Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 1029175, 14 pages
https://doi.org/10.1155/2018/1029175

Research Article

Provoking the Adversary by Detecting Eavesdropping and Jamming Attacks: A Game-Theoretical Framework

Ahmed Salem,[1] **Xuening Liao**,[2,3] **Yulong Shen**,[1] **and Xiaohong Jiang**[2]

[1]*School of Computer Science and Technology, Xidian University, Xi'an, China*
[2]*School of System Information Science, Future University Hakodate, Hokkido, Japan*
[3]*School of Computer Science, Shaanxi Normal University, Xi'an, China*

Correspondence should be addressed to Ahmed Salem; engahmedsalem2@outlook.com

Received 28 April 2018; Accepted 25 July 2018; Published 28 August 2018

Academic Editor: Li Sun

Copyright © 2018 Ahmed Salem et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper investigates the secrecy and reliability of a communication where the user is assisting an Intrusion Detection System (IDS) in detecting the adversary's attack. The adversary is assumed to be sophisticated such that it can conduct eavesdropping and jamming attacks. The IDS is equipped with the capability of detecting both of those attacks. Two scenarios were considered; the first scenario is that the user is trying to detect the adversary by assisting the IDS, and the second scenario is that the user is equipped with a silent time slot in its communication protocol besides assisting the IDS, in order to provoke the adversary into jamming the channel, thus detecting it with a higher probability. Interestingly, adding the capability of detecting eavesdropping attacks pushed the adversary into conducting jamming attacks much more, thus aiding in detecting the adversary earlier. All of that was modeled by means of stochastic game theory, in order to analyze and study the behavior and the interactions between the user and the adversary. Results show a major improvement in the first scenario by 188% and an improvement by 294% in the second scenario in the game value when the probability of detecting eavesdropping attacks was 0.3, which represents the payoff that the user gains in terms of secrecy and reliability.

1. Introduction

The problem of ensuring a secure and reliable wireless communication is challenging due to several reasons. On one hand, the broadcast nature of wireless channels makes it difficult to shield transmitted signals from unintended recipients. On the other hand, possible interference from other transmitters may degrade the received signals at the receiver. An adversary may exploit this weakness to its benefit and behave either as a passive eavesdropper who tries to intercept signals from ongoing transmissions without being detected [1, 2] or as a malicious user (jammer), which transmits jamming signals to the intended receiver. Thus, studies on security and reliability of wireless communications are of great importance for the design of next generation networks.

Lots of techniques were adopted in securing wireless systems, such as relaying [3–6], caching [7], and game theory, which models the conflict and cooperation between intelligent rational selfish decision-makers, as it has been recognized as a promising method to model the interplay between the legitimate user and the adversary in the network [8]. Assuming a network with one source-destination pair and an adversary, the source node aims to transmit the information securely/reliably to the destination, while the adversary attempts to wiretap/jam the signal. Thus, there is a conflict of benefits between the source node and the adversary. This can be modeled as a two-player game and the source node and the adversary act as two players of the game [9, 10]. Based on the types of the adversary (i.e., an eavesdropper, a jammer, and an active adversary), the game can be divided into three categories.

For networks with a jammer, the source node and the jammer will act as two players. The authors in [11] studied a network where the timing channel was exploited at the nodes to achieve resilience to the jamming attacks. They modeled the interactions between the nodes and the jammer based on game theory and the Nash equilibrium was studied.

Furthermore, the investigation was conducted with perfect and imperfect knowledge of the jammer's utility function. In [12], the authors considered a network where a user is trying to ensure a reliable communication with the existence of a reactive jammer. The authors solved the game by investigating Stackelberg equilibrium. In [13], the authors investigated an antijamming problem by using Stackelberg game model, where they followed it by using Hierarchical Power Control Algorithm (HPCA) to obtain Stackelberg equilibrium. In [1], the authors considered two kinds of jammers, a random jammer and a sophisticated jammer. The random jammer was equipped with the capability of employing a silent mode besides the capability of employing a jamming mode. The sophisticated jammer was equipped with two capabilities: (a) communicating as a law-obedient user, by acting as a relay, and (b) conducting a jamming attack and acting as a malicious user. They constructed optimal antijamming transmission strategies and a stochastic game was used in modeling the game between the user and the adversary. In this work, a silent mode was employed to the user to assist an IDS in detecting the adversary.

For networks with an active eavesdropper, the source node and the active eavesdropper will act as two players [14, 15]. In [14], the authors studied a network, where a user is transmitting to a destination with the existence of an active eavesdropper. That eavesdropper imposes a jamming signal to facilitate its eavesdropping, with the existence of its own residual self-interference. The authors established a game-theoretical framework, where closed-form strategies were obtained. Moreover, they analyzed the secrecy outage probability for the legitimate link in that hostile situation. In [15], the interactions were formulated by using a hierarchical game framework, where the eavesdropper acts as the leader and the user acts as the follower. Thus obtaining the optimal transmission strategy that maximizes the secrecy rate.

For networks with an active adversary who can act as either a passive eavesdropper or an active jammer, the game should consider these differences while being designed. In [16], the authors investigated a Multiple-Input Multiple-Output (MIMO) wiretap channel with an active adversary. They examined the legitimate transmitter and the adversary by modeling their interactions as a two-person zero-sum game and derived equilibrium strategies for the extensive form of the game under scenarios with perfect and imperfect information. In [8], a game theoretic approach was followed in dealing with a network, where a number of users are transmitting their message via several relays in the existence of an active adversary, who is capable of launching eavesdropping and jamming attacks. A fictitious play-based algorithm was proposed to assist in reaching the mixed strategy Nash equilibrium, and results show that an improvement can be achieved in the average expected utility per user up to 49.4%. Moreover, eavesdropping and jamming attacks on mobile Cyber-Physical Systems (CPSs) were studied in [17], where a Stackelberg game was used to maximize the secrecy rate between sensors and controllers. Recently, a new approach that considers a more sophisticated adversary with dual capability of conducting either eavesdropping or jamming attack has been proposed in [9]. In [9], a stochastic game was used in modeling the game between a user and an adversary. Two games were proposed, the two games assumed that the adversary can conduct an eavesdropping or a jamming attack. The user was assisting an IDS by exploiting the usage of a silent mode, which provokes the adversary into jamming the communication to facilitate the detection process. In the first game, the IDS can only detect jamming attacks, and in the second game, a time slot was incorporated in the transmission protocol, where the user will be silent, in order to provoke the adversary into conducting a jamming attack, and, therefore, the adversary can be easily detected. In [1, 9], an OFDM system was applied to model the channels between the user, the adversary, and the destination, where the game-theoretical techniques were applied to study and analyze the behavior of a user and an adversary in a network. In [18], the authors studied the secure communication while satisfying the throughput requirements needed by the higher-layer services. They investigated a fair strategy, which satisfies the two objectives (i.e., ensure secrecy and sufficient throughput), such that security and throughput performances can be finally modeled.

These works demonstrated that game theory is a promising approach that can be used in modeling the interplay between the legitimate user and the adversary. It is notable, however, that all the aforementioned works targeted the security or reliability performances of the network without any help of an IDS which can detect eavesdropping and jamming attacks. In our previous work, we propose a new paradigm where the IDS is equipped with the capability of detecting passive eavesdropping and jamming attacks [19], and the adversary is equipped with the capability of conducting passive eavesdropping and jamming attacks. We have proved that, by adopting the IDS in the system, the security and reliability performances can be greatly improved. As an extended work of our previous study, we aim to explore in this paper the reliability and security of a system with one source-destination pair and an adversary with the capabilities of both eavesdropping and jamming. The IDS is adopted in the system and we consider a silent mode at the source node. The contributions of this paper can be summarized as follows:

(i) Propose two new games: the basic game and the extended game, to model the interactions between the source node and the adversary. This is achieved by using stochastic game modeling techniques. In the basic game, the silent mode is unavailable at the source node, and the silent mode is available at the source node in the extended game

(ii) Derive the optimal probabilities and game values for the user and the adversary for the proposed basic game and extended game

(iii) Conduct extensive numerical analysis to validate the efficiency of the proposed games in terms of game values, and results show that our proposed games can assist in the detecting of the adversary by provoking it into conducting a jamming attack. We also made comparisons between our proposed games and the conventional game to demonstrate the performance improvements achieved by our proposed games in

terms of the security and the ability of provoking the adversary. It is observed that a major improvement was achieved for the basic game by 188% and by 294% for the extended game when we set the probability of detecting eavesdropping attacks as 0.3.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model and present the abilities of the IDS to protect the user (Alice) from the adversary (Eve) while providing the needed mathematical formulations and assumptions. In Section 3, we formulate and solve the stochastic game between Alice and Eve. In Section 4, we investigate and present our model when a silent time slot is added to the communication protocol besides the capability of the IDS in detecting eavesdropping and jamming attacks. In Section 5, we present the results derived and analyze the meaning behind them thoroughly. Finally, we conclude this paper in Section 6.

2. System Model and Problem Formulation

Our proposed network consists of a source (Alice), a destination (Bob), and an eavesdropper (Eve). The communication between Alice and Bob needs to be secured against attacks that exploit the link's own secrecy and reliability. Eve acts as an active adversary that is capable of conducting eavesdropping and jamming attacks. In PHY security, the figure of merit is the secrecy rate, which is defined as the difference between the transmission rate of the source-destination link and that of the source-eavesdropper link [20]. For a Gaussian channel, the achievable secrecy rate equals the difference between the mutual information accumulated at the destination and that accumulated at the eavesdropper, which is not less than zero [21]. This leads us to derive the secrecy capacity under an eavesdropping attack as follows: $\mathcal{U}_{sc}(\mathbf{P}) = \max\{\mathcal{U}(\mathbf{P}, 0) - \mathcal{U}_e(\mathbf{P}), 0\}$, in which $\mathcal{U}_{sc}(\mathbf{P})$ is the secrecy capacity achieved under an eavesdropping attack, $\mathcal{U}(\mathbf{P}, 0)$ is the transmission capacity when no attacks are being conducted, and $\mathcal{U}_e(\mathbf{P})$ is the receiving capacity achieved by Eve while conducting an eavesdropping attack.

Detecting passive eavesdropping attacks relies heavily on detecting the Local Oscillator (LO) leakage power that receivers/eavesdroppers emit from their antennas [22, 23]. The leakage power that is being emitted is an inevitable reverse leakage that couples back through the input port and radiates out of the receiver's/eavesdropper's antenna [24], which is represented as being the signal **E** that aids in detecting passive eavesdropping attacks. Unfortunately, detecting this leakage power directly is impractical for two reasons [25]. Firstly, it would be difficult for the receive circuitry to detect the LO leakage over larger distances. In [25], it was shown that a distance of 20 m would take the order of seconds to detect the LO leakage with a high probability. The detection in practical systems will need to be made in the order of milliseconds at worst. The second reason is that it would be impractical to detect the LO leakage directly because its very variable, and it depends on the receiver/eavesdropper circuitry, model, and year of manufacture. Hence, we assumed that the IDS is capable of performing its operations as a cognitive node. Hence, cognitive radios tend to have a higher probability in detecting the passive receivers/eavesdroppers successfully [23–25].

Alice is always transmitting the signal **P**, and Eve is always transmitting either the signal **E** or the signal **J** when an eavesdropping or a jamming attack is being conducted, respectively. The signal **E** represents the LO leakage that radiates inevitably from the eavesdropper's antenna. Alice's IDS is capable of detecting passive eavesdropping and jamming attacks that are being conducted by Eve. Note that the reliability of the channel is neither affected nor compromised by the signal **E**.

If Eve is eavesdropping, the signal **E** will be inevitably sent while Eve is acting as a receiver for what Alice is sending, which will exploit the secrecy of the communication, and leads Alice to conduct her best response by sending the signal P_e, which will increase the secrecy capacity and satisfy the following inequality:

$$\mathcal{U}(\mathbf{P}, \mathbf{E}) \leq \mathcal{U}(P_e, \mathbf{E}), \tag{1}$$

where $\mathcal{U}(\mathbf{P}, \mathbf{E})$ is the resulting transmission capacity when Alice is transmitting the signal **P** to Bob and Eve is conducting an eavesdropping attack (i.e., emits the signal **E**), and $\mathcal{U}(P_e, \mathbf{E})$ is the transmission capacity when Alice is transmitting her best response signal P_e against an eavesdropping attack, while Eve is eavesdropping. Note that, $\mathcal{U}$ represents the payoff, which is the value of the game when Alice wins if the payoff is positive. Hence, the transmission capacity can be considered as the payoff that Alice wins or losses depending on the payoff's value and whether it is positive, zero, or negative. This yields an equilibrium/saddle point, in which $\mathcal{U}(P_e, \mathbf{E})$ will be the payoff to Alice [26].

On the other hand, if Eve was conducting a jamming attack by sending **J**, then, as a countermeasure, Alice's best response will be conducted by sending the signal P_j. This will lead to the following inequality:

$$\mathcal{U}(\mathbf{P}, \mathbf{J}) \leq \mathcal{U}\left(P_j, \mathbf{J}\right), \tag{2}$$

where $\mathcal{U}(\mathbf{P}, \mathbf{J})$ is the transmission capacity when Alice is transmitting **P** and Eve is conducting a jamming attack, and $\mathcal{U}(P_j, \mathbf{J})$ is the transmission capacity when Alice is transmitting her best response signal P_j while Eve is jamming. In that case, an equilibrium will be reached, which will make $\mathcal{U}(P_j, \mathbf{J})$ be the payoff that Alice will obtain.

An OFDM system is being used in this paper with n separate channels, in which those channels are modeled as Additive White Gaussian Noise (AWGN) channels. The channel coefficients between Alice and Bob, Alice and Eve, and Eve and Bob are denoted as $h_{A,B}$, $h_{A,E}$, and h_J, respectively. Reducing the reliability could be attained through jamming attacks that Eve transmits to Bob through the channel h_J. Guaranteeing the secrecy of the channel was done by following the assumption $h_{A,E} \leq h_{A,B}$ [27]. The signal strategy vector for Alice is **P**, where $\mathbf{P} = (P_1, P_2, \ldots, P_n)$. Eve is associated with a jamming signal strategy vector **J**, where $\mathbf{J} = (J_1, J_2, \ldots, J_n)$. Hence, as a conclusion on what was mentioned before regarding signal **E**, it is not considered as a

		Eve	
		E	J
Alice	E	$\mathcal{U}(P_e, \mathbf{E})$ / $(\beta, 1\text{-}\beta)$	$\mathcal{U}(P_e, \mathbf{J})$ / $(\gamma, 1\text{-}\gamma)$
	J	$\mathcal{U}(P_j, \mathbf{E})$ / $(\beta, 1\text{-}\beta)$	$\mathcal{U}(P_j, \mathbf{J})$ / $(\gamma, 1\text{-}\gamma)$

Figure 1: The first malicious state of the game Γ_{EJ}.

$\overline{\mathcal{U}}$	(0,1)

Figure 2: The second safe secure state of the game Γ_{EJ}.

threat on the reliability of the communication. As a result, the signal **E** was not associated with its own channel coefficient. According to [9], the following expressions can be calculated as follows:

$$\mathcal{U}(\mathbf{P}, \mathbf{J}) = \sum_{i=1}^{n} \ln\left(1 + \frac{h_{A,B}P_i}{h_J J_i + \sigma^2}\right), \quad (3)$$

$$\mathcal{U}_e(\mathbf{P}) = \sum_{i=1}^{n} \ln\left(1 + \frac{h_{A,E}P_i}{\sigma_E^2}\right), \text{and} \quad (4)$$

$$\mathcal{U}_{sc}(\mathbf{P}) = \sum_{i=1}^{n} \left(\ln\left(1 + \frac{h_{A,B}P_i}{\sigma^2}\right) - \ln\left(1 + \frac{h_{A,E}P_i}{\sigma_E^2}\right)\right), \quad (5)$$

where P_i is the signal transmitted by Alice through channel i and J_i is the jamming signal transmitted by Eve through channel i. The variances of the noises in the channels of Alice $\longrightarrow$ Bob and Alice $\longrightarrow$ Eve are denoted by σ and σ_E, respectively.

3. The Basic Stochastic Game

3.1. Introduction. In this game, Eve is provided with the capability of performing two kinds of actions (i.e., attacks). The first action is conducting a passive eavesdropping attack and the second action is performing a jamming attack. Eve can choose which attack she prefer to perform. Eve is assumed to choose only one attack at a time. Obviously, Eve will be cautious about choosing which kind of attack to conduct, due to the capability of Alice's IDS in detecting both kinds of attacks. Hence, Alice and Eve are defined to be rational and selfish.

3.2. The Game Modeling. We model the game as a two-state stochastic game as shown in Figures 1 and 2. This model is inspired from the study in [9], where Alice assists an IDS in detecting only jamming attacks. We propose a new scenario, in which Alice's IDS can detect passive eavesdropping attacks, besides detecting jamming attacks.

This game consists of two states. The first state is the malicious state, which the game always begins with, and the second state is the safe secure state, which happens when Eve is detected and removed from the game. Each entry in a state corresponds to a specific action pair that is being performed by Alice and Eve, respectively. Each action pair entry consists of two triangles, the upper left triangle represents the instantaneous payoff (current transmission rate) of Alice in the game, while the lower right triangle gives the probability distribution associated with the future states. As an example, in the first state, in Figure 1, the first block, which is associated with the action pair (E, E), the instantaneous payoff for Alice is shown to be $\mathcal{U}(P_e, E_e)$, and the probability that the next state is state 1 or state 2 is assigned by the probabilities β and (1-β), respectively.

3.3. The Probability Distribution. Eve's detection in both kinds of attacks is represented by a probability distribution. The probability distribution is divided into two probabilities, first, the probability of a missed detection and second, the detection probability. The probability of missed detection is assigned to be β and γ for eavesdropping and jamming attacks, respectively. The missed detection probability also represents the probability of repeating the first state. The detection probability is (1-β) and (1-γ) for eavesdropping and jamming attacks, respectively. The detection probability represents the probability of moving to the second state. We assumed that the probability of a missed detection and the probability of a successful detection are the same in both of the transmission modes of Alice while Eve is performing a specific kind of attack.

3.4. The Epoch Progression. As the epoch progresses, there will be a discount that is being performed on the payoffs, which is modeled by the discount factor δ. The purpose of using a discount factor δ, is to ensure the following: (1) the game will eventually end, (2) the probability of infinite playing will be zero, and (3) all the expected payoffs will be finite [28]. The discount factor δ can be interpreted as a measure of urgency in communications: $\delta = 0$ corresponds to the highest urgency and the transmission must be done in the current time slot. When the urgency is at its peak (i.e., $\delta = 0$), the security will be low as such precautions related to performing the best responses will be missed. If δ was assigned to a high value, this means that a delay can be introduced and the current transmission can be done in other time slots, not necessarily the current one, and this will improve the security.

3.5. Successful and Missed Detection. If Eve was not detected, the game will move to the next time slot and it will be played recursively with a discount factor δ.

If Eve was detected, then Alice will move from the malicious state (i.e., state 1) to the safe secure state (i.e., state 2), and Eve will be removed from the game. In the safe secure state, Alice will send her optimal signal that is designed for the case where there are no threats in the communication (i.e., $P_0 = \text{argmax}_{\mathbf{P}}\mathcal{U}(\mathbf{P}, 0)$).

3.6. Shapley-Bellmann Equation. We denote the game played in state 1 as Γ_{EJ} and the game played in state 2 as Γ_{END}. In state 2, Eve was already detected and Alice can transmit with rate $\overline{\mathcal{U}}$, and the total discounted payoff in state 2 is equal to

$(1+\delta+\delta^2+\cdots)\overline{\mathcal{U}} = \overline{\mathcal{U}}/(1-\delta)$. Studying the malicious state will require modeling the stochastic game Γ_{EJ} as in (6).

$$\Gamma_{EJ} = \begin{matrix} \\ E \\ J \end{matrix} \begin{matrix} \begin{matrix} E \end{matrix} & \begin{matrix} J \end{matrix} \\ \begin{pmatrix} \mathcal{U}(P_e, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\beta)}{1-\delta} & \mathcal{U}(P_e, \mathbf{J}) + \gamma\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\gamma)}{1-\delta} \\ \mathcal{U}(P_j, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\beta)}{1-\delta} & \mathcal{U}(P_j, \mathbf{J}) + \gamma\delta\Gamma_{EJ} + \dfrac{\overline{\mathcal{U}}\delta(1-\gamma)}{1-\delta} \end{pmatrix} \end{matrix} \tag{6}$$

The notations used in (6) are clarified in [28, 29]. The game is modeled as a two-player zero-sum game, in which what one player wins, the other player loses. A zero-sum game models the payoff of the second player (i.e., Eve) as the negative of the payoff of the first player (i.e., Alice). This leads to assigning the second component (i.e., Eve's payoff) of the payoff vector as the negative of the first component (i.e., Alice's payoff) [29]. In a nutshell, what Alice wins, Eve loses.

Equation (6) is a mathematical representation of the two states in the stochastic game shown in Figures 1 and 2. Equation (6) has four entries that represent the four action pairs that the game consists of. For example, we consider the first entry that represents the action pair (E, E), which is $\mathcal{U}(P_e, \mathbf{E}) + \beta\delta\Gamma_{EJ} + \overline{\mathcal{U}}\delta(1-\beta)/(1-\delta)$. The first term $\mathcal{U}(P_e, \mathbf{E})$ represents the instantaneous payoff gained by Alice from being in that mode (i.e., (E, E)). The second term $\beta\delta\Gamma_{EJ}$ highlights the fact that failing in detecting an eavesdropping attack, which consequently will lead to repeating the first state (i.e., Γ_{EJ}), follows a probability distribution (i.e., β in that case). A discount factor δ was also added to that part to ensure that the game will eventually end. Note that the discount factor δ is understood as a measure of urgency for the wireless communication in this work. Finally, the last part, which is $\overline{\mathcal{U}}\delta(1-\beta)/(1-\delta)$, represents the probability distribution of transferring into the next state (i.e., $(1-\beta)$) with the discount factor δ and the total discounted payoff $\overline{\mathcal{U}}/(1-\delta)$ in state 2.

A stationary strategy maps each single state into an action. Stationary strategies are strategies that are independent of the history of previous plays and the current time of the game, which led us to solve this game by using them. This game has an equilibrium in stationary strategies as it is a discounted game. The solution of this game could be given as a solution to the Shapley-Bellmann equation. Shapley-Bellmann equation defines the value of each state recursively in terms of every other state. The Shapley-Bellmann equation for the game Γ_{EJ} is as follows:

$$\mathcal{V} = val\begin{pmatrix} \mathcal{V}_{ee} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{ej} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \\ \mathcal{V}_{je} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{jj} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \end{pmatrix}, \tag{7}$$

in which $\mathcal{V}$ is the value of the game. Note that, according to the *minimax theorem*, for every finite two-player zero-sum game, there is a game value $\mathcal{V}$. If $\mathcal{V}$ is zero, then we say the game is fair. If $\mathcal{V}$ is positive, we say the game favors player I (i.e., Alice), and if $\mathcal{V}$ is negative, we say the game favors player II (i.e., Eve) [28].

$$\mathcal{V} = \max_x \min_y \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} \mathcal{V}_{ee} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{ej} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \\ \mathcal{V}_{je} + \beta\delta\mathcal{V} + \dfrac{(1-\beta)\delta\overline{\mathcal{U}}}{1-\delta} & \mathcal{V}_{jj} + \gamma\delta\mathcal{V} + \dfrac{(1-\gamma)\delta\overline{\mathcal{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{8}$$

By incorporating the probabilities of the mixed strategies in solving this game, we will have (8), in which x_e and x_j are the probabilities of Alice in using the actions E and J, respectively. The probabilities y_e and y_j are the probabilities that Eve will conduct the actions of E and J, respectively. Hence, $x_e + x_j = 1$ and $y_e + y_j = 1$. The payoffs $\mathcal{V}_{ee}, \mathcal{V}_{ej}, \mathcal{V}_{je}$, and $\mathcal{V}_{jj}$ are defined as follows:

$$\mathcal{V}_{ee} = \mathcal{U}(P_e, \mathbf{E}),$$
$$\mathcal{V}_{ej} = \mathcal{U}(P_e, \mathbf{J}),$$
$$\mathcal{V}_{je} = \mathcal{U}(P_j, \mathbf{E}), \text{ and}$$
$$\mathcal{V}_{jj} = \mathcal{U}(P_j, \mathbf{J}). \tag{9}$$

Referring to II-8 in [28] shows that calculating the average payoff depends on the probability of conducting the actions by the two participating players in a 2x2 game. Calculating the average payoff can use the mixed strategy P (i.e., x_e and x_j for Alice) and Q (i.e., y_e and y_j for Eve) for the first and the second players in conducting their actions, respectively. The average payoff to player 1 will be $P^T AQ = \sum_{i=1}^{m}\sum_{j=1}^{n} p_i a_{ij} q_j$, where A is the game matrix. Note that i and j represents the row's and the column's index, respectively. In a nutshell, (8)

calculates the average payoff (i.e., the game value $\mathscr{V}$) in the case of mixed strategies by incorporating the probabilities of conducting the actions of interest into the equation.

For every two-player zero-sum game, there is a value for the game and a mixed strategy for player I (i.e., Alice) and player II (i.e., Eve). Alice's average gain is at least $\mathscr{V}$ no matter what Eve does, and Eve's average loss is at most $\mathscr{V}$ no matter what Alice does. This is called *minimax theorem*, which investigates $\mathscr{V}$ in three cases, which are as follows. (1) If $\mathscr{V}$ is zero, then the game is fair. (2) If $\mathscr{V}$ is positive, then the game favors Alice. (3) If $\mathscr{V}$ is negative, then the game favors Eve. The main justification for these assumptions came from *utility theory*. Since this game is a two-player zero-sum game, then $\max_x \min_y$ coincides with $\min_y \max_x$ as in (8). Assuming that $P_e \neq P_j$ will lead to the following inequalities:

$$\begin{aligned} &\mathscr{V}_{ee} > \mathscr{V}_{je} \text{ and} \\ &\mathscr{V}_{jj} > \mathscr{V}_{ej}. \end{aligned} \tag{10}$$

3.7. Choosing Pure Equilibrium Strategies. This game has four strategies, which are (E, E), (E, J), (J, E), and (J, J). Choosing which strategy can be a pure equilibrium strategy depending on whether the strategy of interest can be a saddle point or not. The strategy can be considered to be a saddle point when it provides the maximum payoff in its column and the minimum payoff in its row in the game's matrix. In this game, if an equilibrium cannot be reached in pure strategies, then it can be found in mixed strategies. We start by inspecting each single strategy whether it can satisfy the conditions of being a saddle point (pure equilibrium strategy) or not.

3.7.1. Strategy (E, E). In order for strategy (E, E) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, E) satisfies both of those conditions as $\mathscr{V}_{ee} > \mathscr{V}_{je}$, which makes it a pure equilibrium strategy. After this step we proceed to calculate its expected payoff, which can be calculated as follows:

$$\mathscr{V} = \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{11}$$

As this strategy is (E, E), the x_e and y_e will be equal to 1. The expected payoff will be equal to

$$\mathscr{V} = \frac{(1-\delta)\,\mathscr{V}_{ee} + (1-\beta)\,\delta\overline{\mathscr{U}}}{(1-\delta)\,(1-\beta\delta)}. \tag{12}$$

3.7.2. Strategy (E, J). In order for strategy (E, J) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

The second condition is satisfied in some circumstances, but the first condition will never be satisfied, due to the assumption that $\mathscr{V}_{jj} > \mathscr{V}_{ej}$. This means that strategy (E, J) is not a pure equilibrium strategy.

3.7.3. Strategy (J, E). In order for strategy (J, E) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

The second condition is satisfied in some circumstances, but the first condition will never be satisfied, due to the assumption that $\mathscr{V}_{ee} > \mathscr{V}_{je}$. This means that strategy (J, E) is not a pure equilibrium strategy.

3.7.4. Strategy (J, J). In order for strategy (J, J) to be a pure equilibrium, it must satisfy the following two conditions:

(1) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, J) satisfies both of those conditions as $\mathscr{V}_{jj} > \mathscr{V}_{ej}$, which makes it a pure equilibrium strategy. After this step we proceed to calculate its expected payoff, which can be calculated as follows:

$$\mathscr{V} = \begin{pmatrix} x_e \\ x_j \end{pmatrix}^T \begin{pmatrix} 0 & 0 \\ 0 & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \tag{13}$$

As this strategy is (J, J), x_j and y_j will be equal to 1. The expected payoff will be equal to

$$\mathscr{V} = \frac{(1-\delta)\,\mathscr{V}_{jj} + (1-\gamma)\,\delta\overline{\mathscr{U}}}{(1-\delta)\,(1-\gamma\delta)}. \tag{14}$$

3.8. Evaluating Equilibrium in Mixed Strategies. By referring to (7), we can consider the game value to be as follows:

$$\mathscr{V} = val \begin{pmatrix} A & B \\ D & C \end{pmatrix}. \tag{15}$$

Then consequently, A, B, C, and D will be as follows:

$$A = \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{16}$$

$$B = \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{17}$$

$$C = \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \text{ and} \tag{18}$$

$$D = \mathscr{V}_{je} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}. \tag{19}$$

Now all the needed terms are written compactly, which will aid in the next mathematical evaluations. Evaluating the mixed stationary equilibrium for X_e, Y_e, the game value $\mathscr{V}$ will be as follows:

$$X_e = \frac{C-D}{A-B+C-D}, \tag{20}$$

$$Y_e = \frac{C-B}{A-B+C-D}, \tag{21}$$

$$\mathscr{V} = \frac{AC-BD}{A-B+C-D}. \tag{22}$$

We follow the same setting as in a previous study in [9]: $\mathscr{V}_{ee} = 1.3$, $\mathscr{V}_{ej} = 0.1$, $\mathscr{V}_{je} = 0.5$, $\mathscr{V}_{jj} = 0.5$, and $\overline{\mathscr{U}} = 3$. The mixed stationary equilibrium for X_e, Y_e, and the game value $\mathscr{V}$ will be as follows:

$$X_e = -\frac{5\delta(\beta-\gamma)(\delta\mathscr{V}-\mathscr{V}+3)}{6(\delta-1)}, \tag{23}$$

$$Y_e = \frac{1}{3}, \tag{24}$$

$$\mathscr{V} = -\frac{(15\delta - 6\beta\delta - 12\delta\gamma + 3)}{(6\delta + 2\beta\delta + 4\delta\gamma - 2\beta\delta^2 - 4\delta^2\gamma - 6)}. \tag{25}$$

Needless to say, before evaluating X_e and Y_e, the game value $\mathscr{V}$ must be evaluated first. Note that δ is a discount factor and it takes values from 0.1 to 0.9, and β and γ are probabilities and they take values from 0.1 to 0.9.

3.9. The Game's Operation. After substituting the value of $\mathscr{V}$ and evaluating the conditions for stationary equilibrium strategies in a closed form for equilibrium in pure and mixed strategies, the following conditions are investigated, in order to decide whether the equilibrium will be in pure or mixed strategies, and thereby obtaining the optimal probabilities for Alice and Eve (i.e., x_e, x_j, y_e, and y_j), and the game values and these conditions are as follows.

3.9.1. Condition 1. If $(\mathscr{V}_{ee}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)) < (\mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta))$ and $(\mathscr{V}_{ee}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)) > (\mathscr{V}_{je}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta))$, then the action (E, E) is a saddle point, which will make x_e and y_e equal to one, and the game value for this case will be equal to (12).

3.9.2. Condition 2. If $(\mathscr{V}_{jj}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)) < (\mathscr{V}_{je}+\beta\delta\mathscr{V}+(1-\beta)\delta\overline{\mathscr{U}}/(1-\delta))$ and $(\mathscr{V}_{jj}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)) > (\mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta))$, then the action (J, J) is a saddle point, which will make x_j and y_j equal to one, and the game value for this case will be equal to (14).

		Eve: E	Eve: J
Alice	E	$\mathscr{U}(P_e, \mathbf{E})$ / $(\beta, 1-\beta)$	$\mathscr{U}(P_e, \mathbf{J})$ / $(\gamma, 1-\gamma)$
	J	$\mathscr{U}(P_j, \mathbf{E})$ / $(\beta, 1-\beta)$	$\mathscr{U}(P_j, \mathbf{J})$ / $(\gamma, 1-\gamma)$
	S	0 / $(\beta, 1-\beta)$	0 / $(\gamma_s, 1-\gamma_s)$

Figure 3: The first malicious state of the game Γ_{EJS}.

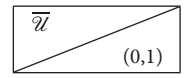


Figure 4: The second safe secure state of the game Γ_{EJS}.

3.9.3. Condition 3. If both conditions 1 and 2 were not satisfied, then a mixed stationary equilibrium arises. Calculating equilibrium in mixed strategies can be done by following (15)-(19), which will lead to (23)-(25).

4. The Extended Stochastic Game

4.1. Introduction. In this game, Alice is aiding an IDS in detecting eavesdropping and jamming attacks. Alice is provided by an additional mode, where she keeps silent, in order to provoke Eve into performing a jamming attack. Strategic allocation of that silent mode is crucial for the successful and effective operation of this mode, where the benefits can be flourished and the secrecy of communication can thrive. A stochastic game has been modeled, in order to tackle this problem and, therefore, the actions of Alice and Eve can be analyzed and investigated even further. It is shown that adding a silent time slot into the transmission protocol can improve the secrecy. Indeed some problems might arise like the delay that such a mode introduces to the communication, but the analysis shows that the benefits and gains can exceed the drawbacks.

4.2. The Game Modeling. As the previous game, we model this game as a two-state stochastic game as shown in Figures 3 and 4. The first state is assumed to be the malicious state, where the communication is being eavesdropped upon or being jammed. It is always assumed that the game is beginning with that state. The second state is the safe secure one. In the stochastic game, remaining in the same state (i.e., state 1) or transferring to the other state (i.e., state 2) depends on a probability distribution. In Figures 3 and 4, the game table for our extended stochastic game is presented. The payoffs for the silent mode are zero; however, Alice will use that mode as it allows her to detect Eve early and remove her from the game and, consequently, she can transmit efficiently without worrying about eavesdropping or jamming attacks.

Figure 3 is the first malicious state, where the probability γ_s is being introduced, as it represents the probability of a missed detection of a jamming attack while Alice is silent. We assumed that γ_s is less than γ, which means that detecting

jamming attacks launched by Eve while Alice is silent is more effective than detecting jamming attacks while Alice is transmitting [9]. Note that the IDS is responsible for detecting Eve whether she is eavesdropping or jamming; however, detecting jamming attacks while being silent is far more efficient and successful. Figure 4 is the second safe secure state that Alice wants to reach. Note that the instantaneous payoffs for the action pairs (S, E) and (S, J) are zero, due to the delay that the silent mode introduces to the communication.

4.3. The Probability Distribution. Detecting Eve is being represented by a probability distribution. If Eve was successfully detected, the game will move to the second state. If Eve was missed, then the cycle will repeat itself until Eve gets detected. The behavior of the game regarding γ and β is the same as the last game. However, some changes are being introduced to this game regarding γ_s. The probability of a successful detection of a jamming attack while Alice is in the silent mode is (1- γ_s), and the probability of a missed detection of a jamming attack while Alice is in the silent mode is γ_s. The probability γ_s was designed to be less than γ, which highlights the effectiveness of detecting Eve's jamming attacks while being silent.

In the case where Alice is silent and Eve is eavesdropping (i.e., the (S, E) action pair), the probability distribution is (β, 1-β), as, in that case, Eve can get provoked to launch a jamming attack especially when the probability of detecting eavesdropping attacks gets higher, and the payoff is zero, due to the delay that the communication will suffer while Alice is being silent.

4.4. The Epoch Progression. The epoch progression in this extended stochastic game is the same as the one that was introduced in the basic stochastic game without any change in its definition or operation.

4.5. Successful and Missed Detection. If Eve was not detected, the game will move to the next time slot and it will be played recursively with a discount factor δ, the same as in the basic game.

If Eve was detected, then Alice will move from the malicious state (i.e., state 1) to the safe secure state (i.e., state 2), the same as in the basic game, adding to that the higher probability in detecting Eve's jamming attacks, especially when Alice is silent as (1 - γ_s) > (1 - γ).

4.6. Shapley-Bellmann Equation. We denote the game in state 1 as Γ_{EJS} and the game played in state 2 as Γ_{END}. In state 2, Eve was already detected and Alice can transmit with rate $\overline{\mathscr{U}}$, which is the most efficient way in communication as no eavesdropping or jamming attacks are being expected.

The extended stochastic proposed game can be presented by (26). The notations have the same meaning and operation as the ones used in the basic stochastic game. The action pairs (S, E) and (S, J) are shown too in (26), where there are no payoffs for both of these actions, but there is a probability distribution assigned to each one of them.

$$\Gamma_{EJS} = \begin{matrix} \\ E \\ J \\ S \end{matrix} \begin{matrix} \qquad E \qquad\qquad\qquad\qquad J \\ \begin{pmatrix} \mathscr{U}(P_e,\mathbf{E}) + \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \mathscr{U}(P_e,\mathbf{J}) + \gamma\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma)}{1-\delta} \\ \mathscr{U}(P_j,\mathbf{E}) + \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \mathscr{U}(P_j,\mathbf{J}) + \gamma\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma)}{1-\delta} \\ \beta\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\beta)}{1-\delta} & \gamma_s\delta\Gamma_{EJS} + \dfrac{\overline{\mathscr{U}}\delta(1-\gamma_s)}{1-\delta} \end{pmatrix} \end{matrix} \quad (26)$$

The action pair (S, E) is represented as $\beta\delta\Gamma_{EJS} + \overline{\mathscr{U}}\delta(1-\beta)/(1-\delta)$. The first part $\beta\delta\Gamma_{EJS}$ represents the probability distribution regarding the case of a missed detection of an eavesdropping attack that can happen with a probability of β and consequently will lead to the repetition of the first state (i.e., Γ_{EJS}), adding to that a discount factor δ to ensure that the game will eventually end. The second part $\overline{\mathscr{U}}\delta(1-\beta)/(1-\delta)$ represents the probability distribution of transferring into the second state, which can happen with a probability of $(1-\beta)$, adding to that the total discounted payoff $\overline{\mathscr{U}}/(1-\delta)$ along with the discount factor δ.

The action pair (S, J) is represented as $\gamma_s\delta\Gamma_{EJS} + \overline{\mathscr{U}}\delta(1-\gamma_s)/(1-\delta)$. The first part $\gamma_s\delta\Gamma_{EJS}$ represents the probability distribution regarding the case of a missed detection of a jamming attack that can happen with a probability of γ_s and consequently will lead to the repetition of the first state (i.e., Γ_{EJS}). The second part $\overline{\mathscr{U}}\delta(1-\gamma_s)/(1-\delta)$ represents the probability distribution of transferring into the second state, which can happen with a probability of $(1-\gamma_s)$, adding to that the total discounted payoff $\overline{\mathscr{U}}/(1-\delta)$.

$$\mathscr{V} = \max_x \min_y \begin{pmatrix} x_e \\ x_j \\ x_s \end{pmatrix}^T \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\delta\overline{\mathscr{U}}}{1-\delta} \\ \mathscr{V}_{je} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\delta\overline{\mathscr{U}}}{1-\delta} \\ \beta\delta\mathscr{V} + \dfrac{(1-\beta)\delta\overline{\mathscr{U}}}{1-\delta} & \gamma_s\delta\mathscr{V} + \dfrac{(1-\gamma_s)\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \quad (27)$$

Equation (27) shows the assignment to the optimal probabilities for each action that Alice and Eve can do during the operation of that system. It is shown that there are three actions for Alice in that game, which are being in the eavesdropping mode, jamming mode, or the silent mode. This makes the optimal probabilities be as follows: $x_e + x_j + x_s = 1$. Similarly for Eve, as she is equipped with the action of eavesdropping or jamming, which makes her optimal probabilities for this game be as follows: $y_e + y_j = 1$. Furthermore, by referring to II-8 in [28], it is shown that the average payoff to player 1 is $P^T AQ = \sum_{i=1}^{m} \sum_{j=1}^{n} p_i a_{ij} q_j$ in the case of mixed strategies. Thus by incorporating the probabilities of conducting the actions of interest into the equation, we get (27).

The Shapley-Bellmann equation, where equilibrium strategies can be studied and investigated, is shown in

$$\mathscr{V} = val \begin{pmatrix} \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ \mathscr{V}_{je} + \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ \beta\delta\mathscr{V} + \dfrac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta} & \gamma_s\delta\mathscr{V} + \dfrac{(1-\gamma_s)\,\delta\overline{\mathscr{U}}}{1-\delta} \end{pmatrix}, \tag{28}$$

in which $\mathscr{V}$ is the value of the game. This game is a two-player zero-sum game. By referring to (26), we follow the same assumptions as in the basic stochastic game such that $P_e \neq P_j$, which leads to the following inequalities:

$$\begin{aligned} &\mathscr{V}_{ee} > \mathscr{V}_{je} \text{ and} \\ &\mathscr{V}_{jj} > \mathscr{V}_{ej}. \end{aligned} \tag{29}$$

4.7. Choosing Pure Equilibrium Strategies. This game has six strategies, which are (E, E), (E, J), (J, E), (J, J), (S, E), and (S, J). Now we start testing which of those strategies can be a saddle point, in which pure equilibrium can be reached. As the equations are quite lengthy, we used the same setting as in [9], in which $\mathscr{V}_{ee} = 1.3, \mathscr{V}_{ej} = 0.3, \mathscr{V}_{je} = 0.8, \mathscr{V}_{jj} = 0.5, \overline{\mathscr{U}} = 5$, and $\gamma = 0.8$. We assume that our proposed parameters β and γ_s are equal to 0.8 and 0.5, respectively. Searching for the pure equilibrium strategies will be based on those parameters.

4.7.1. Strategy (E, E). In order for strategy (E, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, E) will not be a pure equilibrium strategy as the first condition will never be satisfied, unlike the other two conditions, which are always satisfied.

4.7.2. Strategy (E, J). In order for strategy (E, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (E, J) will not be a pure equilibrium strategy as the second condition will never be satisfied, unlike the first condition, which is always satisfied, and the third condition, which is sometimes satisfied based on the parameters.

4.7.3. Strategy (J, E). In order for strategy (J, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, E) will not be a pure equilibrium strategy as the first and second conditions will never be satisfied, unlike the third condition, which is always satisfied.

4.7.4. Strategy (J, J). In order for strategy (J, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (J, J) is a pure equilibrium strategy as all the conditions are satisfied. Specifically, the first two conditions are always satisfied, and the third condition depends on the parameters. The expected payoff can be calculated as follows:

$$\begin{aligned} &\mathscr{V} \\ &= \begin{pmatrix} x_e \\ x_j \\ x_s \end{pmatrix}^T \begin{pmatrix} 0 & 0 \\ 0 & \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \dfrac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_e \\ y_j \end{pmatrix} \end{aligned} \tag{30}$$

Needless to say, as the considered strategy is (J, J), this means that $x_e = 0$, $x_j = 1$, and $x_s = 0$. The same applies for y as $y_e = 0$ and $y_j = 1$. According to that, the game value will be as follows:

$$\frac{\mathscr{V}_{jj} + (1-\gamma)\,\delta\overline{\mathscr{U}}/(1-\delta)}{1-\gamma\delta}. \tag{31}$$

4.7.5. Strategy (S, E). In order for strategy (S, E) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) < \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ee} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{je} + \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (S, E) will not be a pure equilibrium strategy as the second and third conditions will never be satisfied, unlike the first condition, which is always satisfied.

4.7.6. Strategy (S, J). In order for strategy (S, J) to be a pure equilibrium, it must satisfy the following conditions:

(1) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \beta\delta\mathscr{V} + (1-\beta)\delta\overline{\mathscr{U}}/(1-\delta)$

(2) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

(3) $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$

Strategy (S, J) will not be a pure equilibrium strategy as the first condition will never be satisfied, unlike the other two conditions, which can be satisfied based on the parameters.

4.8. Evaluating Equilibrium in Mixed Strategies. By referring to (28), we can consider the game value to be as follows:

$$\mathscr{V} = val\begin{pmatrix} A & B \\ D & C \\ E & F \end{pmatrix}. \tag{32}$$

Consequently, A, B, C, D, E, and F will be as follows:

$$A = \mathscr{V}_{ee} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{33}$$

$$B = \mathscr{V}_{ej} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{34}$$

$$C = \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + \frac{(1-\gamma)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{35}$$

$$D = \mathscr{V}_{je} + \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{36}$$

$$E = \beta\delta\mathscr{V} + \frac{(1-\beta)\,\delta\overline{\mathscr{U}}}{1-\delta}, \tag{37}$$

$$F = \gamma_s\delta\mathscr{V} + \frac{(1-\gamma_s)\,\delta\overline{\mathscr{U}}}{1-\delta}. \tag{38}$$

The extended game has three equilibria in mixed strategies, which are *EJ*, *ES*, and *JS*.

Equilibrium in mixed strategies for *EJ* can be evaluated by using (20), (21), and (22) with (33), (34), (35), and (36).

The mixed stationary equilibrium for *ES* can be obtained by evaluating X_{es}, Y_{es}, and $\mathscr{V}_{es}$ as follows:

$$X_{es} = \frac{F-E}{A-B+F-E}, \tag{39}$$

$$Y_{es} = \frac{F-B}{A-B+F-E}, \tag{40}$$

$$\mathscr{V}_{es} = \frac{AF-BE}{A-B+F-E}. \tag{41}$$

For the sake of brevity, we omitted evaluating those equations as the obtained equations were so lengthy.

The mixed stationary equilibrium for *JS* can be obtained by evaluating X_{js}, Y_{js}, and $\mathscr{V}_{js}$ as follows:

$$X_{js} = \frac{F-E}{D-C+F-E}, \tag{42}$$

$$Y_{js} = \frac{F-C}{D-C+F-E}, \tag{43}$$

$$\mathscr{V}_{js} = \frac{DF-CE}{D-C+F-E}. \tag{44}$$

For the sake of brevity, we omitted evaluating those equations too as the obtained equations were so lengthy.

4.9. The Game's Operation. In the extended game, there will be six conditions that game might be residing in. The conditions are as follows.

4.9.1. Condition 1. If $\mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta) > \gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta)$, then a pure equilibrium in (J, J) arises. The probabilities x_e, x_s, and y_e will be equal to zero, and the probabilities x_j and y_j will be equal to 1. The game value will be as in equation (31).

4.9.2. Condition 2. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{es} > \mathscr{V}_{js}$, then the game value will be equal to $\mathscr{V}_{es}$, and the optimal probabilities will be as in (39) and (40).

4.9.3. Condition 3. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) > \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{js} > \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{js}$, and the optimal probabilities will be as in (42) and (43).

4.9.4. Condition 4. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{ej} < \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{es}$, and the optimal probabilities will be as in (39) and (40).

4.9.5. Condition 5. If $\gamma_s\delta\mathscr{V} + (1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{jj} + \gamma\delta\mathscr{V} + (1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$ and $\mathscr{V}_{ej} > \mathscr{V}_{es}$, then the game value will be equal to $\mathscr{V}_{ej}$, and the optimal probabilities will be as in (20) and (21) while considering the assumptions and parameters for the extended game.

Table 1: Optimal probabilities for each specified game value $\mathscr{V}$.

Game value $\mathscr{V}$	X_e	X_j	X_s	Y_e	Y_j
$\mathscr{V}_{jj}$	0	1	0	0	1
$\mathscr{V}_{ej}$	X_{ej}	1-X_{ej}	0	Y_{ej}	1-Y_{ej}
$\mathscr{V}_{es}$	X_{es}	0	1-X_{es}	Y_{es}	1-Y_{es}
$\mathscr{V}_{js}$	0	X_{js}	1-X_{js}	Y_{js}	1-Y_{js}

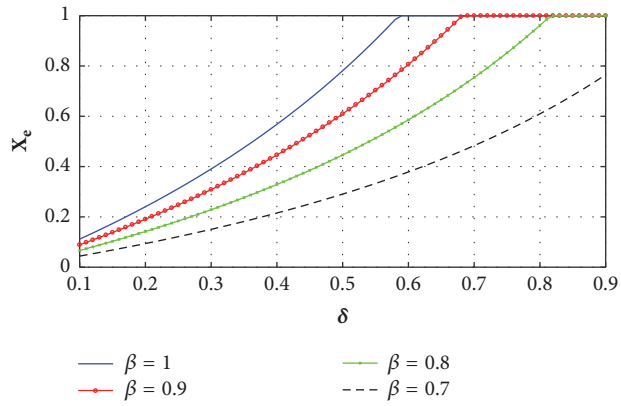


Figure 5: X_e for the basic game.

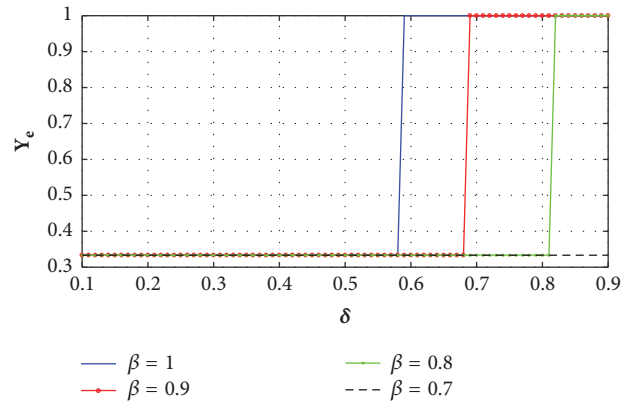


Figure 6: Y_e for the basic game.

4.9.6. Condition 6. If $\gamma_s\delta\mathscr{V}+(1-\gamma_s)\delta\overline{\mathscr{U}}/(1-\delta) < \mathscr{V}_{ej}+\gamma\delta\mathscr{V}+(1-\gamma)\delta\overline{\mathscr{U}}/(1-\delta)$, then the game value will be equal to $\mathscr{V}_{ej}$ and the optimal probabilities will be as in (20) and (21).

While considering these conditions, Alice will have three probabilities for the actions that she might consider and the same goes for Eve regarding her two actions. In Table 1, the probabilities are clarified in accordance with each game value that was chosen based on the aforementioned conditions.

5. Results and Analysis

In this section, the optimal probabilities for Alice and Eve and the game value obtained from our proposed games will be presented and investigated. Moreover, we compare our results with the existing work in the literature, in order to validate and verify the effectiveness of our proposed games in providing a better secrecy and reliability to the wireless communication between Alice and Eve.

5.1. Results from the Basic Game. Considering the same setting as the previous study [9], $\mathscr{V}_{ee} = 1.3$, $\mathscr{V}_{ej} = 0.1$, $\mathscr{V}_{je} = 0.5$, $\mathscr{V}_{jj} = 0.5$, and $\overline{\mathscr{U}} = 3$. We fixed γ as 0.5 and we show the optimal probabilities of our basic game for the source Alice to be in the eavesdropping mode and the adversary to be eavesdropping, for $\beta = 1, 0.7, 0.8$, and 0.9, in Figures 5 and 6, respectively. It is worth noting that as $\beta = 1$ our basic scheme will be the same as the conventional game [9].

From Figures 5 and 6, we can see that, as the discount factor δ increases, the optimal probabilities in our basic game and the available game in [9] will increase. This is due to the reason that δ represents the urgency of the communication and the larger the δ is, the lower the urgency of the communication is. Thus, as δ increases, the urgency of the communication decreases and Alice and Eve will go slower toward being in the jamming mode.

Another observation from Figures 5 and 6 indicates that differences between the optimal probabilities in Figures 5 and 6 become more clear when δ takes higher values (higher values of δ means lower communication urgency), thus giving more opportunities for Alice and Eve to take precautions to achieve their goal, i.e., to transmit securely and reliably (Alice's goal) or to eavesdrop or jam the signal (Eve's goal).

Moreover, the results in Figures 5 and 6 indicate that, as the probability of a missed detection of an eavesdropping attack (i.e., β) decreases, the game value of being in the eavesdropping mode increases and Alice and Eve thus start shifting into the jamming mode. This occurs due to the improvement in detecting eavesdropping attacks, which will lead Eve into jamming the signal and consequently; Alice will follow that by being in the jamming mode.

We then illustrate how the overall game values vary with the discount factor δ in Figure 7, from which we can find that the game values increase as δ increases. This is due to the same reason as that for Figures 5 and 6. We can also see from Figure 7 that the game value increases as β decreases. This is because as the probability of detecting eavesdropping attacks increases, the probability of a secure transmission of the information increases and thus the security performance of the system is being improved. Moreover, Figure 7 shows that a noticeable improvement can occur to the game value, especially when δ takes values higher than 0.6. Actually, an improvement of 188% is noticed in the game value after

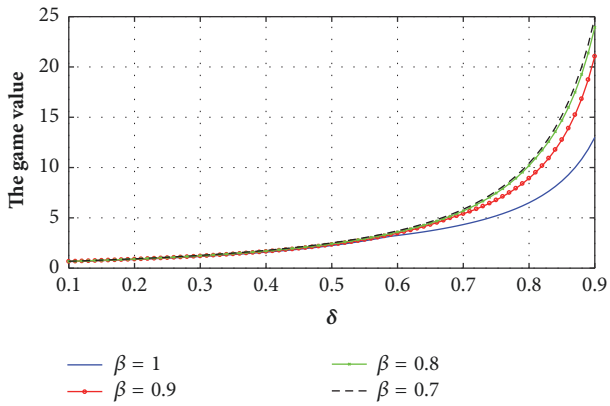


FIGURE 7: The game value for the basic game with $\beta = 0.9$, $\beta = 0.8$, and $\beta = 0.7$, and for the game in [9] with $\beta = 1$.

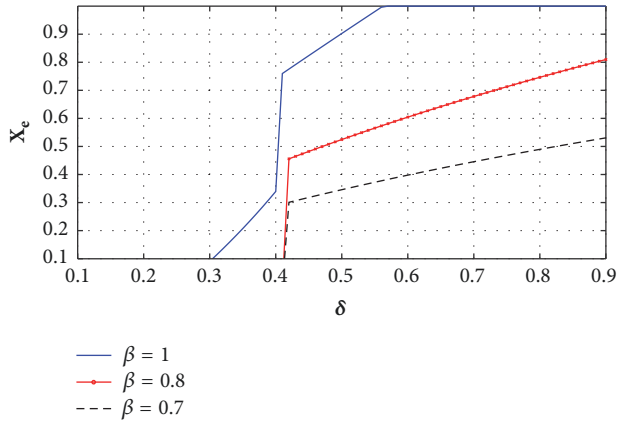


FIGURE 8: X_e for the extended game.

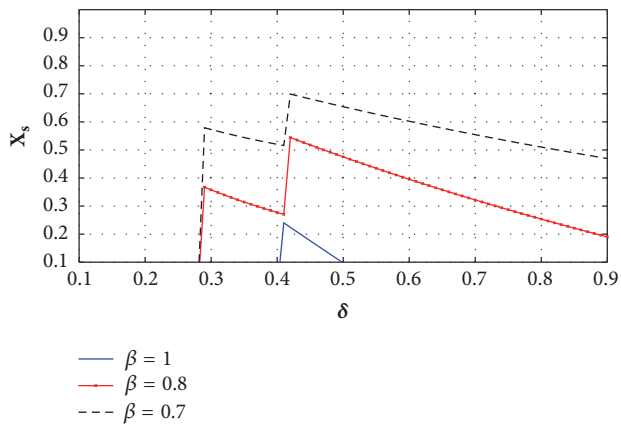


FIGURE 9: X_s for the extended game.

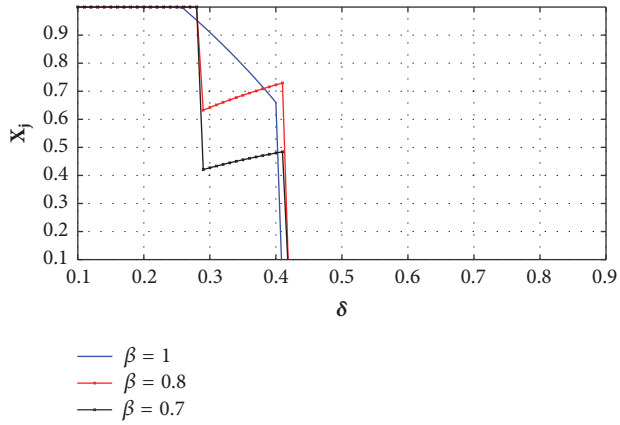


FIGURE 10: X_j for the extended game.

adding the capability of detecting eavesdropping attacks (even though the capability is low) based on the results in Figure 7.

5.2. Results from the Extended Game. In this proposed extended game, we follow the same setting as the previous study [9]: $\mathcal{V}_{ee} = 1.3$, $\mathcal{V}_{ej} = 0.3$, $\mathcal{V}_{je} = 0.8$, $\mathcal{V}_{jj} = 0.5$, and $\overline{\mathcal{U}} = 5$. We fixed γ as 0.8 and we show the optimal probabilities of our extended game when the source Alice is in the eavesdropping, jamming, and silent modes, and when the adversary Eve is eavesdropping and jamming, for $\beta = 1, 0.8$, and 0.7, in Figures 8, 9, 10, 11, and 12, respectively. It is worth noting that, as $\beta = 1$, our basic scheme will be the same as the conventional game [9].

Figures 8 and 11 show that, as the discount factor δ increases, the optimal probability toward being in the eavesdropping mode for Alice or conducting an eavesdropping attack for Eve will increase for both of them. The figures highlight that, as β decrease, the incentives toward being in the eavesdropping mode for Alice or launching an eavesdropping attack for Eve will decrease, as both of them will move toward jamming. Eve will conduct jamming attacks, which will make Alice alter her strategy into being in the jamming or the silent mode.

Figures 9 and 10 integrate with Figure 8. An observation from those two figures must be captured and it is as follows: as β decreases, both of those figures act in an opposite way. In Figure 9, as β decreases, the probability of being in the jamming mode decreases too, but, in Figure 10, as β decreases, the optimal probability of being in the silent mode increases. This means that, as the detection of eavesdropping attacks improves, Eve will start jamming attacks, which in this extended game will result in Alice utilizing her silent mode to increase the probability of detecting Eve while jamming, thus, removing Eve from the game and improving the security of the communication.

Figures 11 and 12 integrate with each other because they represent the actions that Eve can take. As δ increases, Eve becomes more cautious and avoids getting detected so she just launch eavesdropping attacks. The opposite is captured by Figure 12, where Eve conducts jamming attacks with low values of δ. Decreasing the value of β did not have a remarkable effect on Eve's actions; however, as shown before, it affected Alice's actions in a noticeable way and, consequently, it will affect the game value resulting from this game as shown in Figure 13.

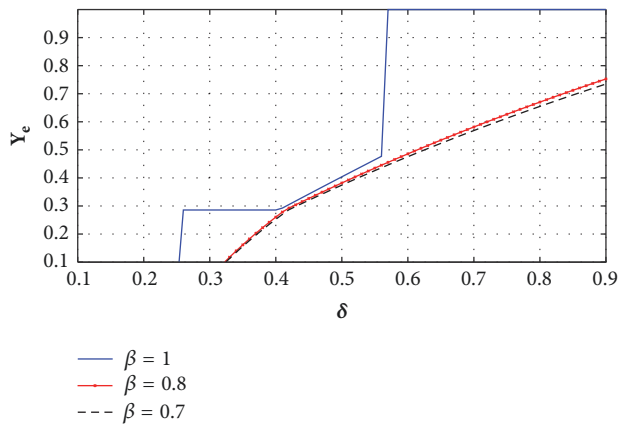


FIGURE 11: Y_e for the extended game.

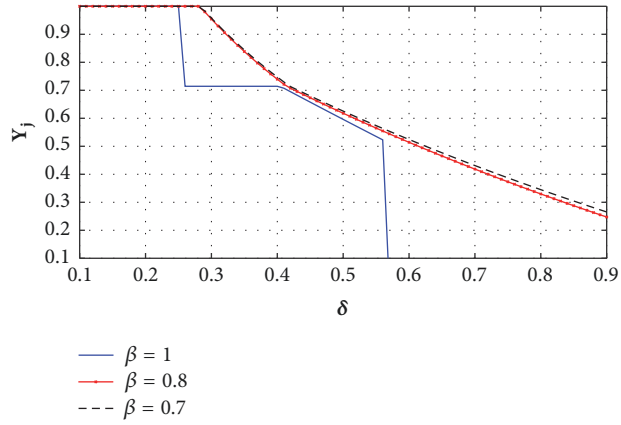


FIGURE 12: Y_j for the extended game.

In Figure 13, the game value is shown, and as δ increases, the game value increases too, for the same reasons mentioned before. Interestingly, when β decreases and becomes 0.8 or 0.7, a huge improvement can be noticed in the game value by 294%. Improvements at high values of β occurs due to embracing the eavesdropping mode by Alice and Eve, as both of them become cautious about choosing the strategy that will generate the highest payoff.

6. Conclusion

This paper studies the secrecy and reliability of a system with one source-destination pair and a sophisticated adversary who conducts eavesdropping and jamming attacks. To analyze and study the behavior and the interactions between the user and the adversary, stochastic game theory is adopted and different games are proposed for different network scenarios. Based on results of the theoretical models, extensive numerical results are then conducted to validate the efficiency of the proposed games. Results show that adding the capability of detecting eavesdropping attacks can push the adversary into jamming the channel much more, which,

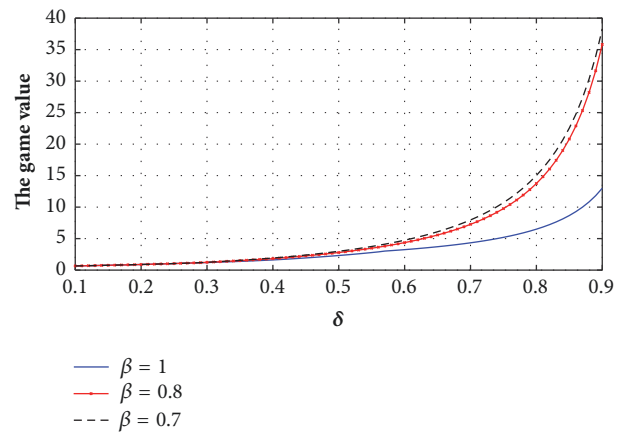


FIGURE 13: The game value for the extended game with $\beta = 0.8$ and $\beta = 0.7$ and for the game in [9] with $\beta = 1$.

on one side, might compromise the reliability of the channel and, on the other side, can aid in detecting the adversary more earlier with an improvement of 188% in the game value. Moreover, when the silent mode is incorporated into the communication protocol of the user, massive payoffs are gained with a huge improvement of 294% in game value. Our work in this paper is of great importance since it can provide theoretical models for the security and reliability study of networks against eavesdropping and jamming attacks, which offers a guideline for the design of future networks.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by The National Key R&D Program of China (Grant no. 2017YFB1400700) and The National Natural Science Foundation of China under Grant nos. U1536202 and 61571352.

References

[1] A. Garnaev and W. Trappe, "Anti-jamming strategies: a stochastic game approach," in *Mobile Networks and Management*, vol. 141 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 230–243, Springer International Publishing, Cham, 2015.

[2] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Ad Hoc Networks*, vol. 129 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 146–161, Springer International Publishing, Cham, 2014.

[3] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel

interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[4] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.

[5] J. Xia, F. Zhou, X. Lai et al., "Cache aided decode-and-forward relaying networks: from the spatial view," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5963584, 9 pages, 2018.

[6] X. Lai, J. Xia, M. Tang, H. Zhang, and J. Zhao, "Cache-aided multiuser cognitive relay networks with outdated channel state information," *IEEE Access*, vol. 6, pp. 897–921, 2018.

[7] F. Shi, L. Fan, X. Liu, Z. Na, and Y. Liu, "Probabilistic caching placement in the presence of multiple eavesdroppers," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2104162, 10 pages, 2018.

[8] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: a game-theoretic approach," in *Proceedings of the Military Communications Conference (MILCOM '11)*, pp. 119–124, November 2011.

[9] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2155–2163, 2016.

[10] A. Garnaev and W. Trappe, "The eavesdropping and Jamming Dilemma in multi-channel communications," in *Proceedings of the 2013 IEEE International Conference on Communications, ICC 2013*, pp. 2160–2164, Hungary, June 2013.

[11] S. D'Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, "Defeating jamming with the power of silence: a game-theoretic analysis," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, 2015.

[12] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Securing wireless transmission against reactive jamming: a stackelberg game framework," in *Proceedings of the 58th IEEE Global Communications Conference, GLOBECOM 2015*, USA, December 2015.

[13] L. Jia, F. Yao, Y. Sun, Y. Xu, S. Feng, and A. Anpalagan, "A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies," *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 818–821, 2017.

[14] X. Tang, P. Ren, and Z. Han, "Combating full-duplex active eavesdropper: a game-theoretic perspective," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, Malaysia, May 2016.

[15] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: a hierarchical game perspective," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1379–1395, 2017.

[16] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82–91, 2013.

[17] L. Yuan, K. Wang, T. Miyazaki, S. Guo, and M. Wu, "Optimal transmission strategy for sensors to defend against eavesdropping and jamming attacks," in *Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017*, France, May 2017.

[18] A. Garnaev and W. Trappe, "Bargaining over the fair trade-off between secrecy and throughput in OFDM communications," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 242–251, 2017.

[19] A. Salem, X. Liao, Y. Shen, and X. Lu, "Provoking the adversary by dual detection techniques: a game theoretical framework," in *Proceedings of the 2017 International Conference on Networking and Network Applications (NaNA)*, pp. 326–329, Kathmandu, October 2017.

[20] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 16–30, 2012.

[21] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[22] P. Sanghoon, L. E. Larson, and L. B. Milstein, "Hidden mobile terminal device discovery in a UWB environment," in *Proceedings of the ICUWB2006: 2006 IEEE International Conference on Ultra-Wideband*, pp. 417–421, USA, September 2006.

[23] G. Zhao, W. Shi, L. Li, and S. Li, "Passive primary receiver detection for underlay spectrum sharing in cognitive radio," *IEEE Signal Processing Letters*, vol. 21, no. 5, pp. 564–568, 2014.

[24] S. M. Weiss, R. D. Weller, and S. Driscol, *New measurements and predictions of uhf television receiver local oscillator radiation interference*, Merrill Weiss Group, Metuchen, 2006.

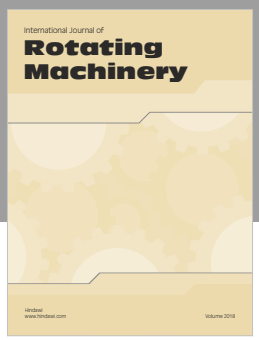
[25] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 124–130, November 2005.

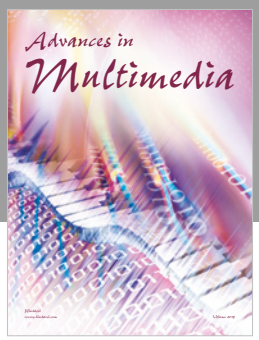
[26] M. Felegyhazi and J.-P. Hubaux, "Game theory in wireless networks: a tutorial," Tech. Rep, 2006.

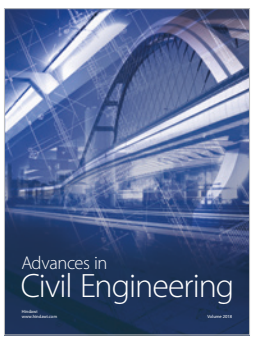
[27] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

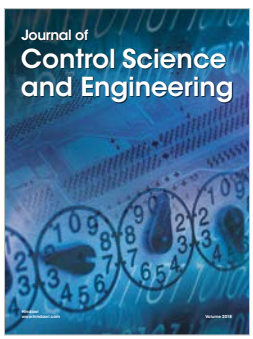
[28] T. S. Ferguson, *Game Theory*, Mathematics Department, UCLA, 2008.

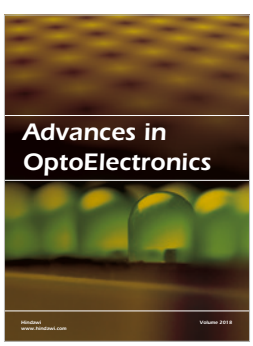
[29] G. Owen, *Game Theory*, Academic Press, New York, NY, USA, 1982.

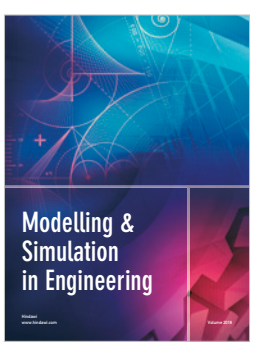


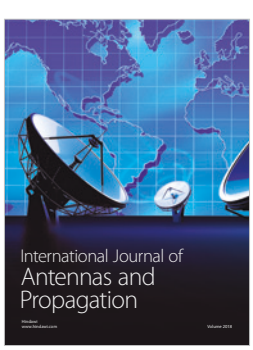


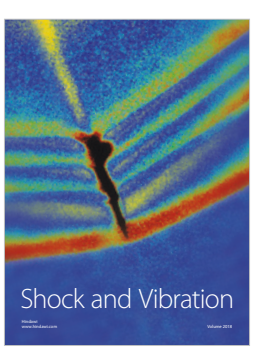


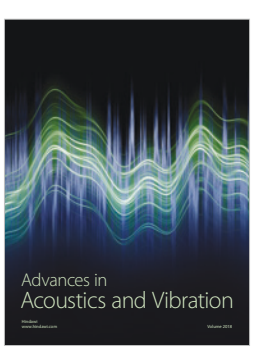












Hindawi

Submit your manuscripts at
www.hindawi.com