Chirp Subcarrier Jamming Attacks: An OFDM Based Smart Jammer Design

Mehmet Akif Durmaz†, Hakan Alakoca†, Güneş Karabulut Kurt†, Cem Ayyıldız‡
† Istanbul Technical University, Wireless Communication Research Laboratory (WCRL), Istanbul, Turkey
‡Turkcell Technology Research and Development Laboratory, Turkcell İletişim Hizmetleri A.Ş., Istanbul, Turkey
{durmazm, alakoca, gkurt}@itu.edu.tr, cem.ayyildiz@gmail.com

***Abstract*—In this study a new jammer design for orthogonal frequency division multiplexing (OFDM) based systems is introduced. We present three new vulnerability attack scenarios based on chirp signals. These are the conventional chirp attack, the cyclic prefix chirp attack and the pilot tone chirp attack. Bit error rate (BER) performances are investigated in presence of chirp based attacks. It is shown that the performance degradation is increased when compared to Gaussian distributed jammers. Chirp signals are also preferable due to nominal peak-to-average power ratios (at least 7 dB lower than Gaussian counterparts).**

***Index Terms*—Jammer attacks, PHY security, OFDM, chirp signal, smart jamming**

I. Introduction

Orthogonal frequency division multiplexing (OFDM) has become a common modulation technique in modern communication systems. This is due to OFDM's robustness across multipath environments, high spectral efficiency and simple channel equalization. On the other hand, providing security is an essential part of the wireless communication networks due to the broadcast nature of the wireless medium. Tight synchronization requirements and sensitivity to channel estimation increase sensitivity of OFDM to jamming attacks. Vulnerabilities of OFDM are still being investigated in presence of adversary attacks. In this study, we examine robustness of OFDM towards a new jammer design which is inspired by the chirp waveform.

The simplest jamming technique is the conventional jamming, referred to as barrage jamming attacks as given in [1]. It has been shown that current applications of OFDM are very sensitive to jamming attacks [2]–[7]. The carrier signal of barrage jamming generated with a random noise waveform may be preferable by the attackers when any knowledge of the target is unachievable. Efficiency of partial band jamming is examined in [2]. While conventional jammers are currently in use, there are few smart jamming techniques which are more effective than jamming the entire band of target signal. Many studies investigate the effects of cyclic prefix (CP) and pilot jamming techniques over the OFDM systems. In [3], the author details that contaminating CP is sufficient in high SNR values for power constrained jammers. Additionally, the CP jammer is more effective when the maximum likelihood estimator is used in the receiver [4]. Another jamming strategy aiming at only the pilot signals to degrade the channel estimation quality at the receiver is presented in [5]. According to [6], jamming one pilot subcarrier has a more extensive effect than jamming one data subcarrier. In [7], the effect of CP and pilot jamming attacks on orthogonal frequency division multiple access (OFDMA) and single carrier frequency division multiple access (SC-FDMA) nodes are investigated via software define radio nodes.

This work was supported by Turkcell İletişim Hizmetleri A.Ş. under grant BSTB032384.

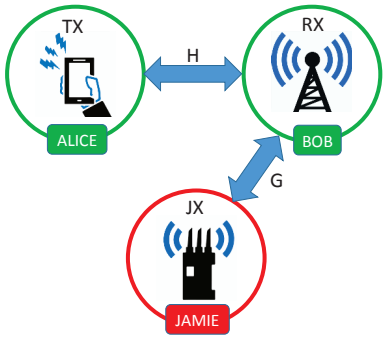

Fig. 1: Three node network model. Alice and Bob are the legitimate nodes. Jamie is an adversary attacker node.

There are several other alternatives for jammer signals, and one prominent candidate is the chirp signal. Chirp signals are usually encountered in some acoustic form for instance bird songs and animal communication signals (frog, whales) [8]. Some bats (specifically microbats) have been using chirp signals for echolocation. Chirp signals are often used in GPS jammers [9], and radar systems. In our work, we investigate the effectiveness of chirp based wideband signals as jamming signals.

Our network model consists of a legitimate transmitter (Alice), a legitimate receiver (Bob) and an adversary attacker node (Jamie), as shown in Figure 1. We intend to demonstrate the network performance of an OFDM based system under different kinds of smart jamming attacks, which are constituted by Jamie. The effect of chirp subcarrier jamming attacks on a system performance is investigated.

Main contributions of this study are:

1. *Designing chirp subcarrier based jamming attacks as an adversary model:* we aim to use the chirp signal, which is commonly used in radar and system identification

978-1-5386-2077-9/17/$31.00 ©2017 IEEE

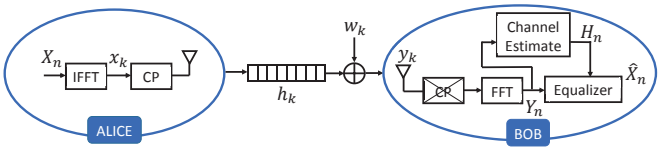

Fig. 2: Transmitter and receiver structure of OFDM based systems.

applications, as an adversary signal generator. It is already known that chirp waveform has a low peak-to-average power ratio (PAPR) requirement. OFDM based smart jamming methods are implemented.

2. *Evaluating and observing existing jamming techniques:* Comparative performance analyses are presented for the existing jamming attacks and our chirp based smart jamming attacks. According to our findings the bit error rate (BER) performance degradation is increased when using chirp waveform as the jammer signal instead of the frequently used version, the Gaussian noise.
3. *PAPR perspective:* Lower PAPR values are desired for transmitters, however PAPR is a critical issue in the AWGN signals. We show that the Gaussian noise signal has a higher PAPR value than chirp based multi-carrier waveform.

The rest of this paper is organized as follows. The OFDM based system model is given in Section II. Jammer models, which are principally examining the current literature, are described in Section III. In Section IV, chirp subcarrier based adversary attack designs are detailed. Simulation results and main findings are covered in Section V. We finally conclude the paper in Section VI.

II. System Model

Let X_n denote the complex symbol assigned to the n^{th} subcarrier of the each OFDM symbol. N denotes for the number of subcarriers, and the subcarrier set is assigned as $\mathcal{N}_F = \{0, 1, \ldots, N-1\}$. In our system model, pilot subcarriers are generated and interleaved in a comb type pilot assignment, at the beginning of every P symbols. Pilot subcarriers used for channel tracking and also synchronization purposes. Generated data subcarriers are combined with pilot subcarriers. After the serial-to-parallel (S/P) conversion block, inverse fast Fourier transform (IFFT) is applied. At the output of the IFFT block, the subcarriers which are in the time domain, x_k, are obtained as

$$x_k = \text{IFFT}(X_n) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} X_n \, e^{\frac{j2\pi kn}{N}}. \tag{1}$$

Then, the parallel-serial (P/S) conversion is implemented. For the CP insertion, the last C symbols of the OFDM symbol are copied to the beginning of the symbol. Analog signals are transmitted over the wireless channel between the OFDM transceiver pair, thus received signal y_k are given as

$$y_k = s_k * h_k + w_k, \tag{2}$$

where h_k is the impulse response of the wireless channel and w_k is the Gaussian noise component. Let y_k represent the received data in time domain with k^{th} sample of each OFDM symbol after the CP removal process. Then, these samples are converted back to frequency domain by using S/P, FFT and P/S blocks. The symbols in frequency domain are obtained as

$$Y_n = \text{FFT}(y_k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} y_{k,l} \, e^{-\frac{j2\pi kn}{N}}. \tag{3}$$

Assuming that the CP length is larger than the channel delay spread, the received symbols can be modeled as

$$Y_n = H_n X_n + W_n. \tag{4}$$

The main block diagram for the OFDM system is given in Figure 2. The S/P and P/S blocks are not shown in the figure for simplicity. Before detecting the transmitted symbols, an equalizer is used to compensate the effects of the channel. The channel estimates are denoted by $\widehat{H}_n$. When $n \in \mathcal{P}$, we obtain noisy channel estimates as

$$\begin{aligned} \widehat{H}_n &= \frac{Y_n}{X_n} = \frac{X_n H_n + W_n}{X_n} = H_n + \frac{W_n}{X_n} \\ &= H_n + \epsilon_n, \end{aligned} \tag{5}$$

where ϵ_n represents the channel estimation error. Considering zero forcing equalization, for $n \in \mathcal{N} \setminus \mathcal{P}$, the received information symbols are obtained as

$$\widehat{X}_n = \frac{Y_n}{\widehat{H}_n} = \frac{X_n H_n}{H_n + \epsilon_n} + \frac{w_n}{H_n + \epsilon_n}. \tag{6}$$

III. Gaussian Noise Based Jamming Models

In this section Gaussian noise based jamming attack models from the leading literature works are introduced.

A. Conventional Jamming Attacks (CoJ)

Conventional jamming attack is a straight-forward attack type. It is constituted by considering an OFDM signal. Transmitted jamming signal in the frequency domain over the n^{th} subcarrier of each OFDM symbol is denoted by J_n. Furthermore, jammer subcarriers are considered to be Gaussian distributed signals $J_n \sim \mathcal{CN}(0, \sigma_j^2)$ with a zero mean and σ_j^2 variance. The effect of σ_j on the signal-to-jammer-and-noise ratio (SJNR) is

$$SJNR = \frac{E_b}{N_0 + J} = \frac{1}{\sigma_n^2 + \sigma_j^2}, \tag{7}$$

where σ_n^2 is the variance of the Gaussian noise, and E_b is the average bit energy.

Like the OFDM transmission, frequency domain symbols are converted back to the time domain symbols, j_k, by using IFFT for $n \in \mathcal{N}$, next CP insertion is operated considering $j_k \sim \mathcal{CN}(0, \sigma_j^2)$ for $k \in \mathcal{N} \cup \mathcal{C}$, where $\mathcal{C}$ represents the set of CP indices. In order to decrease SNR for all tones, the transmission length of a jamming signal is selected as $N + C$.

Barrage jamming is a type of conventional OFDM based jamming that is considered for attacking the complete set of subcarriers, generating a wideband signal.

B. Cyclic Prefix Jamming Attacks (CPJ)

The CP portion of OFDM signals can be used for achieving acquisition and synchronization [10]. Yet, CP is a very critical part of the system, it became a great PHY security vulnerability that is affecting the overall system performance. CP based jamming system is designed in time domain symbols considering as

$$j_k = \begin{cases} j_k & k \in \mathcal{C} \\ 0 & k \in \mathcal{N}, \end{cases} \tag{8}$$

where subcarriers are constructed as $j_k \sim \mathcal{CN}(\mu, \sigma_j^2)$ when $k \in \mathcal{C}$. $\mathcal{C}$ is set of CP and $\mathcal{N}$ is set of carriers. Here, we assume that the attack signal is synchronized with the transmitted signal. The jammer can access the CP knowledge by its protocol-awareness [11].

C. Pilot Tone Jamming Attacks (PJ)

As indicated before, pilot subcarriers are the essential part of OFDM systems, since they are principally used to track channel estimates and also to improve synchronization accuracy. Pilot tone jamming attacks are considered as,

$$J_n = \begin{cases} J_n & n \in \mathcal{P} \\ 0 & n \in \mathcal{N} \setminus \mathcal{P}, \end{cases} \tag{9}$$

where $J_n \sim \mathcal{CN}(\mu, \sigma_j^2)$ and $\mathcal{P}$ represents the set of pilot tone when $n \in \mathcal{P}$. Similar to the case of CP jamming, pilot tone jamming attacks must be synchronized with the target. We assume that the jammer has apriori knowledge of the pilot symbol positions (i.e. frequency indices).

IV. Chirp Subcarrier Based Jamming Model

Chirp signal has an exclusive waveform principally used in linear frequency modulation, in a form of sinusoid waveform where its frequency increases or decreases with time. Sweep frequency $f_i(t)$ is defined from f_0 to f_1 corresponding to a sweep period, T. There are many swept-frequency cosine signal generation approaches in the literature. For linear chirp, frequency sweep is generated as $f_i(t) = f_0 + kt$, where k is an indicator for chirpyness factor defined as,

$$k = \frac{f_1 - f_0}{T}.$$

Time domain function for linear chirp can be expressed as

$$j_{ch} = \sin\left[\phi_0 + 2\pi\left(f_0 t + \frac{k}{2}t^2\right)\right],$$

where the initial phase is denoted by ϕ_0. In this study, we aim to use sweep frequency pattern as smart jamming symbols instead of frequently used jamming model that makes use of Gaussian distributed random variables.

The main block diagram of the chirp subcarrier jamming is given in Figure 3. First, chirp generated symbols denoted by j_{ch}, are passed through the S/P conversion block. Next, FFT process is operated. The complex symbols of frequency domain are denoted by J_{ch}, which is used for subcarrier distribution (assignment). For each jamming scenario there are different subcarrier distributions. Subsequently, subcarriers are passed through IFFT and then CP portions are inserted. Output signals are denoted by j'_{ch}.

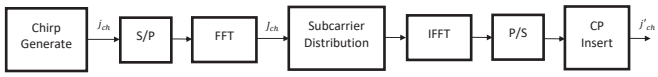

Fig. 3: Chirp subcarrier generation based OFDM jamming model.

A. Conventional Chirp Based Jamming Attacks (Chirp CoJ)

We design this type of attacks based on conventional jamming CoJ, yet signal generation aspects are alternated to chirp pattern instead of the Gaussian noise. The transmitted jamming subcarriers are located within the complete subcarrier set for $n \in \mathcal{N}$ in frequency domain and are located $k \in \mathcal{C}$ for CP in time domain. Considering the chirp jammer block diagram, J_{ch} is utilized for frequency domain, j'_{ch} is employed for time domain signals.

B. Cyclic Prefix Chirp Based Jamming Attacks (Chirp CPJ)

As indicated in the previous section, vulnerable attacks in CP partition may cause communication disruption due to tight synchronization requirements of OFDM. Hence, the Chirp CPJ attacks are designed inspired by CPJ. Considering (8), we alternate time domain symbols as $j_k = j'_{ch}(t)$ when $k \in \mathcal{C}$.

C. Pilot Tone Chirp Based Jamming Attacks (Chirp PJ)

As pointed out earlier, the effect of pilot tone jamming, Chirp based pilot tone jamming is designed similar to PJ. Even though, signal generation is differ from PJ by means of using chirp pattern. Chirp PJ attacks effect OFDM system like (9), where $J_n = J_{ch}$ is different from PJ attacks.

D. Attack Comparison

CP jamming has similar effects to barrage jamming, but it is more power efficient because the power is divided between only CP subcarriers. Pilot tone jamming achieves better results then others and it is also more power efficient, since the power is divided between pilot subcarriers. Chirp based jamming attacks achieve slightly better results then previous attacks. Due to the lower PAPR value of chirp signals, these attacks need less power then previous type of attacks. The pilot tone chirp based jamming demonstrates the highest impact scenario in this study.

V. Simulation Results

Our simulations are established considering an OFDM channel model is given in Section II. Data and pilot tones are passed through IFFT, and CP is inserted. 4-PSK and 16-QAM signals are used for data portion. Moreover, pilot tones are assigned corresponding to every 8^{th} subcarrier is a pilot tone. We use 256 point IFFT for our simulations. The length of CP is determined as 1/8 of the OFDM frame. Next, OFDM signal

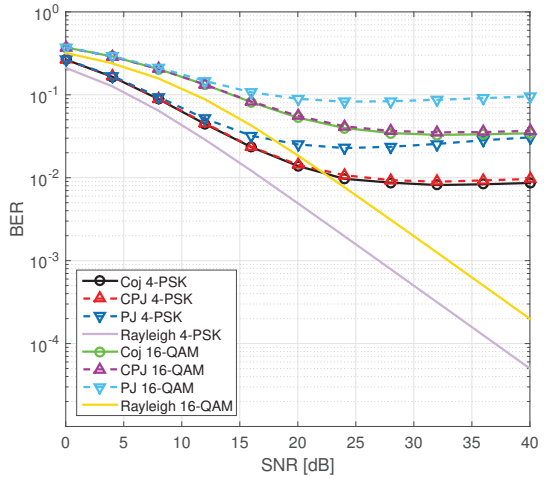

Fig. 4: BER performance while increasing SNR of three jamming attacks on OFDM with respect to 4-PSK and 16-QAM modulations.

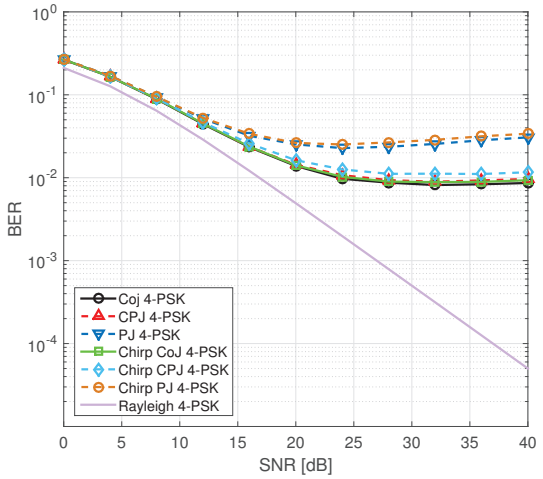

Fig. 5: BER performance while increasing SNR of three Gaussian noise based jamming attacks versus three chirp based jamming attacks on OFDM considering 4-PSK modulation.

are sent over an 8-tap random channel with AWGN. The attack signal pass through a different channel, and jammer signal is constituted using jammer model and chirp symbol jamming model, which are described in Sections III and IV, respectively. Chirp parameters of jammers are $f_0 = 0$, $f_1 = 256$ and $T = 1/512$. Received signal is equalized using the minimum mean-squared estimator. Simulations are run 10000 times for different SNR values and different jammer variances. In this study, we use jammer variances (σ_j^2) in order to quantify the intensity of the adversary attack, instead of signal-to-jammer ratio. Furthermore, each adversary attack power is normalized in time domain to get a fair comparison.

A. Performance of Existing Smart Jamming Attacks

First, we evaluate system performance under existing OFDM based smart jamming attacks. BER performances of CoJ, CPJ and PJ are given in Figure 4. An increase in the modulation order from 4-PSK to 16-QAM, increases the destructive effects of all jamming attacks significantly. We choose 0.01 for σ_j in this simulations. For instance, BER performances using 4-PSK modulation at 40 dB SNR value with CoJ, CPJ and PJ are observed as 8.643×10^{-3}, 9.656×10^{-3} and 30.66×10^{-3}, respectively. PJ types attacks are the most vulnerable attack type considering other scenarios. BER values are increased at 40 dB SNR with 16-QAM modulation, 34.33×10^{-3}, 36.73×10^{-3} and 95.74×10^{-3} for CoJ, CPJ and PJ, respectively. Moreover, according to results performances of CoJ and CPJ are close, yet CPJ has a superior performance.

B. Effect of Chirp Subcarrier Jamming Attacks

We also examine the effect of the chirp based smart jamming attacks with respect to existing smart jamming models. Figure 5 depicts, system performance considering 4-PSK modulation scheme for both three Gaussian noise based well-known attacks against three chirp based advisor attacks under the σ_j of 0.01. BER measurements in presence of chirp based attacks are given as 9.33×10^{-3}, 11.64×10^{-3} and 33.93×10^{-3} for Chirp CoJ, Chirp CPJ and Chirp PJ respectively. According to our findings, chirp based jammers decrease the communication quality more severely than Gaussian distribution based attacks. We also note that, we can observe the significant impact of Chirp PJ type jamming attacks.

C. PAPR Performance of Chirp Signal

High PAPR value is the most unfavorable impact for the transmitter side due to decrease the signal to quantization noise ratio in presence of possible clipping. As aforementioned, chirp signal has a lower PAPR value than Gaussian distributed signal. Figure 6 depicts the complementary cumulative distribution function (CCDF) values against PAPR for chirp signal and Gaussian signal. According to simulation results PAPR values of Chirp signal and Gaussian signal are approximately 3.1 dB and 10.1 dB, respectively.

D. System Performance

As we pointed out before, the system performance is demonstrated with regards to different jammer constraints, where $\sigma_j = 0.01$. Vulnerability of these jamming attack scenarios under varying σ_j is presented in Figure 7. Figure 8 demonstrates BER performance differences of OFDM system corresponding to varied σ_j and SNR values between existing Gaussian noise based attacks and Chirp based attacks, respectively. Increasing σ_j affects BER performance difference adversely. The variation between chirp CPJ and CPJ are higher than others. For example, BER differences under $\sigma_j = 1$ and 40 dB SNR are 0.025, 0.042 and 0.026 given for conventional, CP and pilot attacks respectively. Efficiency of Chirp CoJ

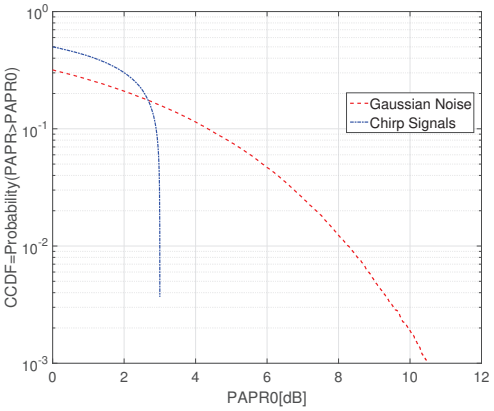

Fig. 6: PAPR of chirp waveform and Gaussian noise.

and Chirp CPJ attacks are observed as significantly higher σ_j values at any SNR, yet Chirp PJ attacks are efficient for both higher σ_j and SNR values.

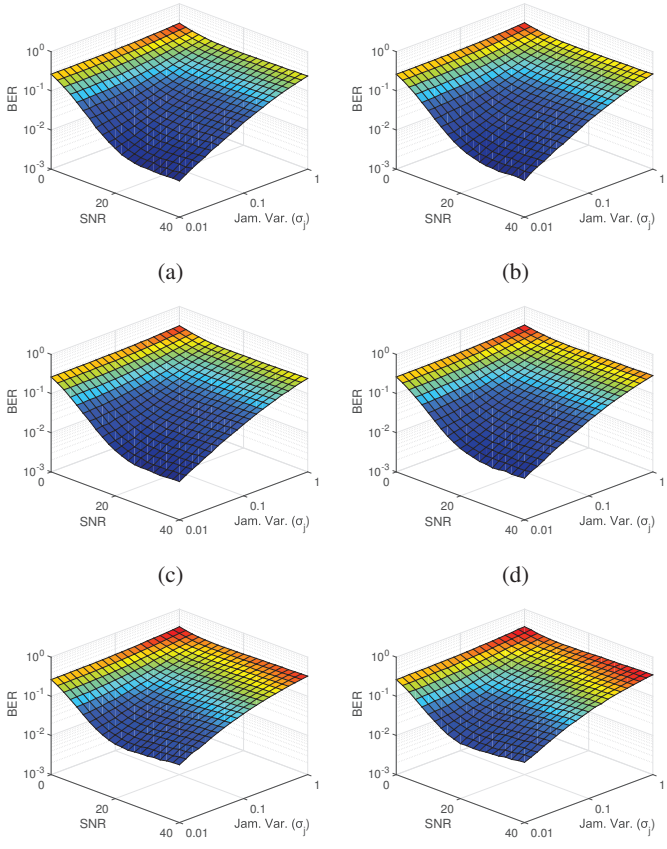

Fig. 7: BER values considering distinct jammer variances (σ_j) and SNR values of Chirp CoJ, Chirp CPJ and Chirp PJ jamming attacks. (a) CoJ, (b) Chirp CoJ, (c) CPJ, (d) Chirp CPJ, (e) PJ, (f) Chirp PJ.

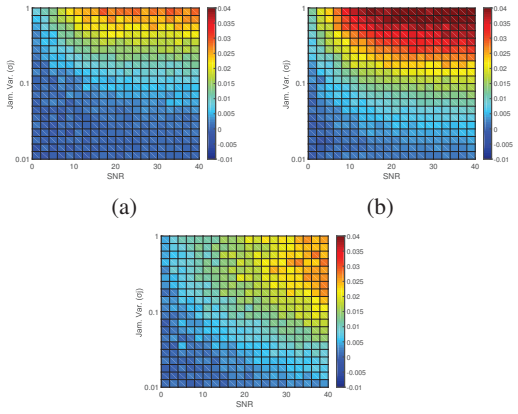

Fig. 8: BER difference of considering varying jammer variance σ_j and SNR values. (a) Difference between Chirp CoJ and CoJ, (b) Difference between Chirp CPJ and CPJ, (c) Difference between Chirp PJ and PJ.

VI. Conclusion

In this study, smart chirp subcarrier jamming attacks are proposed. The performances of OFDM systems are compared in presence of chirp based and traditional Gaussian noise jammers. According to our findings, chirp subcarrier based jamming system is effective as a jammer waveform, with a low PAPR value and a high performance degradation ratio.

References

[1] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[2] 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 Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314, 2015.

[3] A. L. Scott, "Effects of cyclic prefix jamming versus noise jamming in OFDM signals," DTIC Document, Tech. Rep., 2011.

[4] J. A. Mahal, C. Shahriar, and T. C. Clancy, "Emulated CP jamming and nulling attacks on SC-FDMA and two novel countermeasures," in *IEEE Military Communications Conference (MILCOM)*, 2015, pp. 275–280.

[5] S. Ahn, W. Lee, K. E. Lee, and J. Kang, "Deterministic pilot jamming symbol design for enhanced physical layer secrecy," in *IEEE Military Communications Conference (MILCOM)*, 2016, pp. 385–389.

[6] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

[7] H. Alakoca, H. B. Tugrel, G. K. Kurt, and C. Ayyildiz, "CP and pilot jamming attacks on SC-FDMA: Performance tests with software defined radios," in *IEEE 10th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2016, pp. 1–6.

[8] P. Flandrin, "Time frequency and chirps," in *Aerospace/Defense Sensing, Simulation, and Controls*. International Society for Optics and Photonics, 2001, pp. 161–175.

[9] R. H. Mitch, M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "Signal acquisition and tracking of chirp-style GPS jammers," in *Proc. of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)*, 2013, pp. 2893–2909.

[10] J.-J. Van de Beek, M. Sandell, P. O. Borjesson *et al.*, "ML estimation of time and frequency offset in OFDM systems," *IEEE Transactions on Signal Processing*, vol. 45, no. 7, pp. 1800–1805, 1997.

[11] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 47–54, 2016.