j_k;\ k = 1, 2. \tag{15}$$

where

$$N_k = \int_0^{T_s} n(t)\psi_k(t)dt;\ j_k = \int_0^{T_s} j(t)\psi_k(t)dt;\ k = 1, 2. \tag{16}$$

This shows that r_k is a Gaussian random variable, with mean value equals to

$$\mathbf{E}\{r_k|x_m(t)\} = x_{mk};\ k = 1, 2. \tag{17}$$

Therefore, (17) can be expanded as

$$\mathbf{E}\{(r_1 - x_{m1})(r_2 - x_{m2})|x_m(t)\} = \mathbf{E}\{(n_1 + j_1)(n_2 + j_2)\}. \tag{18}$$

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

$$\text{var}\{r_k|x_m(t)\} = \frac{N_o}{2} + \iint_0^T K_j(t-\tau)\psi_k(t)\psi_k(\tau)dtd\tau, \tag{19}$$

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

$$f_{r_1r_2|x_m(t)}(R_1, R_2) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(\frac{-(R_1 - x_{m1})^2}{2\sigma^2}\right) \times\exp\left(\frac{-(R_2 - x_{m2})^2}{2\sigma^2}\right). \tag{20}$$

If the symbol $x_m(t)$ is transmitted, the probability that the receiver decodes it correctly $P_r(C|m)$ is given as [38]

$$P_r(C|m) = P_r(L_{ml}^1 \le r_1 \le L_{mu}^1, L_{ml}^2 \le r_2 \le L_{mu}^2), \tag{21}$$

where L_{ml}^1 and L_{mu}^1, and L_{ml}^2 and L_{mu}^2 are the lower and upper bounds of r_1, and r_2 respectively, Therefore, 21 can be expanded as

$$P_r(C|m) = \int_{L_{ml}^1}^{L_{mu}^1}\int_{L_{ml}^2}^{L_{mu}^2} f_{r_1r_2|x_m(t)}(R_1, R_2)dR_1dR_2, \tag{22}$$

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

$$P_r(C|m) = \int_{g_{ml}}^{g_{mu}} \frac{1}{\sqrt{2\pi}}\exp\frac{-(z)^2}{2}dz \int_{h_{ml}}^{h_{mu}} \frac{1}{\sqrt{2\pi}}\exp\frac{-(w)^2}{2}dw \tag{23}$$

where

$$\begin{aligned} h_{ml} &= \frac{L_{ml}^2 - x_{m2}}{\sigma};\ h_{mu} = \frac{L_{mu}^2 - x_{m2}}{\sigma}; \\ g_{ml} &= \frac{L_{ml}^1 - x_{m1}}{\sigma};\ g_{mu} = \frac{L_{mu}^1 - x_{m1}}{\sigma}; \end{aligned} \tag{24}$$

Following [38], specific evaluation of (23) based on (24) requires that all possible transmitted signals to be considered. Due to signal symmetry, it is possible to calculate $P_r(C|m)$ for every QAM scheme despite the tedious nature of this technique. It can be demonstrated that, irrespective of the QAM scheme considered, there are four signals for which $P_r(C|m)$ is

$$P_r(C|m) = \Psi^2(d), \tag{25}$$

where $\Psi(d) = 1 - Q(d)$ is the cumulative distribution function of the standard Gaussian distribution and d is a constant defined as

$$d = \left[\frac{\text{SNR}}{1 + \text{SNR}\cdot\text{JSR}}\right]^{\frac{1}{2}}. \tag{26}$$

For 16 QAM, there are 8 signals for which

$$P_r(C|m) = \Psi(d)(1 - 2Q(d)). \tag{27}$$

Finally, the remaining 4 signals for 16 QAM have

$$P_r(C|m) = (1 - \Psi(d))^2. \tag{28}$$

Therefore, 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:

$$\begin{aligned} P_e = 1 - \frac{1}{4}\Big\{&\Psi^2(d) + 2\Psi(d)[1 - 2Q(d)] \\ &+ [1 - 2Q(d)]^2\Big\} \end{aligned} \tag{29}$$

B. QPSK MODULATED JAMMING WAVEFORM

It was shown in [39] 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 [40]. Here, a perfect channel estimation is assumed, such that the jamming signal is 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

$$\begin{aligned} j(t) = &\sqrt{\frac{P_J}{2}}\cos\left(\frac{2\pi}{M}(m-1)\right)\psi_1(t) \\ &+\sqrt{\frac{P_J}{2}}\sin\left(\frac{2\pi}{M}(m-1)\right)\psi_2(t) \end{aligned} \tag{30}$$

It was shown in [39] that, in the presence of any jamming signal $\bar{j}$, the average probability of error P_e of an M-QAM signal in an AWGN channel is given by

$$\begin{aligned} &P_e(j, \text{SNR}, \text{JNR}) \\ &\approx \tfrac{1}{2}\left(1 - \tfrac{1}{\sqrt{M}}\right)\left[\text{erfc}\left(\sqrt{\text{SNR}}\tfrac{d_{\min}}{2} + \sqrt{\text{JNR}}j\right)\right. \\ &\left.+\text{erfc}\left(\sqrt{\text{SNR}}\tfrac{d_{\min}}{2} - \sqrt{\text{JNR}}j\right)\right] \end{aligned} \tag{31}$$

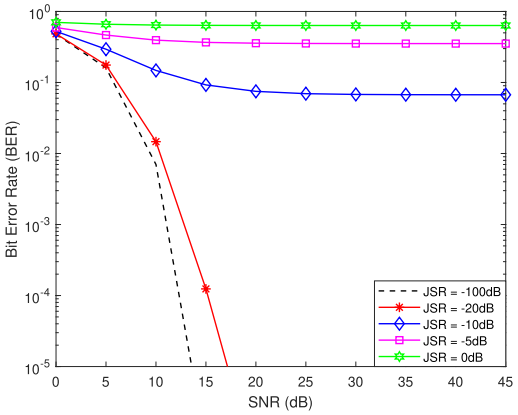

FIGURE 3. BER of IEEE 802.11n system in the presence of Gaussian noise jamming signal.

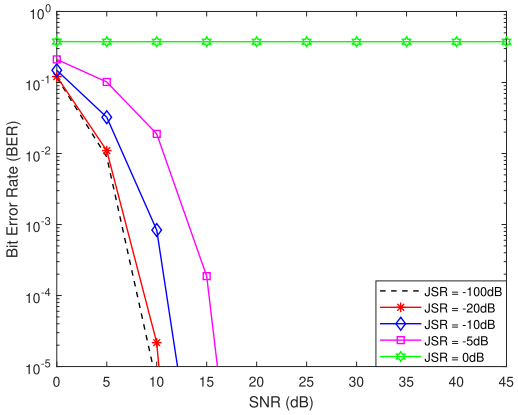

FIGURE 4. BER of IEEE 802.11n system in the presence of QPSK modulated jamming signal.

where $j = \mathbf{Real}\bar{j}$ or $j = \mathbf{Imag}\bar{j}$, and d_{min} denotes the minimum distance of the M-QAM modulation scheme.

The jammer intends to maximize (31) 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 $\mathbf{E}(a^2) \leq 1/2$ 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

$$\max_{f_A} \int_a P_a\left(a, \text{SNR}, \text{JNR}\right) f_A da;\ \ s.t.\ \mathrm{E}\left(a^2\right) \leq \frac{1}{2}$$
$$\equiv \max_{f_A} \mathbf{E}\left\{P_e\left(a, \text{SNR}, \text{JNR}\right)\right\};\ \ s.t.\ \mathrm{E}\left(a^2\right) \leq \frac{1}{2} \quad (32)$$

Considering that the jamming signal has at most two signal levels a_1 and a_2 [39], the PDF of the jamming signal along any signalling dimension can be expressed as

$$f_A(a) = \lambda\delta(a - a_1) + (1 - \lambda)\delta(a - a_2);\ \ \lambda \in [0, 1]$$
$$\lambda a_1^2 + (1 - \lambda)a_2^2 \leq \frac{1}{2}, \quad (33)$$

where λ 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 (33), the overall P_e along any signaling dimension can be generalized to

$$P_e\left(\lambda, a_1, a_2, SNR, JNR\right) \approx \tfrac{1}{2}\left(1 - \tfrac{1}{\sqrt{M}}\right)\left[\lambda\Gamma_1 + (1 - \lambda)\Gamma_2\right], \quad (34)$$

where Γ_1 and Γ_2 are expressed as

$$\Gamma_1 = \text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} + \sqrt{\text{JNR}}a_1\right)$$
$$+\text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} - \sqrt{\text{JNR}}a_1\right), \quad (35)$$
$$\Gamma_2 = \text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} + \sqrt{\text{JNR}}a_2\right)$$
$$+\text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} - \sqrt{\text{JNR}}a_2\right). \quad (36)$$

For a QPSK jamming signal when the IEEE 802.11n signal uses M-QAM, it was shown that [39]

$$\sqrt{\text{SNR}\frac{d_{\min}^2}{2}} < \sqrt{\text{JNR}} \cdot \tanh\left[2\sqrt{\text{SNR}\frac{d_{\min}^2}{2}\text{JNR}}\right]. \quad (37)$$

From (37), it can be noted that when $\text{SNR}\frac{d_{min}^2}{2} > 1$, $\tanh\left[2\sqrt{\text{SNR}\frac{d_{\min}^2}{2}\text{JNR}}\right] \approx 1$. Thus, it can be deduced that $\text{SNR}\frac{d_{\min}^2}{2} \ll \text{JNR}$. Based on this, it was shown in [39] and [21] that for the case of using QPSK as a jamming signal with an M-QAM signal, (34) can be simplified as

$$P_e = \frac{1}{2}\left(1 - \frac{1}{\sqrt{M}}\right)\left[\text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} + \sqrt{\frac{\text{JNR}}{2}}\right)\right.$$
$$\left.+\text{erfc}\left(\sqrt{\text{SNR}}\frac{d_{\min}}{2} - \sqrt{\frac{\text{JNR}}{2}}\right)\right]. \quad (38)$$

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

$$P_e = \frac{3}{8} \times \left[\text{erfc}\left(\sqrt{\text{SNR}}\left(1 + \sqrt{\text{JSR}}\right)\right)\right.$$
$$\left.+\text{erfc}\left(\sqrt{\text{SNR}}\left(1 - \sqrt{\text{JSR}}\right)\right)\right]. \quad (39)$$

Comparing the performance of the system under Gaussian noise jamming in (29) and that of QPSK modulated jamming in (39), we can deduce that Gaussian noise jamming is more effective in terms of degrading the system's performance. Substituting $\Psi\left(d\right) = 1 - Q\left(d\right)$, (29) can be simplified to

$$P_e = 3Q\left(d\right) - \frac{9}{4}Q^2\left(d\right). \quad (40)$$

Therefore, given that $Q\left(d\right)$ is a monotonically decreasing function, for a constant SNR, (40) will decay rapidly with increasing JSR due to the quadratic function. Whereas,

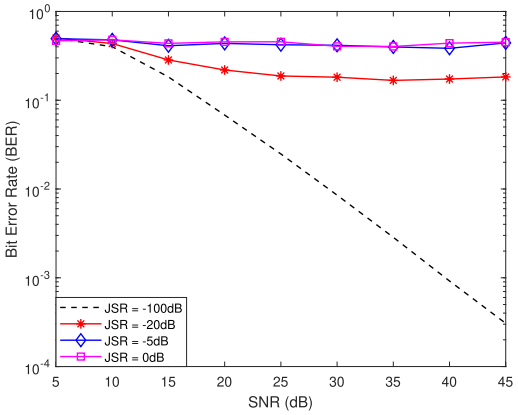

FIGURE 5. BER of IEEE 802.11n victim system in the presence Gaussian noise waveform with varying JSR.

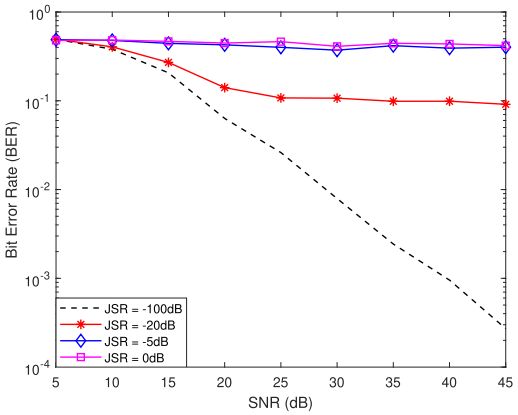

FIGURE 6. BER of IEEE 802.11n victim system in the presence QPSK modulated waveform with varying JSR.

(39) will decay slowly with increasing JSR. This is also intuitive, as the Gaussian noise waveform has no inherent pattern, as is the case with the QPSK modulated waveform.

V. NUMERICAL AND SIMULATION EVALUATIONS

In this section, we present numerical and simulation results in order to identify the most effective jamming waveforms in WLAN IEEE 802.11n. In particular, we quantify the impact of the earlier analyzed jamming waveforms, namely (i) Gaussian noise and (ii) QPSK modulated signals, on the considered IEEE 802.11n system.

A. NUMERICAL RESULTS FOR AWGN CHANNEL SCENARIO

In Sec. IV, the BER performance of the underlying system model under Gaussian noise and QPSK jamming waveforms was obtained as in (29) and (39) respectively. Fig. 3 demonstrates the impact of a 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 0dB, the performance is severely degraded where a BER > 0.1 is experienced over all SNR values.

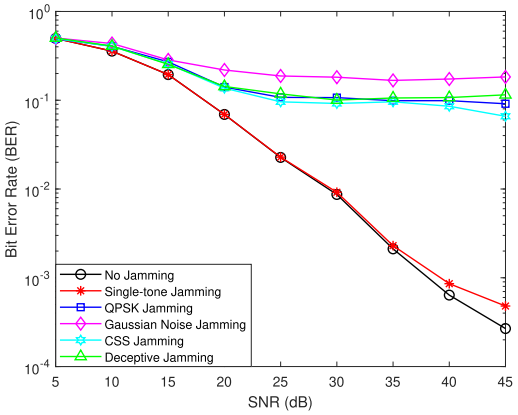

FIGURE 7. BER of IEEE 802.11n victim system in the presence of jamming signals.

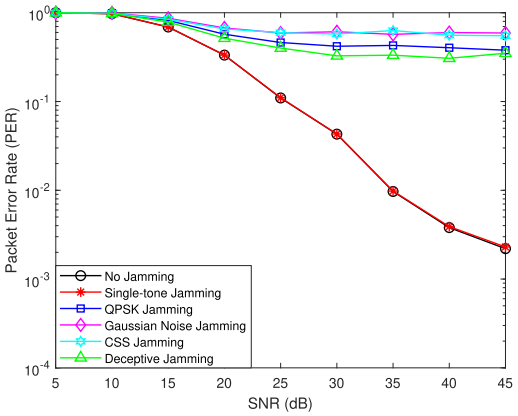

FIGURE 8. PER of IEEE 802.11n victim system in the presence of jamming signals.

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 $=$ 0dB, 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 $=$ 0dB. This indicates that both waveforms are able to completely corrupt all transmitted packets when JSR $=$ 0dB, 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 single-tone signal, a Long Range (LoRa) chirp spread spectrum (CSS) modulated signal, and a deceptive jamming signal. The signal model representation of the single-tone jamming waveform is expressed as:

$$j(t) = \sqrt{2P_J}\sin\left(2\pi f_j t + \theta_j\right), \tag{41}$$

TABLE 3. 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

where f_j is the jamming tone frequency, and θ_j is the random jammer phase. The complex baseband LoRa waveform with equivalent discrete-time baseband signal given as [41]

$$j_k[n] = e^{j2\pi\left(\frac{n^2}{2N}+\left(\frac{k}{N}-\frac{1}{2}\right)\right)}, \tag{42}$$

where $N = 2^{\mathrm{SF}}$ is the total number of LoRa samples, $n = 0, 1, 2, \cdots, (N-1)$ is the sample index. On the other hand, in order to simulate deceptive jamming, we assume that the jammer is also employing IEEE 802.11n with MCS = 4.

All the simulations are end-to-end simulations and are performed by employing the wlanHTConfig and wlanTGnChannel system objects of the MATLAB WLAN toolbox. Unless otherwise stated, adopted simulation parameters are presented in Table 3.

Fig. 5, shows that the Gaussian noise jamming waveform has a destructive impact on the considered system. We find that for JSR = 0dB, the BER > 0.1 is achieved. This agrees with the analysis results obtained for the AWGN scenario. However, it should be noted that even at lower $-20 <$ JSR $<$ 0dB, 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 the QPSK modulated jamming waveform also causes a 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 = 0dB.

Fig. 7 compares the effects of different jamming waveforms (as well as the absence of jamming). Fig. 7 shows that when JSR $= -20$dB, the Gaussian noise, QPSK modulated, deceptive jamming, and CSS modulated waveforms have a more noticeable impact than the single-tone waveform. In specific, it can be observed that BER ≈ 0.6 is experienced when the considered waveforms are employed for jamming except the single-tone waveform. Furthermore, it can be seen that, for SNR $<$ 35dB, the single-tone waveform has negligible impact on system performance, and hence, the BER performance of the system under single-tone waveform jamming is similar to the scenario where no jamming is present. Alternatively, it can be observed that the other waveforms can cause significant deterioration to the system BER performance, in which an error floor is observed for SNR $>$ 20dB.

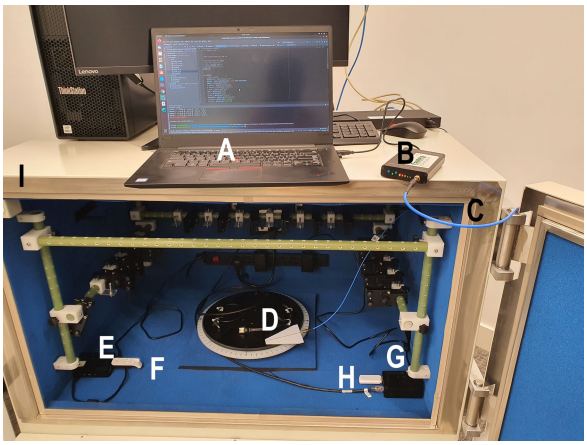

FIGURE 9. Experimentation Testbed: *A* Host for HackRF, *B* HackRF One, *C* SME Cable, *D* SME Antenna, *E*, and *G* Raspberry pi nodes, *F*, and *H* Wi-Fi dongles, and *I* RF Isolation Chamber.

In Fig. 8, it is observed that all considered waveforms with the exception of single-tone waveform achieved a PER = 1 for SNR $<$ 10dB when JSR $= -20$dB. On the other hand, when single-tone waveform is employed as a jamming signal to disrupt communication of the victim system, the system performance is similar in terms of *PER* when JSR $= -20$dB. This shows how ineffective a single-tone signal is compared to the other investigated jamming waveforms. Moreover, this further demonstrates that overall, the Gaussian noise is a more effective jamming waveform to attack IEEE 802.11n victim system with MCS $= 4$ compared to other non-optimized digitally modulated waveforms.

VI. EXPERIMENTAL RESULTS

We implement JamRF, a jamming framework based on GNU Radio interfaced with HackRF SDR, and make this available to the community[2] as a platform for further research. The experimental setup depicted in Fig. 9 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) [42] as a routing protocol instead of Hybrid Wireless Mesh Protocol (HWMP) of IEEE 802.11s standard.

A. EXPERIMENTAL SETUP

The project requires both hardware and software tools. These are presented in Table 4 and 5 respectively. Unless otherwise stated, are summarized in Table 6.

B. IMPLEMENTED JAMMERS

The specific implemented jammers are summarized in Table 8. We will now discuss these jammers in depth.

[2]https://github.com/tiiuae/jamrf

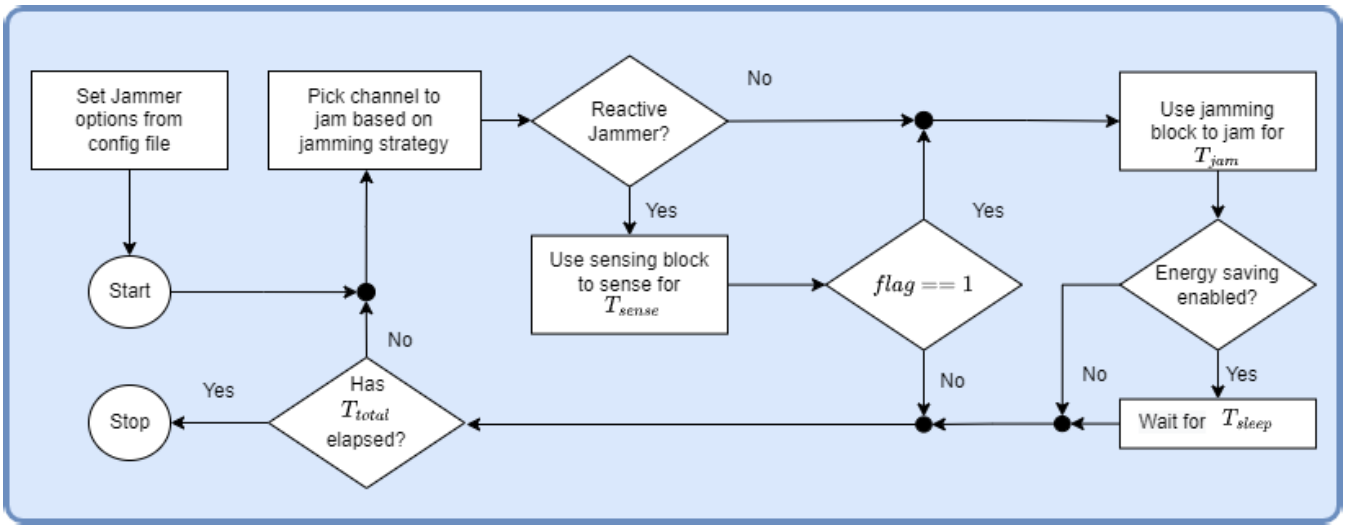

FIGURE 10. Detailed top-level structure JamRF with HackRF one built on top of GNU Radio.

TABLE 4. Experimental testbed hardware specifications.

Component	Version/model
Jammer radio host	Lenovo ThinkPad X1 Extreme Gen 3
Host device	Raspberry Pi4
Jammer radio	HackRF One
Sender and receiver interface	wubr-508n Dongle
SME Cables	Tonearm series 300
Spectrum Analyzer	Tektronix RSA306B

TABLE 5. Experimental testbed software specifications.

Component	Version/model
Jammer radio host	Ubuntu 20.04
Host device	Ubuntu 20.04
Sender traffic generator	Iperf v3.0
Jammer SDR	GNURadio v3.8.0
Simulation software	Matlab r2021b

TABLE 6. Experimental parameters.

Parameter	Value
Type of traffic	UDP
Node transmission frequency	2.462 GHz
Transmission period	300 s
P_T	30 dBm
P_J	6 dBm
d_{TR}	1 m
d_{JR}	0.5 m

1) CONSTANT JAMMER

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

2) 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 Wi-Fi with 14 channels, the jammer sequentially hops from one channel to the next sequentially.

TABLE 7. Mapping HackRF gain settings to Power.

RF (dB)	IF (dB)	BB (dB)	Power (dBm)
0	1	20	-40
0	5	20	-35
0	10	20	-30
0	15	20	-25
0	20	20	-20
0	25	20	-15
0	20	20	-10
0	36	20	-5
0	41	20	0
0	47	20	5
14	39	20	10
14	47	20	13

3) 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.

4) 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

TABLE 8. Implemented jammers and features in JamRF.

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

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

$$P = \frac{1}{2N} \sum_{i=0}^{N} |x(i)|^2 \tag{43}$$

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 (γ) 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.

5) 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.

C. JamRF DESIGN CONFIGURATION

Fig. 10 depicts the JamRF toolbox's high-level structure. Because of the aforementioned reasons, the HackRF one was chosen. The JamRF script is then executed after the configurations are set using the provided config files. A channel is chosen and jamming is performed based on a jamming strategy. If the jammer is proactive, jamming will take place using the jamming block depicted in Fig. 11. If the jammer is reactive, the sensing block shown in Fig. 12 is executed first, and if channel activity is detected, the jamming block follows.

D. RESULTS AND DISCUSSIONS

The HackRF has three gain settings that need to be tuned in order to realize a specific transmit power. The gain controls are at the RF, intermediate frequency (IF), and baseband (BB) stages. In this experiment, we tuned the gains of the HackRF and measure the transmit power using a spectrum analyzer. The measurements are as presented in Table 7.

Moreover, the aim of jamming is to achieve 100% transmission disruption even in challenging conditions.

TABLE 9. HackRF time constraints.

Time	Proactive	Reactive
t_{boot}	450 ms	450 ms
t_{jam}	1.82 s	1.82 s
t_{sense}	0	2.99 s

TABLE 10. 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

An RF jammer needs to react quickly to hit the packet for the minimal required jamming duration. For instance, in IEEE 802.11n, a 1000 byte packet transmitted with a rate of 10 Mbps has an on-air time of 800 μs. Due to this tight requirement, we carry out some time constraint measurements for the HackRF, in order to identify the timing requirements, see Fig. 13, and Table 9, where t_{boot}, t_{sense}, and t_{jam} are the time required by the HackRF to boot, sense, and jam respectively. In proactive jammer, the minimum time requirement to execute jamming operation is $1.82s$. Whereas, reactive jammer has the t_{sense} that allows it to detect channel activity before jamming. The minimum timing requirement for reactive jammer to jam a channel using HackRF is $\approx 4.81s$ which is $\approx 2.6\times$ greater than proactive jammer.

Table 10 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 10 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 operation.

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. 14. 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

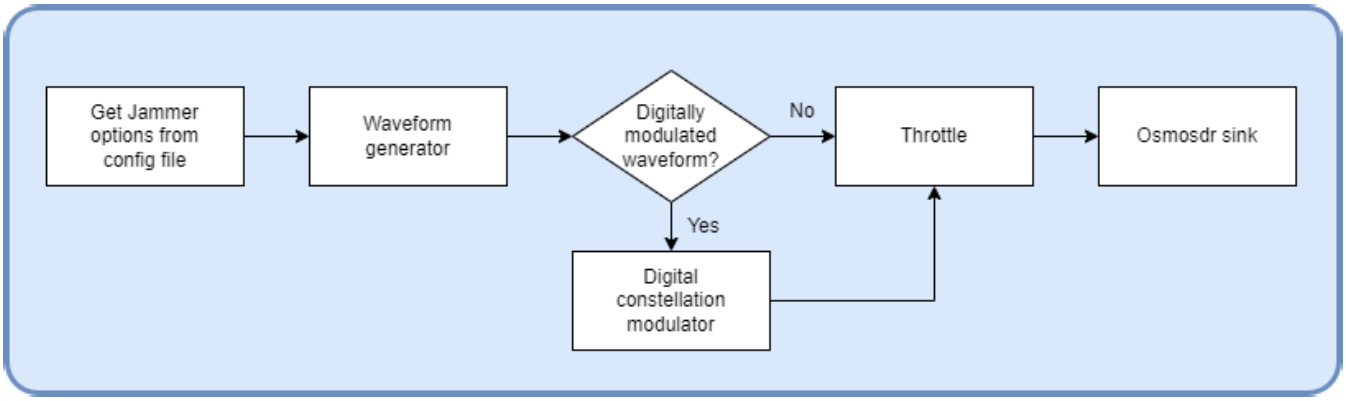

FIGURE 11. GNU Radio building blocks for the JamRF jamming block.

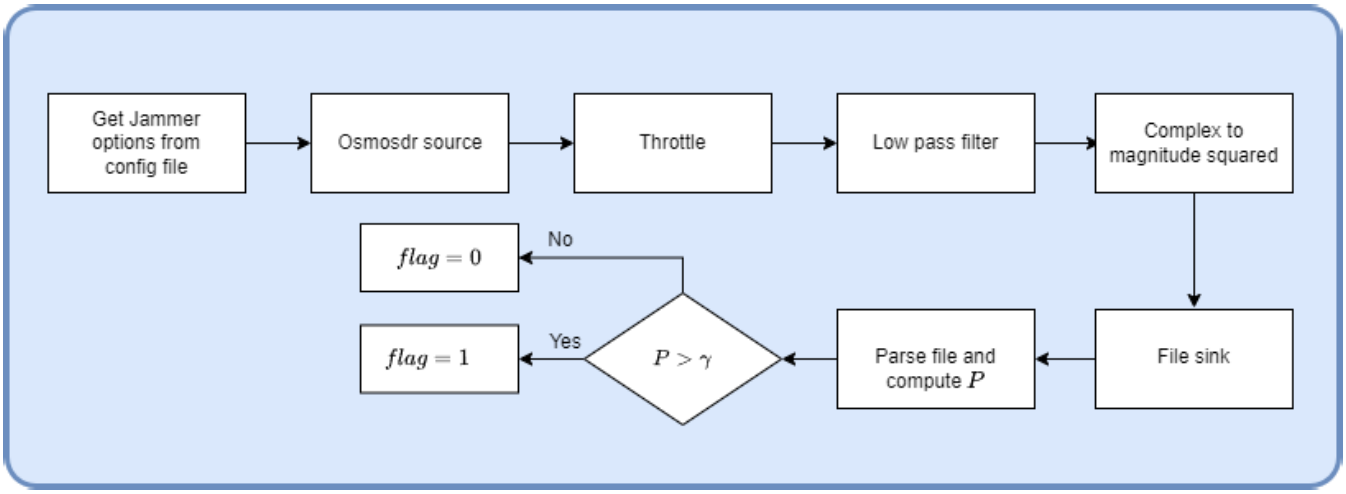

FIGURE 12. GNU Radio building blocks for the JamRF sensing block.

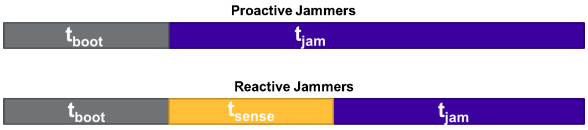

FIGURE 13. Jamming time requirements.

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

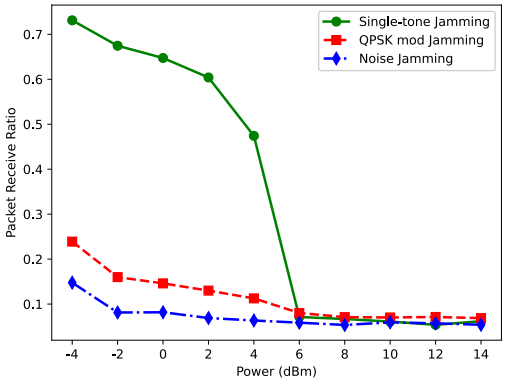

FIGURE 14. Impact of jamming waveforms on the underlying IEEE 802.11n system.

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. 15, it is observed that PRR decreases with increasing distance between adjacent channels.

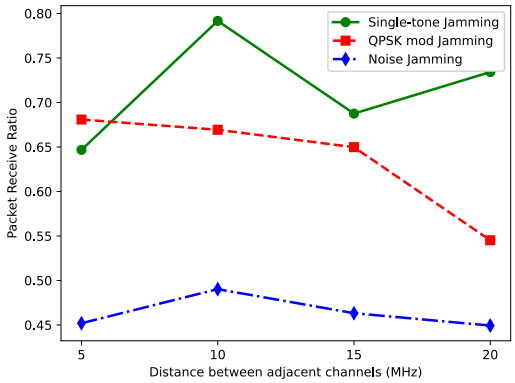

FIGURE 15. Impact of the distance between adjacent channels for jamming using HackRF.

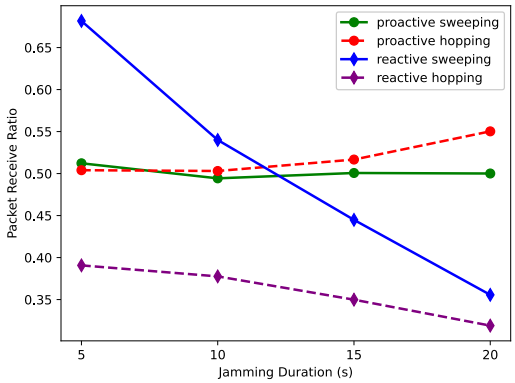

FIGURE 16. Jamming Performance of proactive and reactive jammers versus jamming duration.

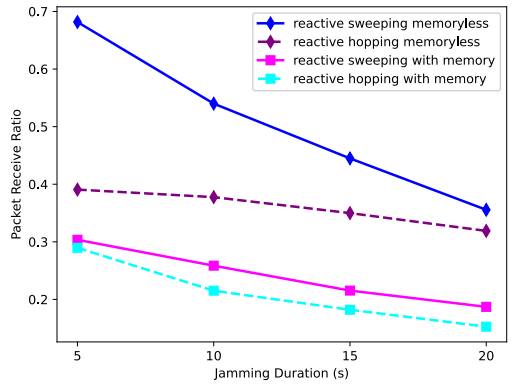

FIGURE 17. Jamming Performance of stateful reactive jammers versus jamming duration.

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. 16, 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 ≈70%, whereas the corresponding proactive jammer resulted in PRR ≈ 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. 17. 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. CONCLUSION

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.

The obtained analytical and simulation results, as well as the experimental results, showed that system performance degraded under jamming attacks. Furthermore, while simulation results show a 100% PER for both QPSK modulated and Gaussian noise waveforms, experimental results show a packet loss ratio (1- PRR) of around 80% for both QPSK modulated and Gaussian noise waveforms under constant jamming attack. The $t_{boot} = 450$ms HackRF time constraint in a proactive jammer accounts for the 20% difference between simulation and experimental results. This demonstrates that the hardware time constraints are the major disadvantage of using low-cost SDRs (such as the HackRF) to implement these jamming techniques. To address this, we added a channel awareness feature that increased the reactive jammer's performance by about 10%.

Furthermore, the Gaussian noise is shown to consume fewer CPU resources compared to QPSK and at the same

time achieves 100% PER. Moreover, 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," 2021, *arXiv:2101.00292*.

[2] M. A. 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. Sensor Syst. (DCOSS)*, Jul. 2021, pp. 319–326.

[3] Ettus Research LLC. *Universal Software Radio Peripheral (USRP)*. Accessed: Jun. 20, 2022. [Online]. Available: http://www.ettus.com

[4] M. Ossmann. *HackRF One*. Accessed: Jun. 20, 2022. [Online]. Available: https://greatscottgadgets.com/hackrf/

[5] Nuand. *BladeRF 2.0*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.nuand.com/bladerf-2-0-micro/

[6] RTL-SDR. *Blog R820T RTL2832U*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.rtl-sdr.com/

[7] Airspy. *Airspy R2*. Accessed: Jun. 20, 2022. [Online]. Available: https://airspy.com/

[8] Perfect Jammer. *EO-08-007 Jammer*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.perfectjammer.com/wireless-wifi-bluetooth-jammers.html

[9] *TX-100 Jammer*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.perfectjammer.com/5g-cellphone-signal-jammers.html

[10] *M16-5G M16-A M16-B Jammer*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.perfectjammer.com/desktop-16-antennas-cellphone-5g-jammers.html

[11] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11 b/g WLAN tolerance to jamming," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, vol. 3, Oct./Nov. 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. Secur. Privacy Commun. Syst.* Berlin, Germany: 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 Mil. Commun. Conf. (MILCOM)*, Nov. 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)*, Apr. 2014, pp. 2697–2706.

[15] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1486–1499, Jul. 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. Privacy Wireless Mobile Netw.*, 2020, pp. 89–98.

[17] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "Performance of IEEE 802.11 under jamming," *Mobile 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.*, vol. 99, no. 14, pp. 5–9, Aug. 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, Dec. 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. Wireless Netw. Secur. (WiSec)*, vol. 2011, pp. 47–52.

[21] E. M. Shaheen, "Performance of MIMO IEEE802.11n WLAN in presence of QPSK jammer with inphase/quadrature origin offsets," *Wireless 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 IEEE802.15.3a channel models," in *Proc. Can. Conf. Electr. Comput. Eng. (CCECE)*, May 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 Navigat.*, vol. 10, no. 5, pp. 850–861, Jun. 2016.

[24] Y. Fan, X. Liao, and A. V. Vasilakos, "Physical layer security based on interference alignment in K-user MIMO Y 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 Wireless Commun. Lett.*, vol. 6, no. 5, pp. 662–665, Oct. 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, Oct. 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, Jun. 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, Nov. 2015.

[29] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers-analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation)," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 09 2011.

[30] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 256–265.

[31] 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, Dec. 2014.

[32] 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, 1st Quart., 2014.

[33] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2010.

[34] S. Mehmood, A. N. Malik, I. M. Qureshi, M. Z. U. Khan, and F. Zaman, "A novel deceptive jamming approach for hiding actual target and generating false targets," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–20, Apr. 2021.

[35] M. Viswanathan, "Gaussian waves," in *Wireless Communication Systems in MATLAB*, 2nd ed. Independently Published, 2014. [Online]. Available: https://www.gaussianwaves.com/2014/07/power-delay-profile/

[36] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[37] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Norwood, MA, USA: Artech House, 2011. [Online]. Available: http://books.google.com/books?id=cty3iVlvkNAC&pgis=1

[38] D. C. Bukofzer, "Performance of receivers in digital radio applications operating in the presence of noise and jamming," in *Proc. IEEE Mil. Commun. Conf., Commun.-Comput., Teamed (MILCOM)*, Oct. 1986, pp. 39–51.

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

[40] S. D. Amuru and R. M. Buehrer, "Optimal jamming strategies in digital communications—Impact of modulation," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1619–1624.

[41] O. Afisiadis, M. Cotting, A. Burg, and A. Balatsoukas-Stimming, "On the error rate of the LoRa modulation with interference," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 1292–1304, Feb. 2019.

[42] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, *Better Approach to Mobile Ad-Hoc Networking (Batman)*, IETF Draft, Jan. 2008, pp. 1–24. [Online]. Available: https://www.open-mesh.com/

ABUBAKAR S. ALI (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from Bayero University Kano, Kano, Nigeria, in 2014, and the M.S. degree in communications and signal processing from the University of Leeds, Leeds, U.K., in 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Khalifa University, Abu Dhabi, United Arab Emirates. From 2018 to 2019, he was a Lecturer with the Department of Electrical Engineering, Bayero University Kano. His research interests include low-power wireless communications, machine learning, artificial intelligence, and optimization for communications and networking.

MICHAEL BADDELEY (Member, IEEE) received the M.Eng. degree in computer and electronic systems from the University of Strathclyde, Glasgow, U.K., in 2010, and the Ph.D. degree in software defined networking for the Industrial Internet of Things from the University of Bristol, U.K., in 2020. He is currently a Lead Wireless Researcher with the Secure Systems Research Centre (SSRC), Technology Innovation Institute (TII), Abu Dhabi, United Arab Emirates. His current research interests include robust wireless communication for ad-hoc and infrastructure-less mesh networks, such as interference mitigation, spectral coexistence, and end-to-end dependability across a mesh-cloud continuum.

LINA BARIAH (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in communications engineering from Khalifa University, Abu Dhabi, United Arab Emirates, in 2015 and 2018, respectively. She was a Visiting Researcher with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, in 2019, and an Affiliate Research Fellow with the James Watt School of Engineering, University of Glasgow, U.K. She is currently a Senior Researcher with the Technology Innovation Institute, a Visiting Research Scientist at Khalifa University, and an Affiliate Researcher with the University at Albany, USA. She was a member of the Technical Program Committee of a number of IEEE conferences, such as ICC and GLOBECOM. She is a Senior Member of the IEEE Communications Society, the IEEE Vehicular Technology Society, and the IEEE Women in Engineering. She is also an organizing/chairing a number of workshops. She serves as a session chair and an active reviewer for numerous IEEE conferences and journals. She is also an Associate Editor of the IEEE COMMUNICATION LETTERS, an Associate Editor of the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, and an Area Editor of *Physical Communication* (Elsevier). She is a Guest Editor of *IEEE Network* magazine and the *RS Open Journal on Innovative Communication Technologies* (RS-OJICT).

MARTIN ANDREONI LOPEZ (Member, IEEE) received the bachelor's degree in electronic engineer from the Universidad Nacional de San Juan (UNSJ), Argentina, in 2011, the master's degree in electrical engineering from the Federal University of Rio de Janeiro (COPPE/UFRJ), in 2014, and the Ph.D. degree from the Teleinformatics and Automation Group (GTA), COPPE/UFRJ, and the Phare Team of Laboratoire d'Informatique Paris VI (LIP6), Sorbonne Universite, France, in 2018. He was a Researcher at the Samsung Research and Development Institute, Brazil. He is currently a Network Security Researcher with the Secure System Research Center, Technology Innovation Institute, Abu Dhabi, United Arab Emirates. He has coauthored several publications and patents in the area of security, virtualization, traffic analysis, and big data.

WILLIAN TESSARO LUNARDI (Member, IEEE) received the Ph.D. degree in computer science from the University of Luxembourg. He is currently a Machine Learning Researcher with the Secure Systems Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates. He is also working on machine learning for network security, physical layer security, and jamming detection. He has published over 25 research papers in scientific international journals, conferences, and book chapters. His research interests include machine learning and combinatorial optimization.

JEAN-PIERRE GIACALONE (Member, IEEE) received the Engineering degree from the from the École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications (ENSEEIHT), Toulouse, France. He worked as an Expert in software architecture for Advanced Driving Assistance Systems at Renault and as a Principal Engineer and Architect within the Mobile Systems Technologies Group at Intel. He is currently the Vice President of Secure Communications Engineering with the Secure Systems Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates. He is responsible for carrying out research on secure communications, with a focus on improving resilience of cyber-physical and autonomous systems. He holds 19 patents and has coauthored 15 research papers accepted for publication in international journals and conference proceedings.

SAMI MUHAIDAT (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2006. From 2007 to 2008, he was a NSERC Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Canada. From 2008 to 2012, he was an Assistant Professor with the School of Engineering Science, Simon Fraser University, BC, Canada. He is currently a Professor with Khalifa University, and an Adjunct Professor with the Department of Systems and Computer Engineering, Carleton University, Canada. His research interests include wireless communications, optical communications, the IoT with emphasis on battery-less devices, and machine learning. He is currently an Area Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and a Lead Guest Editor of the IEEE OJ-COMS Large-Scale Wireless Powered Networks with Backscatter Communications Special Issue. He served as a Senior Editor and Editor for the IEEE COMMUNICATIONS LETTERS, a Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, and an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.