International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 3, June 2021, pp. 2178~2190
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i3.pp2178-2190

An enhanced OFDM light weight physical layer encryption scheme

Ahmed A. Alabdel Abass[1], Navya Prarthana Divvala[2]
[1]Department of Electrical Engineering and Department of Biomedical Engineering, University of Thi-Qar, Thi-Qar, Iraq
[2]Department of Electrical and Computer Engineering, Rutgers University, New Jersey, United State of America

Article Info

Article history:

Received May 1, 2020
Revised Dec 9, 2020
Accepted Dec 16, 2020

Keywords:

Active adversary
Alamouti scheme
iJam
OFDM phase encryption

ABSTRACT

The broadcast nature of wireless networks makes them susceptible to attacks by eavesdroppers than wired networks. Any untrusted node can eavesdrop on the medium, listen to transmissions and obtain sensitive information within the wireless network. In this paper, we propose a new mechanism which combines the advantages of two techniques namely iJam and OFDM phase encryption. Our modified mechanism makes iJam more bandwidth efficient by using Alamouti scheme to take advantage of the repetition inherent in its implementation. The adversary model is extended to the active adversary case, which has not been done in the original work of iJam and OFDM phase encryption. We propose, through a max min optimization model, a framework that maximizes the secrecy rate by means of a friendly jammer. We formulate a Zero-Sum game that captures the strategic decision making between the transmitter receiver pair and the adversary. We apply the fictitious play (FP) algorithm to reach the Nash equilibria (NE) of the game. Our simulation results show a significant improvement in terms of the ability of the eavesdropper to benefit from the received information over the traditional schemes, i.e. iJam or OFDM phase encryption.

Corresponding Author:

Ahmed A. Alabdel Abass
Department of Electrical Engineering and Department of Biomedical Engineering
University of Thi-Qar
Thi-Qar, Iraq
E-mail: ahmed-abd-h@utq.edu.iq

1. INTRODUCTION

Security in the physical layer has been investigated by many researchers, for example, in [1-8] and the references therein. Some reasons for the importance of the security at the physical layer are:

– Spoofing the signal from the wireless communication link and then breaking its security, or jamming the signal
– The encryption at the physical layer is faster than the other layers, and has the least effect on the system when changed or modified

The main themes in the physical layer security can be drawn either from the perspective of information theory and error correcting codes like in [4], or from statistical signal processing, which is mostly followed in [5-7]. In [1, 2], the approach is more likely to be a third perspective which follows a signal processing method. However, there is no real distinction among these approaches because the eavesdropper can exploit the weakness in the communication link regardless of the approach used. As a result, building a secure communication link requires building blocks from all approaches, and this is what we are trying to accomplish in this work. Additionally, with the advances going on such as the Internet of things, there is a need for light but secure communications protocols. Physical layer security protocols are light and depend only on the channel information which already has to be determined to establish a communication link.

In [1], a protocol called iJam is proposed to be used for establishing a link to share the key. The idea of iJam is to purposely jam the transmitted signal, received signal, or both at some desired locations. Jamming the transmitted signal is done in the case where the adversary, who is assumed to be passive, is capable of extracting the signal that is jammed by the receiver only. Jamming by the receiver only is the main idea of iJam. This is because, in the ideal case, the jamming is done by the receiver only at specific locations, after which the transmitter sends another copy of the same signal and the receiver jams this copy again at other locations. After jamming the two transmissions of the same signal in some specific locations, the receiver reconstructs or "stiches" the signal as shown in Figure 1.

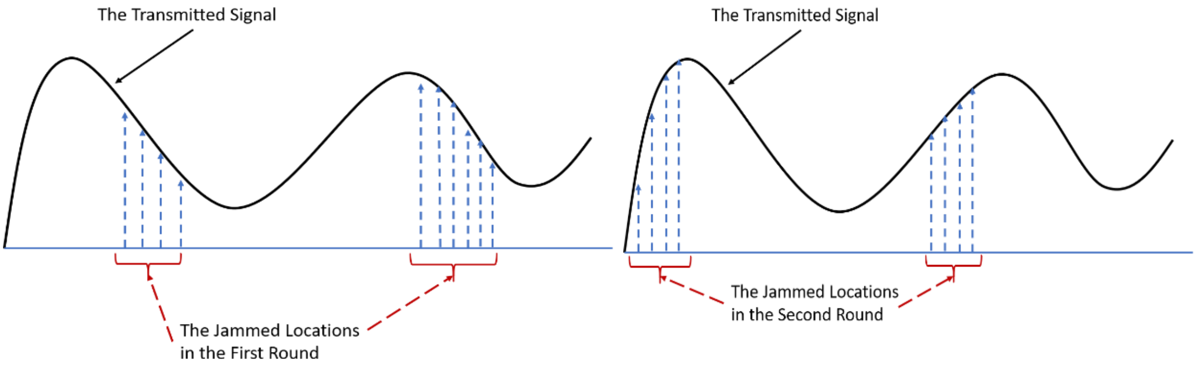

The Transmitted Signal
The Jammed Locations in the First Round
The Transmitted Signal
The Jammed Locations in the Second Round

Figure 1. iJam at work: the sender repeats its transmission; the receiver-cum-jammer randomly jams complimentary samples in the original signal and its repetition; to decode, the receiver-cum-jammer, stitches together un-jammed samples to create a clean symbol [1]

However, the simple case of iJam is location dependent. Meaning that the adversary can set up a statistical test, as derived in [1], to see which samples from the signal are jammed and which are not by measuring their variance. This testing strategy is explained as follows [1]:

$$\begin{aligned}&Pr(H_0|C_0,C_1,C) \geq Pr(H_1|C_0,C_1,C)\ if\ \ H_0\ true\\&Pr(H_0|C_0,C_1,C)\ <\ Pr(H_1|C_0,C_1,C)\ if\ \ H_1\ true\end{aligned} \tag{1}$$

where C_0 denotes the first OFDM sample received by the eavesdropper, C_1 denotes the second, H_0 denotes the hypothesis that C_0 is jammed, H_1 denotes the hypothesis that C_1 is jammed and C is the condition that one of C_0 and C_1 is jammed. Substituting probabilities of H_0 and H_1 under the Gaussian probabilities and rearranging the terms, the optimal decision can be written as [1]:

$$|C_0|^2 \overset{H0\ >}{\underset{<\ H1}{}} |C_1|^2 \tag{2}$$

This happens when the jammer is either too close or too far from the receiver. A remedy for this is proposed by a slightly complicated and time inefficient mechanism which is basically built by jamming the signal at the transmitter and at the receiver. This is done with a lot of repetitions. The details are shown in [1]. On the other hand, the authors in [2], proposed that the encryption can be done based on an OFDM property of being sensitive to phase noise. It is well known that there are two main problems in OFDM, phase noise and peak to average power ratio "PAPR". The phase noise causes the loss of the orthogonally among the subcarriers. The PAPR results from non-linearity of the amplifier which is because each OFDM time symbol is a linear combination of other frequency domain symbols and sometimes this sum is outside of the linear operation region of the amplifier which results in the signal being clipped. The basic block diagram for OFDM modulator is shown in Figure 2. In the receiver side, the reverse modulation operation takes place. In the classical encryption schemes, ciphering is done before the symbol mapping stage. The new approach followed in [2] is to do the ciphering after the IFFT stage at the transmitter and before it at the receiver. Figure 3 shows the encryption process. The decryption is done in reverse.

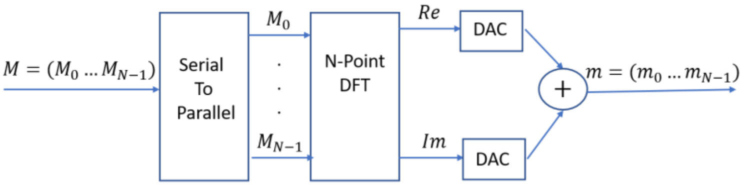


Figure 2. Baseband OFDM transmitter

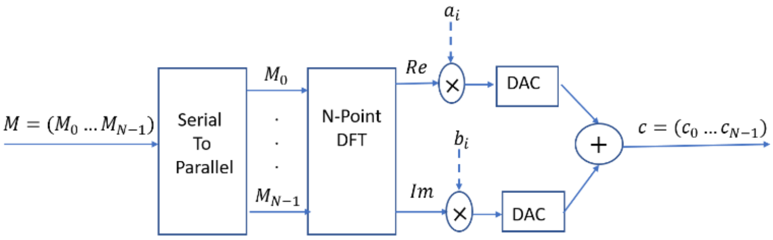


Figure 3. OFDM Encryption [2]

Equations (3), (4), (5) and (6) describe the classical and the encrypted OFDM symbols. For (3) and (4), the frequency domain symbols $M = (M_0 ... M_{N-1}) \in C^N$ are modulated symbols to be transmitted. The number of values M_k can take is 2^r, where r is number of bits per symbol and it will depend on the underlying modulation scheme. i.e., r = 2 for QPSK and r = 4 for 16-QAM. Their corresponding baseband time domain OFDM symbol $m = (m_0 \dots m_{N-1})$obtained by performing inverse discrete Fourier transform (IDFT) on M as

$$m_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} M_k e^{j2\pi ik/N}, \ \{i, k\} \in \{0,1, \dots, N-1\} \tag{3}$$

In general, m_i is complex valued. By simply applying the discrete Fourier transform (DFT), correct modulated symbols can be recovered as

$$M_k = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} m_i e^{-j2\pi ik/N}, \ \{i, k\} \in \{0,1, \dots, N-1\} \tag{4}$$

The encryption process that is described in [2] uses two pseudo-random sequences acting on the real, a_i, and imaginary, b_i, parts of time domain data symbols m_i from (3). The process is described by the following equation

$$c_i = Re\{m_i\} \times a_i + j\ Im\{m_i\} \times b_i \tag{5}$$

It has to be mentioned that choosing OFDM in [1, 2] to do the iJam and the phase encryption over other signaling schemes such as BPSK is due to the nature of the OFDM signal. An OFDM symbol is a summation of N- random variables, where N is the size of FFT/DFT which is usually > 64. According to the central limit theorem, this summation is a Gaussian random variable so in the case of adding the noise in the iJam in the correct locations, the adversary will not be able to reconstruct the signal, because the signal has a Gaussian nature. However, this cannot be achieved with BPSK for example. In BPSK, as shown in [1], the adversary can recover most of the jammed symbols.

2. PROBLEMS WITH iJam AND OFDM PHASE ENCRYPTION

In this section we briefly review the drawbacks for the originally proposed iJam [1] and OFDM phase encryption [2]. These techniques are simple and powerful, but they have some problems that can be exploited by the adversary.

2.1. Problems with iJam

One of the problems with iJam is the location dependence, meaning that the adversary can change its location to gain a clean, unjammed, version of the transmitted signal. To solve this issue, the authors in [1] proposed a protocol involving joint jamming between the transmitter and the receiver. However, even with the solution proposed in [1], iJam still depends on the location of the adversary. Another point mentioned in [1] is that OFDM has to have a cyclic prefix "CP" which usually consists of a part of the symbol re-appended to its end for the sake of combating the inter-symbol interference. The CP represents exposed information. In [1], the author proposed jamming the CP too, but since the CP requires the first or the last 25% of the symbol to be re-appended, iJam has to always jam the same portion of the OFDM symbol corresponding to the CP. As a result, the adversary can deduce the jammed or unjammed locations by looking to the CP. This is in addition to the assumption that the adversary is passive, which is used in both proposals [1, 2].

2.2. Problems with OFDM phase encryption

The authors in [2] have shown that their algorithms break under known plaintext attack, which is expected because the encryption is a one-time pad cipher [8]. Another problem is that they are assuming that the transmitter and the receiver know the values of the encryption keys. In this work, we tackle only the first problem. The second problem of the key-sharing is not in the scope of this paper.

3. THE PROPOSED PHYSICAL LAYER ENCRYPTION SYSTEM

In this part we explain two mechanisms to deal with the adversary that can be active or passive. In this first part, we explain how to deal with a passive adversary. In the second part, we assume an active adversary that can have more abilities to avoid the iJam protocol, the OFDM phase encryption, or both through modeling the problem as a max min optimization problem that is a Zero-sum game model.

3.1. The proposed scheme for a passive adversary

By combing both the OFDM phase encryption and the simplest form of iJam (where the receiver only jams the received signal), we can build a more secure link. This can be done either directly or with enhanced spectral efficiency. However, there still a possibility of an attack which occurs when the iJam noise is not high enough to distort the symbols and there is a known plain text. Although the feasibility of such an attack is low, our proposed scheme is still stronger than both protocols individually, and simpler than the iJam alone.

3.1.1. Direct combining

OFDM phase encryption method does not suffer from the location dependency problem like the iJam method, the adversary will not be able to deduce which symbols were jammed by constructing the statistical test above. The adversary can only detect symbols that are jammed by receiver and these symbols are already encrypted. The drawback of this method is the loss of bandwidth, because the signal has to be transmitted twice. The block diagram for this scheme is shown in Figure 4 where the noise is an AWGN.

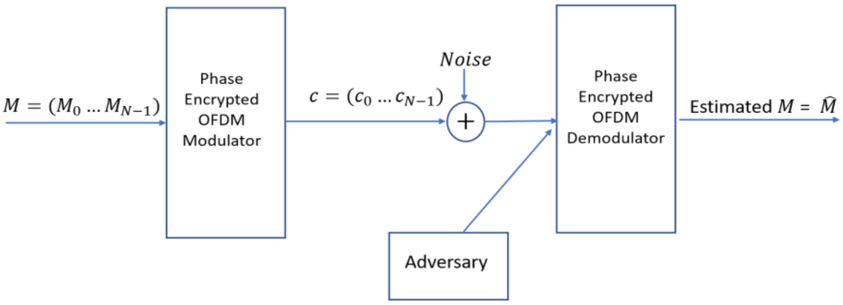

$M = (M_0 \dots M_{N-1})$
Phase Encrypted OFDM Modulator
$c = (c_0 \dots c_{N-1})$
$Noise$
+
Phase Encrypted OFDM Demodulator
Estimated $M = \hat{M}$
Adversary

Figure 4. Baseband phase encrypted OFDM transceiver

3.1.2. The bandwidth efficient combining scheme

iJam scheme requires the original signal and its copy to perform the jamming and the stitching at the receiver. Meaning that for two transmission periods, the transmitter sends the same signal. This lowers the efficiency of the system by half. A simple solution is to use a system with multiple antennas or any other spatial multiplexing method. In this paper, we use the simplest method to do this is which is the Alamouti transmission scheme [9]. Simply put, the Alamouti scheme is a method of processing the transmitted signal such that it is easy for the receiver to build a set of simultaneous equations and solve them to extract the original transmitted signal. To illustrate this concept, we will consider the case of two transmitting antennas and one receiving antenna. Furthermore, even the case of two transmitting antennas and two receiving antennas can be converted to the above case by turning one of the antennas off at the reception to lower the operating cost (for example to reduce the power). The proposed transceiver block diagram is shown in Figure 5. At the first time instant, the first symbol is transmitted from Antenna 1, and the conjugate of the second symbol is transmitted from Antenna 2. At the second time instant, the second symbol is transmitted from Antenna 1, and the negative conjugate of the first symbol is transmitted from Antenna 2. The purpose of the conjugations and negations is to make the detection easier at the receiver. Specifically, this formulation provides an algorithm to build a system of two simultaneous equations with two variables. The details of transmission and detection can be found in [9] and are out of the scope of this work. At the receiving side, the receiver jams the received signal as proposed in [1], but also has to compute the inverse of these negation and conjugation operations.

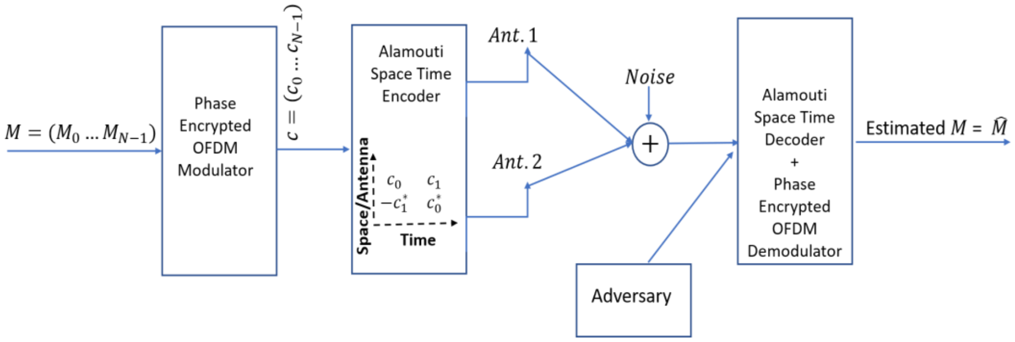

$M = (M_0 \dots M_{N-1})$
Phase Encrypted OFDM Modulator
$c = (c_0 \dots c_{N-1})$
Alamouti Space Time Encoder
Space/Antenna
c_0 c_1
$-c_1^*$ c_0^*
Time
$Ant. 1$
$Ant. 2$
$Noise$
$+$
Adversary
Alamouti Space Time Decoder + Phase Encrypted OFDM Demodulator
Estimated $M = \hat{M}$

Figure 5. The new two-branch transmit diversity Alamouti scheme with two transmit antennas

3.2. The proposed scheme for an active adversary

The above schemes are designed for the case of a passive adversary that is only able to receive the signal and to perform calculations on it. As a result, if the signal is encrypted, it should be difficult for the adversary to extract something useful from it. However, the adversary can be active and act strategically. One possibility is that the adversary can change its location to get a cleaner version of the transmitted signal exploiting the receiver limited jamming power ability, since the power is always a resource that has to be used efficiently. For the sake of clarity, the active adversary scenario is shown in Figure 6. The desired signals from the transmitter to the receiver are plotted in solid lines and the channels are marked as $\{h_{rt}\}$, $and\ \{r, t\} \in \{1,2\}$ where r means the receiving antenna and t means the transmitting antenna. The jamming signal and the eavesdropped signal are denoted by differently dotted lines. The channels $g_1\ and\ g_2$ are the eavesdropped signals channel coefficients between the transmitter and the adversary, while g_3 is the channel coefficient between the friendly jammer and the adversary. Finally, $g_4\ and\ g_5$ are the channel coefficients between the friendly jammer and the receiver. Note that we assume the adversary and the jammer have only one antenna for simplicity. This assumption is valid because the nature of the space time receiving algorithm that collects the signal from different channels and combines them. The adversary intention of getting a cleaner version of the transmitted signal can be for many reasons, such as storing the encrypted message to process it later by more advanced decryption tools or if the adversary has compromised some of the phase encryption keys. In this case the adversary is active by making moves to avoid the jamming from the receiver. This situation can still be handled by the concept of using, hiring, a friendly jammer which is an entity used by the transmitter and the receiver, interchangeably called Tx-Rx pair, to establish a secure communication link by jamming the transmitted signal. In this case, the signal will be jammed at the intended receiver as well as the adversary. The adversary will not be able to benefit from the eavesdropped information even if we consider the case of compromised phase encryption keys. However, this scenario is proposed for sensitive information transmission and it depends on the transmitter-receiver pair to judge if such technique is needed or not. On the other hand, the adversary can try to fool the transmitter to force it to jam the signal which leads to disrupting the communication link and no one will get useful information. This strategic interaction between the Tx-Rx pair and the adversary can be modeled using game theoretic models and in particular Zero-sum games. A game G is defined by a set of players N, a set of strategies that players use S, and a set of the players' payoffs or payoff (utility) functions $U,$ and expressed as $G(N, S, U)$. In this paper, $N = \{Adversary, Transmitter - Receiver\ Pair\} = \{E, Tx\}$. The strategy set for the adversary is $S_A = \{Change\ Location, Do\ not\ Change\ Location\} = \{s_1, s_2\}$. Each strategy is chosen with a probability, or has some preference, $\{y_1, y_2\} \in \mathcal{Y} \in [0,1]$. The strategy set for the Transmitter-Receiver pair is $S_{Tx} = \{Hire\ a\ Friendly\ Jammer, Do\ not\ Hire\ a\ Friendly\ Jammer\} = \{H-On, H-Off\}$, and each strategy is chosen with a probability, or has some preference, $\{z_1, z_2\} \in \mathcal{Z} \in [0,1]$. In this paper, the Zero-sum game formulation is justified, because the adversary wants to cause as much damage as possible to the transmitter. This damage can be by eavesdropping the signal to cryptanalysis it, maybe later, or it can damage the transmitter-receiver pair by fooling them to, unnecessarily, use a friendly jammer that adds noise to the signal and degrades the signal quality at the receiver. This is a good strategy to use if the adversary does not have the abilities to cryptanalysis the signal. As a result, we can assume that the payoffs of the adversary are the losses of the transmitter-receiver pair and vice versa. It is also possible to reformulate this scenario as a non-Zero-sum game by adding penalties to both parties, such as some penalty if the adversary changes its location or giving the adversary only a possible set of locations to move to with each of these locations has its own rewards and costs.

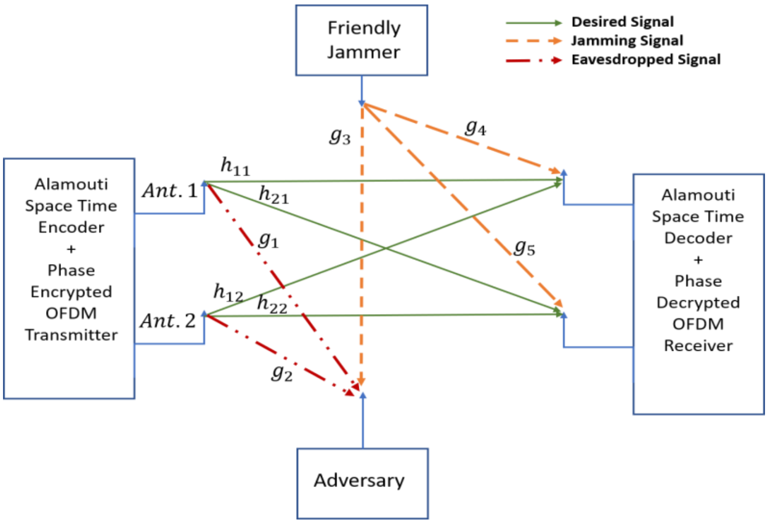


Figure 6. The active adversary scenario with the friendly jammer

However, although this may be an interesting to investigate in details, we abstain from doing it in this paper for the following reasons: i) All non-Zero-sum games can be transformed to Zero-sum games by using appropriate transformations that preserves the game solution which is the Nash equilibria, NE [10], ii) Such analysis needs space and may destruct the reader from the main contributions in this paper, which are the introducing of a lightweight physical layer crypto system and analyzing some of the challenges that face it using different mathematical and simulation tools. However, the extension to the non-Zero-sum games can be tackled in future works. We consider for the payoff function the benefits captured by the secrecy rate R_s, as given in [4], and the cost of using the friendly jammer that is assumed to be a function of the jamming power, i.e., $f(P_J)$. The jamming cost $f(P_J)$ can be a linear or any other monotically increasing function of the jamming power to reflect the fact that hiring a friendly jammer when it is not necessary creates some penalty and this can be a goal to be achieved by the adversary to disturb the communication link. The jamming power is also present in the secrecy rate function. In particular, the transmitter wants to maximize U, while the eavesdropper tries to minimize it. The utility function is defined as

$$U = R_s - f(P_J) \tag{6}$$

The secrecy capacity is defined as [4]

$$R_s = \left(C_{RX}\left(\frac{hP}{g_{45}P_J + \sigma_{Rx}^2}\right) - C_E\left(\frac{g_{12}Px}{|g_3|^2 P_J + \sigma_E^2}\right)\right)^+ \tag{7}$$

where $(Q)^+ = max\{0, Q\}$ and the channel rate $C_O\left(\frac{Q}{R}\right) = ln\left(1 + \frac{Q}{R}\right)$, $O = \{RX, E\}$, P is the transmitted information power, $h = \sum_{i,j=1}^{2} |h_{ij}|^2$, $g_{45} = |g_4|^2 + |g_5|^2$, $g_{12} = |g_1|^2 + |g_2|^2$, σ_{Rx}^2 is the AWGN power at the receiver, σ_E^2 is the AWGN power at the adversary, and $x \in [0,1]$ is the portion of the compromised keys. Assume there is a way to avoid the reply attack by placing some sort of ordering that is protected, so as to cancel this attack. Jamming the signal by adding noise to it can be achieved by making the transmitter believe that the adversary has some compromised keys which leads to added noise that is unknown to the receiver, this attack can successfully degrade the signal quality and increase the bit error rate, "BER", of the received signal and lower the link capacity. Next, we express the game in the normal form shown in Table 1. The row player E gets a payoff a_1, to be explained later, if uses strategy s_1 against the column player Tx the employs a helper jammer strategy $H - On$, and so on. The table entries $a_i,\ i \in \{1,2,3,4\}$ are derived from (6) and (7) as shown below in (8) - (11).

$$a_1 = -\left(\left(C_{RX}\left(\frac{hP}{g_{45}P_J+\sigma_{Rx}^2}\right) - C_E\left(\frac{g_{12}Px}{|g_3|^2P_J+\sigma_E^2}\right)\right)^+ - f\left(P_J\right)\right), \quad (8)$$

$$a_2 = -\left(C_{RX}\left(\frac{hP}{\sigma_{Rx}^2}\right) - C_E\left(\frac{g_{12}Px}{\sigma_E^2}\right)\right)^+, \quad (9)$$

$$a_3 = -\left(C_{RX}\left(\frac{hP}{g_{45}P_J+\sigma_{Rx}^2}\right) - f\left(P_J\right)\right), \quad (10)$$

$$a_4 = -C_{RX}\left(\frac{hP}{\sigma_{Rx}^2}\right) \quad (11)$$

Table 1. The normal form of the proposed Zero-sum game

Tx E	$H - On$ $w.p.z_1$	$H - Off$ $w.p.z_2$
s_1 $w.p.y_1$	$a_1, -a_1$	$a_2, -a_2$
s_2 $w.p.y_2$	$a_3, -a_3$	$a_4, -a_4$

The pure strategy, is a strategy chosen with probability 1 or a pure NE, but it is not always guaranteed to exist. However, all games have a solution in the mixed strategies which is mixed saddle point NE or mixed NE for simplicity. Meaning that each strategy is chosen with a certain probability. One way to find the NE of the game is to formulate an optimization problem for each player. In particular the NE can be found by solving the following linear programs, $LP1$ and $LP2$. Let the payoff matrix A represented as in (12),

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \quad (12)$$

Define the value of the game as $\gamma = y^TAz$, where $\boldsymbol{y^T} = [y_1, y_2]$, $\boldsymbol{z} = [z_1, z_2]^T$**.** The adversary wants to minimize γ over its set of strategies while the transmitter tries to maximize γ over its set of strategies. Meaning that they want to solve the following $min\ max$ optimization problem,

For the adversary: $min_{y \in \mathcal{Y}}\, max_{z \in \mathcal{Z}}\ y^TAz$, (13)

while for the transmitter: $max_{z \in \mathcal{Z}}\, min_{y \in \mathcal{Y}}\ y^TAz.$ (14)

As mentioned above these equations can be formulated as linear programs which can be efficiently solved using many software packages [11].

$$\begin{aligned} &LP1{:}\ The\ adversary\ problem\ \ min\ \gamma \\ &\quad subject\ to{:}\ y \geq 0 \\ &\qquad\qquad 1y = 1 \\ &\qquad\qquad A^Ty \leq \gamma 1 \end{aligned} \quad (15)$$

$$\begin{aligned} &LP2\text{: } The\ transmitter\ problem \quad max\ \gamma \\ &\quad subject\ to\text{: } z \geq 0 \\ &\qquad\qquad 1z = 1 \\ &\qquad\qquad Az \geq \gamma 1, \end{aligned} \tag{16}$$

where $1 = [1,1]$ in (15) and (16).

The players can solve this game and reach the NE by using a learning algorithm without the need to a specialized solver. One such algorithm that is proved to converge to the NE is the fictitious play (FP) [12]. In FP, each player makes independent, fictitious assumptions, about the other player choices and updates their preferences according to (17) and (18) below,

$$\rho_i^{(k+1)} = \rho_i^{(k+1)} + \tfrac{1}{k}\left(\nu_i^{(k)} - {\rho_i}^{(k)}\right),\ i \in N, \tag{17}$$

$$\nu_i^{(k)} = \left[\nu_i^{(k)}\left(u(s_1, \mathcal{S})\right), \nu_i^{(k)}\left(u(s_2, \mathcal{S})\right), \ldots, \nu_i^{(k)}\left(u\left(s_{|\mathcal{S}|}, \mathcal{S}\right)\right)\right].$$

$$k\ is\ the\ iteration\ number\ and\ \nu_i^{(k)}\left(u(s_l, \mathcal{S})\right)$$

$$\nu_i^{(k)}(s_l) = \begin{cases} 1, & if\ I_1\ holds \\ 0, & otherwise, \end{cases} \tag{18}$$

$$I_1 = u^{(k)}(s_l, \mathcal{S}) = \max\nolimits_{\boldsymbol{s} \in \boldsymbol{S}} u_i\left(s_l, \boldsymbol{\rho_{-i}}(k-1)\right).$$

Equation (17) means that at the kth iteration, the ithplayer chooses the strategy s_l that maximizes her payoff and this assigns a value of 1 to $\nu(s_l)$ and 0for the other strategies. When substituting in (17), the strategy with $\nu(s_l) = 1$ gets higher probability of being chosen in the next iteration, since $\nu_i^{(k)} - {\rho_i}^{(k)} \geq 0$, while other strategies with $\nu(.) = 0$ get $\nu_i^{(k)} - {\rho_i}^{(k)} < 0$which reduces their chances of being chosen in the next iteration. It can be seen from (16) and (17) that FP learning algorithm depends on the local information in that each player has and there is no need to coordinate between players to exchange information which applies to the scenario in this paper where the transmitter cannot exchange information with the adversary.

3.3. Security analysis

In this section we discuss some common attacks against the proposed physical layer encryption scheme for the case of passive adversary. The passive adversary is the general case, because the aim of the friendly jammer is to turn the active adversary to a passive.

3.3.1. Statistical attack

It is shown in [1] that iJam by itself can be deciphered by statistical attacks because it is a location dependent. However, by adding the phase noise, the attacker sees only almost AWGN noise. The immunity of the phased encrypted OFDM is shown in [2].

3.3.2. Compromised keys attack

In [2], it is shown that the phase encrypted OFDM system experiences some problems with this type of attack. However, by introducing iJam, this type of attack is weakened due to the ability of iJam to reduce the leaked signal quality through jamming.

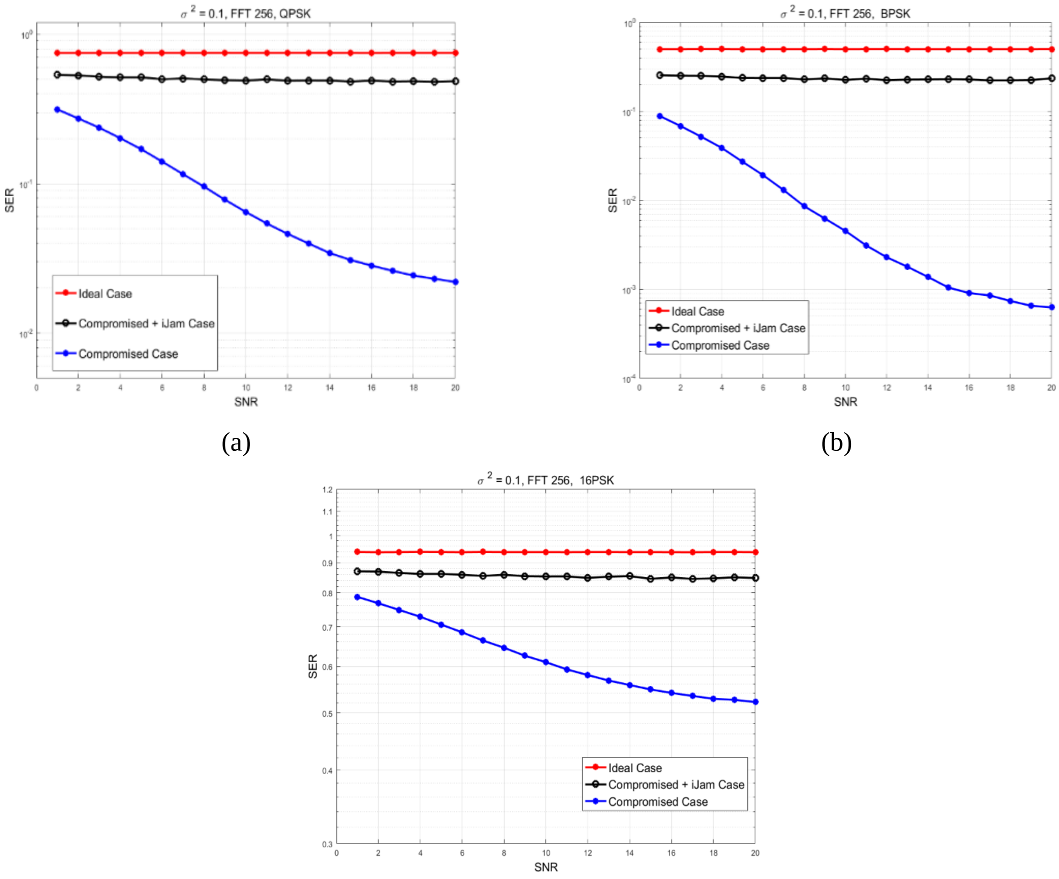
3.3.3. Other attacks

The weakness in both protocols arises for lower modulation schemes like BPSK. However, the proposed scheme in this work lowers the probability of this type of attack. From a theoretical point of view [8], there is no easy way to deduce the relation between the message and its ciphered version because the proposed scheme adds noise to both the phase and the magnitude of the message. By doing this, each symbol has equal probability of occurrence, and this is desirable from a security point of view. Another problem is the initial keys distribution, and one way to solve it is to assume that these keys are distributed through a secure channel or embedding them at the modulator and the demodulator at the installation.

4. SIMULATION RESULTS

The simulation is divided into two parts. The first part, Figures 7, 8 and 9, deals with a passive adversary, while the second part, deals with an active adversary. We use the following parameters to perform our simulations: OFDM FFT sizes 64 and 256, the modulation types BPSK, QPSK, and 16 PSK, the additive white Gaussian noise (jammer noise) with zero mean and variances 0.1, 0.5 and 1 generated according to the procedure described in [13, 14] compromised keys, and MATLAB 2016. In the first part, in Figures 7-9, there are three curves in each figure. The first one entitled Ideal Case represents the case where there are no compromised keys. The second one entitled Compromised + iJam Case represents the case of twenty compromised phase encryption keys of the proposed system that combines iJam with phase encryption. The third curve entitled Compromised Case represents the case of using only phase encryption with twenty compromised keys. There is an improvement achieved by using a combination of iJam and OFDM phase encryption for the case of compromised keys. The first observation from Figures 7-9 is a noticeable improvement in the case of lower modulation schemes, BPSK and QPSK, even when there are compromised keys. In the case of 16 PSK, there isn't much improvement. This is because 16 PSK is more susceptible to noise than BPSK and QPSK. The amount of the AWGN noise plays a vital role in increasing the security of the communication link which motivates the need of the friendly jammer. It is also because the ratio of the compromised keys is less.

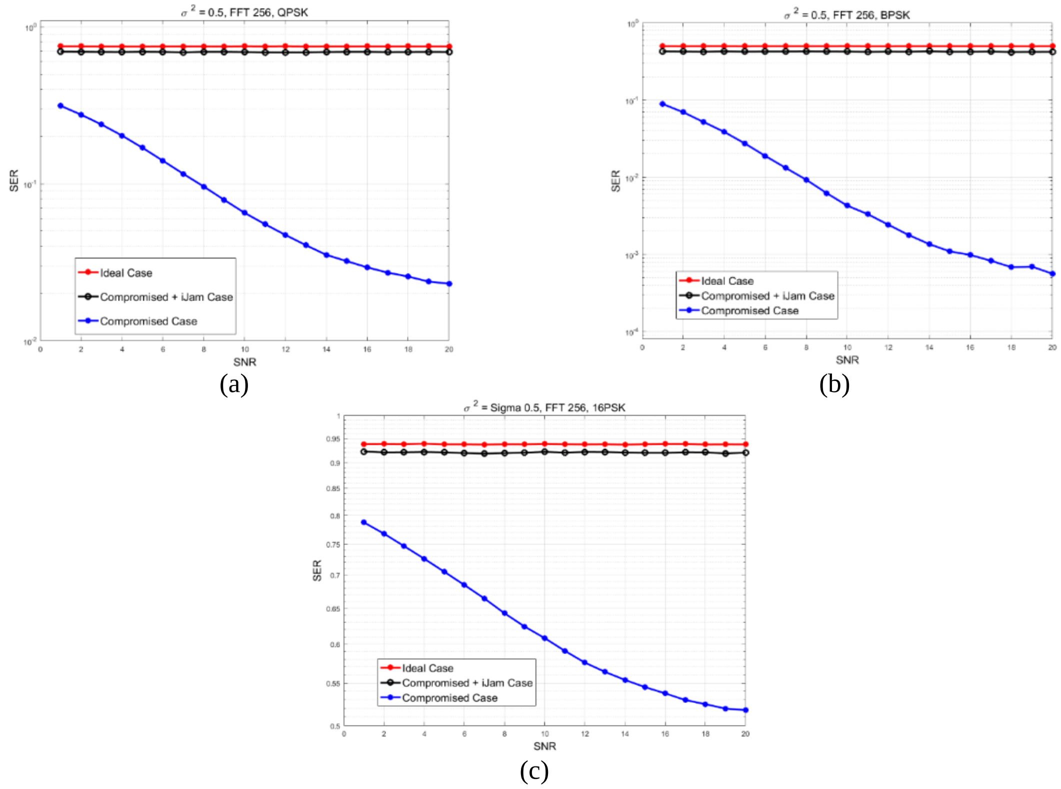
The second part of the simulation is shown in Figure 10, where it shows an example of the convergence to the NE using the FP algorithm and the payoff for each player. It can be seen that the adversary is better to use the first strategy which is to change its location to eavesdrop the communication between the Tx-Rx pair although the Tx-Rx pair is using a friendly jammer. This is only an example to the convergence to the NE which happens in this case to be a pure NE that is $\{s_1, H - On\}$. It should be mentioned that the players are started from some initial points or beliefs and then updated their strategies. The NE can change depending on the players' beliefs or preferences that are assigned to their strategies. The final observation is the amount of payoff that each player is getting in Figure 10-b and Figure 10-c which is approximately -0.91 for the adversary and 0.91 for the Tx-Rx pair which reflects the Zero-sum nature of the game.



(a) (b)

(c)

Figure 7. The BER for the following parameters 7a - $\sigma^2 = 0.1$, FFT 256, QPSK, 7b - $\sigma^2 = 0.1$, FFT 256, BPSK, and 7c - $\sigma^2 = 0.1$, FFT 256, 16PSK

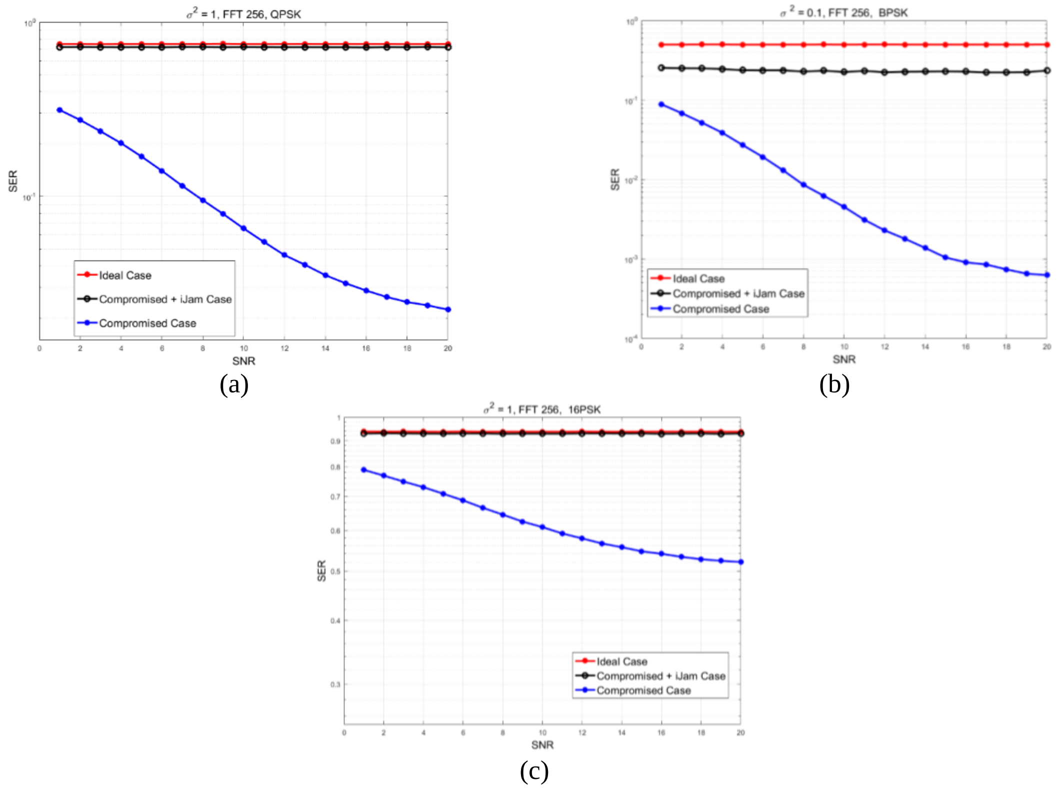


(a)

(b)

(c)

Figure 8. The BER for the following parameters; (a) – $\sigma^2 = 0.5$, FFT 256, QPSK, (b) - $\sigma^2 = 0.5$, FFT 256, BPSK, and (c) - $\sigma^2 = 0.5$, FFT 256, 16PSK

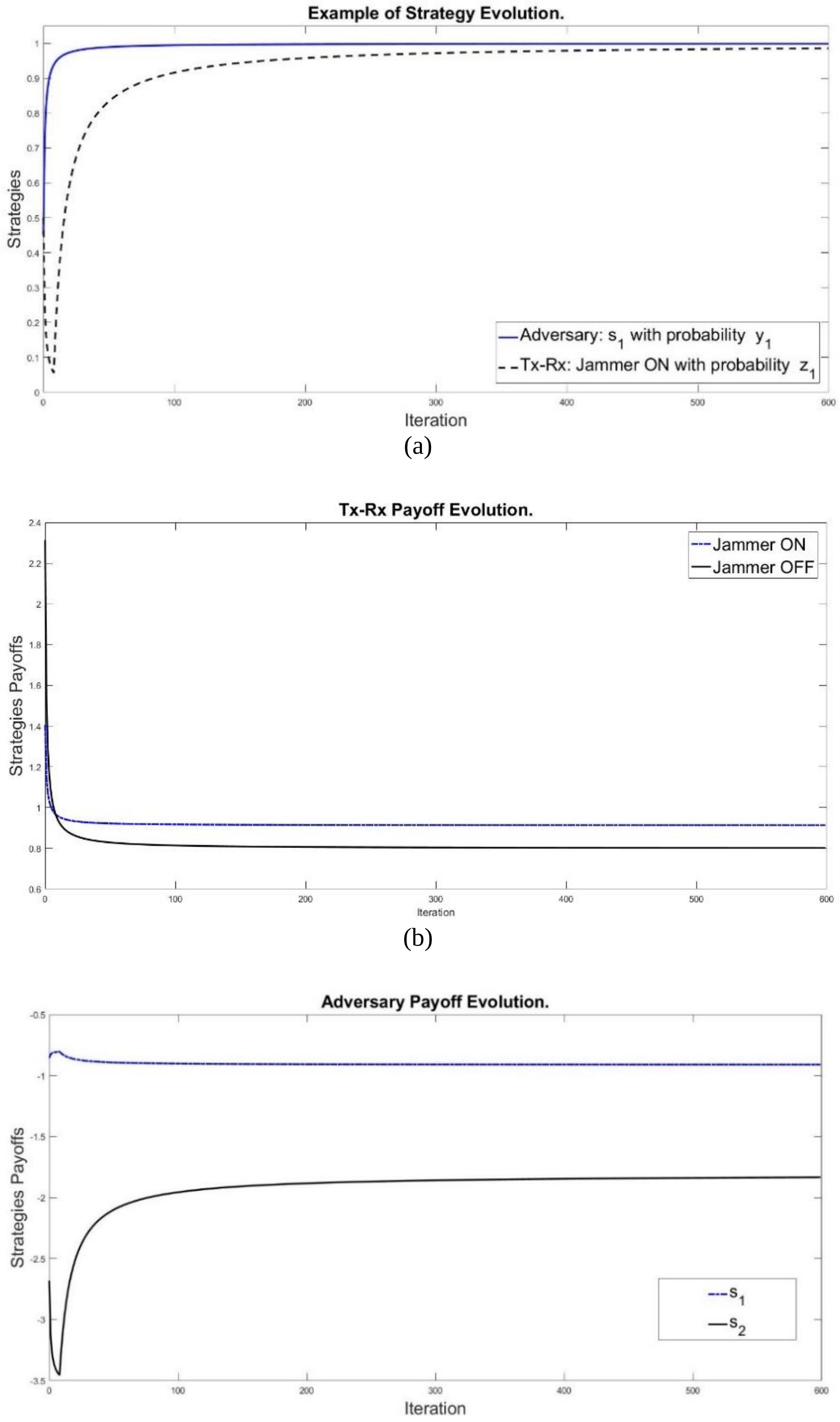


(a)

(b)

(c)

Figure 9. The BER for the following parameters; (a) – $\sigma^2 = 1$, FFT 256, QPSK, (b) $\sigma^2 = 1$, FFT 256, BPSK, and (c) - $\sigma^2 = 1$, FFT 256, 16PSK



(a)

(b)

(c)

Figure 10. The results of the game theoretic modeling where, (a) Strategies evolution, (b) The Tx-Rx pair payoff, (c) The adversary payoff

5. RELATED WORK

This section is intended to give a glimpse of the related work in the literature to our work. It is not meant to be comprehensive by any means. The work on iJam is proposed in [1]. The OFDM phase noise is based in the work in [2]. The work in physical layer security based on signal processing methods is a growing and mature research area, for example [4-9] and [15] for a comprehensive exposure to the material. In [4-9] different signal processing algorithms are presented to maximize the secrecy rate at the physical layer. Along the same line, but with a different objective is the work on secret communications, for example [16]. In secret communications, the transmitter-receiver pair wants to hide the communication activity from the adversary which we believe that our work can be modified to achieve this objective too. On the other hand, game theoretic models have been used extensively to address security related problems [17]. Noncooperative games, for example, are used to model the jammer-user interaction through choosing the optimal transmission power level as in [18-20]. Another type of game models, namely evolutionary games are used to model the cooperation among selfish users to combat jamming attacks [21-22]. Combating active jammers, or smart jammers, is addressed by Stackelberg games in [23-25], where the transmitter-receiver pair hire a friendly jammer and set a price for jamming. A cooperative jamming game model under uncertainty is proposed in [14]. Finally, Zero-sum games are used extensively to model the transmitter-jammer behavior under mutual information as a metric, for example [26]. A closed form expression for a Zero-sum jamming game is given in [27].

6. CONCLUSION

Wireless networks are more susceptible to attacks by eavesdroppers than wired networks where any compromised node can eavesdrop on the medium, listen to transmissions and obtain sensitive information within the wireless network. In this paper, we proposed a technique to prevent an eavesdropper from gaining any secure information from the system. We proposed a new modified mechanism that combines the advantages of two techniques namely iJam and OFDM phase encryption. Our modified mechanism made the iJam more bandwidth efficient by using Alamouti scheme to take advantage of the repetition inherent in its implementation. We extended the adversary model here to the active adversary case, which has not been done in the original work of iJam and OFDM phase encryption. We proposed, through a max min optimization model, a framework that maximizes the secrecy rate by means of a friendly jammer. We formulated a Zero-sum game that captured the strategic decision making between the transmitter receiver pair and the adversary. We apply the FP learning algorithm to reach the NE. Our simulation results showed a significant improvement in terms of the ability of the eavesdropper to benefit from the received information over the traditional schemes, i.e. iJam or OFDM phase encryption.

REFERENCES

[1] S. Gollakota, and D. Katabi, “iJam: Jamming Oneself for Secure Wireless Communication,” *Computer Science and Artificial Intelligence Laboratory Technical Report,* pp. 1-13, 2010.

[2] F. Huo, and G. Gong, “A New Efficient Physical Layer OFDM Encryption Scheme,” *IEEE Conference on Computer Communication (INFOCOM),* Toronto, ON, 2014, pp. 1024-1032.

[3] R. Bassily, et al., “Cooperative security at the physical layer,” *IEEE Signal Processing Magazine,* vol. 30, no. 5, pp. 16-28, Sep. 2013.

[4] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Using the Physical Layer for Wireless Authentication in Time-Variant Channels,” *IEEE Transactions on Wireless Communications,* vol. 7, no. 7, pp. 2571-2579, 2008.

[5] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, and Y. Shah, “Exploiting the Physical Layer for Enhanced Security,” *IEEE Wireless Communications,* vol. 17, no. 5, pp. 63-70, October 2010.

[6] L. Xiao, et al., “PHY-Authentication Protocol for Spoofing Detection in Wireless Networks,” *IEEE Global Telecommunications Conference GLOBECOM,* Miami, FL, 2010, pp. 1-6, 2010.

[7] W. Trappe and L. Washington, “Introduction to Cryptography with Coding Theory,” *Second Edition,* 2006.

[8] X. He, et al., “Is Link Signature Dependable for Wireless Security?,” *Proceedings IEEE INFOCOM, Turin, 2013, pp. 200-204.*

[9] S. M. Alamouti, “A Simple Transmit Diversity Technique for Wireless Communications,” *IEEE Journal on Select Areas in Communications*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.

[10] T. Basar and G. J. Olsder, “Dynamic Noncooperative Game Theory,” *SIAM,* vol. 200, 1995.

[11] J. P. Hespanha, “Noncooperative game theory: An introduction for engineers and computer scientists,” *Princeton University Press,* 2017.

[12] G. W. Brown, “Iterative solution of games by fictitious play,” *Activity analysis of production and allocation,* vol. 13, no. 1, pp. 374-376, 1951.

[13] J. G. Proakis, M. Salehi, and G. Bauch, “Contemporary communication systems using MATLAB,” *Nelson Education,* 2012.

[14] Xu, Zhifan, and Melike Baykal-Gürsoy, “A Cooperative Jamming Game in Wireless Networks under Uncertainty,” *16th EAI International Conference on Security and Privacy in Communication Networks*, 2020.

[15] Bloch, Matthieu, and Joao Barros, “Physical-layer security: From information theory to security engineering,” *Cambridge University Press,* 2011.

[16] Negi, Rohit, and Satashu Goel, “Secret communication using artificial noise,” *IEEE vehicular technology conference,* vol. 62, no. 3, 2005, pp. 1906-1910.

[17] T. Alpcan and T. Basar, “Network security: A decision and game-theoretic approach,” *Cambridge University Press,* 2010.

[18] Y. E. Sagduyu, R. Berry, and A. Ephremides, “Mac games for distributed wireless network security with incomplete information of selfish and malicious user types,” *The Int. Conf. on Game Theory for Networks,* Istanbul, 2009, pp. 130-139.

[19] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Bas¸ar, “Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach,” *Military Communications Conference,* Baltimore, MD, 2011, pp. 119-124.

[20] A. Garnaev and W. Trappe, “The eavesdropping and jamming dilemma in multi-channel communications,” *The International Conference on Communications (ICC),* Budapest, 2013, pp. 2160-2164.

[21] A. A. A. Abass, et al., “Evolutionary game theoretic analysis of distributed denial of service attacks in a wireless network,” *The Annual Conference on Information Science and Systems (CISS),* Princeton, NJ, 2016, pp. 36-41.

[22] G. Jiang, S. Shen, K. Hu, L. Huang, H. Li, and R. Han, “Evolutionary game-based secrecy rate adaptation in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.

[23] D. Yang, J. Zhang, X. Fang, A. Richa, and G. Xue, “Optimal transmission power control in the presence of a smart jammer,” *The Global Communications Conference (GLOBECOM),* Anaheim, CA, 2012, pp. 5506-5511.

[24] Z Han, et al., “Physical layer security game: How to date a girl with her boyfriend on the same table,” *International Conference on Game Theory for Networks*, 2009, pp. 287-294.

[25] Yuan, Zhengmao, Shenghui Wang, Ke Xiong, and Jiajai Xing, “Game theoretic jamming control for the gaussian interference wiretap channel,” *12th International Conference on Signal Processing (ICSP)*, 2014, pp. 1749-1754.

[26] Kashyap, Akshay, Tamer Basar, and R. Srikant, “Correlated jamming on MIMO Gaussian fading channels,” *IEEE Transactions on Information Theory,* vol. 50, no. 9, pp. 2119-2123, 2004.

[27] Slimeni, Feten, et al., “Closed form expression of the saddle point in cognitive radio and jammer power allocation game,” *International Conference on Cognitive Radio Oriented Wireless Networks*, 2016, pp. 29-40.