A Game Theoretic Analysis of Secret and Reliable Communication With Active and Passive Adversarial Modes

Andrey Garnaev, Melike Baykal-Gursoy, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—Secret and reliable communication presents a challenge involving a double dilemma for a user and an adversary. One challenge for the adversary is to decide between jamming and eavesdropping. While jamming can be quite effective in preventing reliable communication of the user, it can also be quite harmful for the adversary since he/she can be detected. On the other hand, eavesdropping is quite safe for the adversary; however, it sometimes may not be so efficient compared to jamming, if the adversary cannot respond to the information gleaned from eavesdropping in a timely manner. The user can either transmit, thus becoming vulnerable to malicious activity, or be in a silent mode in turn delaying his/her transmission. However, by combining these modes properly the user can assist an intruder detection system in detecting the adversary, since transmission can provoke the adversary into a jamming attack, and a strategically allocated silent mode while the jammer continues jamming can increase the probability of detecting the adversary. In this paper, to get insight into this problem, two simple stochastic games are proposed. Explicit solutions are found that lead to the characterization of some interesting properties. In particular, it is shown that under certain conditions, incorporating in the transmission protocol a time slot dealing just with the detection of malicious threats can improve the secrecy and reliability of the communication without extra transmission delay.**

***Index Terms*—Jamming, eavesdropping, secret communication, stochastic games, stationary strategies.**

I. INTRODUCTION

THE problem of establishing secret and reliable wireless communication between a transmitter and a receiver is a challenge involving several different aspects. On the one hand, due to the broadcast nature of wireless communication it is difficult to shield transmitted signals from unintended recipients. On the other hand, due to possible interference from other transmitters the reliability of signals at the receiver may suffer. An adversarial user may exploit these weaknesses to its benefit and behave either as a passive eavesdropper who tries to listen in on an ongoing transmission without being detected (see, for example, models of an interference channel with an external eavesdropper [1], and of secure communications over fading channels [2] and over a fading eavesdropper channel [3]), or as a malicious user (jammer) who tries to degrade the signal quality at the intended receiver (see, for example, works on jamming principles and techniques [4], on detecting jamming attacks [5], on employing artificial noise to improve secret communication [6], on defense against jamming attacks [7], on jamming in multi-channel cognitive radio networks [8], and on jamming of dynamic traffic [9]). In [10] and [11], a new approach to dealing with this problem was suggested, namely, to consider a more sophisticated adversary with the dual capability of either eavesdropping passively or jamming any ongoing transmission, also referred to as an active eavesdropper. In particular, this problem was investigated as a zero-sum game between the user and the sophisticated adversary. That approach was further developed in [12] for the case of many adversaries and the users communicating with others located outside of a secure zone. The users can choose channels on which to communicate, while the adversaries can choose channels to jam or to eavesdrop upon, but they cannot tune the powers they employ. The problem was extended to the case in which the adversary, besides choosing a channel to attack, can tune the jamming power while the user adjusts its transmission power in OFDM (Orthogonal Frequency-Division Multiplexing) (for the low signal-to-interference-plus-noise ratio regime) [13] or CDMA (Code Division Multiple Access) networks [14]. The question of how an adversary's restricted and unknown eavesdropping capability affects the secret communication between a set of users has been investigated in [15] .

In this paper, we propose a new paradigm for the problem of an adversary's dual threat: jamming and eavesdropping. In particular, we consider the potential of incorporating in the transmission protocol a time slot dealing with the detection of a malicious threat to increase secrecy and reliability of the communication. This paradigm arises as a result of a dilemma the users face in meeting the dual jamming and eavesdropping threat. The user can either transmit and suffer from malicious activity or be in a silent mode (not transmit) and suffer from a delay in transmission. However, by properly combining these modes the user can help the IDS (Intrusion Detection System)

Manuscript received January 1, 2014; revised October 5, 2014, February 20, 2015, and July 7, 2015; accepted October 26, 2015. Date of publication November 9, 2015; date of current version March 8, 2016. This work was supported by the National Science Foundation under Grant CMMI-1436288 and Grant CMMI-1435778. The associate editor coordinating the review of this paper and approving it for publication was Y. Guan.

A. Garnaev is with the WINLAB, Rutgers University, North Brunswick, NJ 08901 USA, and also with the Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University, St. Petersburg 198504, Russia (e-mail: garnaev@yahoo.com).

M. Baykal-Gursoy is with the Department of Industrial and Systems Engineering, RUTCOR and CAIT, Rutgers University, Piscataway, NJ 08854-8018 USA (e-mail: gursoy@rci.rutgers.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2498934

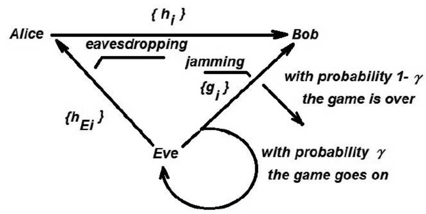


Fig. 1. Relationships between Alice, Bob and Eve in a basic stochastic game.

to detect the adversary, since transmission can provoke the adversary into a jamming attack, and strategically switching to the silent mode while the jammer continues the jamming attack can increase the probability of detecting the adversary.

To get insight into this problem, we propose two simple stochastic games played between a user and an adversary. The first one extends the static scenario of [10] and [11] to the dynamic case, while the second one includes the consideration of silent modes. We give the equilibrium strategies for the players, and values of both games in closed form. We demonstrate that use of a silent mode can be helpful in increasing secrecy and reliability of the communication. The equilibrium strategies are randomized, and thus, the user's strategy specifies a frequency of using the silent mode in the transmission protocol.

Here employing stochastic game tools is quite natural, since the user and the adversary have opposing motivations, and it is uncertain how long the adversary can manage to perform its malicious activity before it is detected. Note that game theory gives a very convenient tool to deal with various problems in network security. In [16], one can find a structured and comprehensive survey of research contributions that analyze and solve security and privacy problems in computer and wireless networks via game-theoretic approaches. Here as examples of game-theoretic approaches, we mention just a few of such works: modeling malicious users in collaborative networks [17], information warfare [18], attack-type uncertainty in a network [19], and packet transmission under jamming [20], [21]. Applications of stochastic games in modeling network security can be found in [22]–[25].

The organization of this paper is as follows: in Section II, we first introduce the model for the dual threat problem (eavesdropping and jamming). In Section III, we formulate and solve the basic stochastic game between the adversary and the user when the user employs only two transmission modes. In Section IV, we extend the basic model and solve it for the case in which the user can employ an extra mode, namely, a silent mode, in which s/he tries to trap the adversary. In Section V, numerical illustrations are presented. Finally, in Section VI, a discussion of the results is offered.

II. Background Setup of the Problem

Our motivating scenario involves a user Alice, who wishes to communicate *secretly* and *reliably* with Bob. Eve, an adversary, wants to obstruct this secret communication between Alice and Bob by means of either eavesdropping or jamming (Figure 1).

Under an eavesdropping attack, the maximum achievable rate for transmission (see, [12]) from Alice to Bob is given by the *secrecy capacity* $u_{SC}(\boldsymbol{P}) = \max\{u(\boldsymbol{P}, 0) - u_E(\boldsymbol{P}), 0\}$, where $u(\boldsymbol{P}, \boldsymbol{J})$ is the capacity of direct transmission between Alice and Bob if Alice transmits the signal $\boldsymbol{P}$ and Eve applies the jamming signal $\boldsymbol{J}$, and $u_E = u_E(\boldsymbol{P})$ is the capacity of Eve as a receiver in the eavesdropper mode.

If Eve works in eavesdropping mode (so, $\boldsymbol{J} = 0$), it is optimal for Alice to transmit a signal $\boldsymbol{P}^E$ maximizing her secrecy capacity, i.e.

$$\boldsymbol{P}^E = \operatorname*{argmax}_{\boldsymbol{P}} u_{SC}(\boldsymbol{P}).$$

If Eve employs the jamming mode, it is optimal for Alice to transmit a signal $\boldsymbol{P}^J$ that is the best response to the worst transmission condition, i.e.

$$\boldsymbol{P}^J = \operatorname*{argmax}_{\boldsymbol{P}} \min_{\boldsymbol{J}} u(\boldsymbol{P}, \boldsymbol{J}).$$

Then, the best response $\boldsymbol{P}^J$ to the worst condition

$$\boldsymbol{J}^J = \operatorname*{argmin}_{\boldsymbol{J}} \max_{\boldsymbol{P}} u(\boldsymbol{P}, \boldsymbol{J})$$

yields an equilibrium (saddle point) in such a way that for any $(\boldsymbol{P}, \boldsymbol{J})$ the following inequalities hold:

$$u\left(\boldsymbol{P}, \boldsymbol{J}^J\right) \le u := u\left(\boldsymbol{P}^J, \boldsymbol{J}^J\right) \le u\left(\boldsymbol{P}^J, \boldsymbol{J}\right),$$

where u is called the value of the game, which is the payoff to Alice at the equilibrium/saddle point.

In this paper, as a basic example we consider a wireless medium with n separate channels (e.g. different subcarriers in an OFDM system), which we model as additive white Gaussian noise (AWGN) channels. Thus, Alice communicates to Bob across n (sub)channels, and the channel responses for these n channels are represented by coefficients h_i, $i \in [1, n]$. The channels from Eve to Alice have corresponding coefficients h_{Ei}, where $h_{Ei} \le h_i$, while the coefficients for the channels from Eve to Bob are represented by g_i. Hence, h_{Ei} is associated with eavesdropping, while g_i is associated with jamming. Also, $\boldsymbol{P} = (P_1, \dots, P_n)$ is a strategy of Alice, where P_i is a signal transmitted by Alice through channel i, $\sum_{i=1}^n P_i = \bar{P}$, and $\bar{P}$ is the total transmitted signal. $\boldsymbol{J} = (J_1, \dots, J_n)$ is a strategy of Eve, where J_i is a jamming signal employed by Eve to jam channel i, $\sum_{i=1}^n J_i = \bar{J}$, and $\bar{J}$ is the total jamming signal. Then,

$$u(\boldsymbol{P}, \boldsymbol{J}) = \sum_{i=1}^n \ln\left(1 + \frac{h_i P_i}{\sigma^2 + g_i J_i}\right),$$

$$u_E(\boldsymbol{P}) = \sum_{i=1}^n \ln\left(1 + \frac{h_{Ei} P_i}{\sigma_E^2}\right),$$

$$u_{SC}(\boldsymbol{P}) = \sum_{i=1}^n \left(\ln\left(1 + \frac{h_i P_i}{\sigma^2}\right) - \ln\left(1 + \frac{h_{Ei} P_i}{\sigma_E^2}\right)\right),$$

where σ^2 and σ_E^2 are the variances of background noises of the main and eavesdropping channels, respectively. An algorithm suggested in [26] can be employed to find the optimal strategy $\boldsymbol{P}^E$ of Alice in eavesdropping mode, while the equilibrium strategies $\boldsymbol{P}^J$ and $\boldsymbol{J}^J$ can be calculated by using the results in [27] for moderate SNR (Signal to Noise Ratio) and in [28] and [29] for low SNR regimes.

III. Basic Game

In this section, we consider Eve as an active agent, who can choose a mode in which to work. Besides the payoffs there is another important difference between jamming and eavesdropping modes, namely, in jamming mode Eve can be detected and her malicious activity can be stopped by eliminating her from the game. We assume that there is a probability $1-\gamma$ of detecting Eve in jamming mode by an IDS. Note that there is quite an extended literature on detecting an intruder's signal or its source (see, for example, books [30]–[32], and papers on the energy detection of the unknown signals [33], [34] and on game-theoretic models of the optimal scanning bandwidth problem [35], [36]). Thus, γ is the probability of not detecting the adversary.

We assume that all the actions (the transmission by Alice and the malicious activity of Eve) are performed in discrete time slots $1, 2, \dots, \infty$ (Figure 1). At each time slot, while Eve is not detected and, so, not eliminated from the game Eve can choose between eavesdropping and jamming modes (respectively denoted by E and J). If jamming mode is selected, then she applies jamming power allocation $\boldsymbol{J}^J$. Alice can choose between two signals to transmit, $\boldsymbol{P}^E$ and $\boldsymbol{P}^J$ (in other words, between two actions denoted by E and J that are the best responses to the eavesdropping and jamming modes of Eve, respectively). If Eve is detected and, so, eliminated from the game, Alice could safely switch to employing the optimal signal for transmission when there are no malicious threats, i.e., $\boldsymbol{P}_0 = \operatorname*{argmax}_{\boldsymbol{P}} u(\boldsymbol{P}, 0)$. Let $\bar{u} := u(\boldsymbol{P}_0, 0)$. If Eve is not detected then the game moves to the next time slot and is played recursively with discount factor δ. This δ can be interpreted as a measure of urgency in communications: $\delta = 0$ corresponds to the highest urgency and means that transmission has to be performed during the current time slot, not later, while increasing δ means that losing a transmission time slot can be more easily compensated in the following time slots. For the sake of brevity, we assume that in both transmission modes the detection probability is the same and is equal to $1-\gamma$. This assumption is motivated by our basic example that Alice in both modes does not reduce the signal, but just reallocates it between channels. So, in general Alice's action does not influence the ability of the IDS to detect intrusion.

This game can be considered as a two-state stochastic game as shown in Fig. 2. State 1 represents the malicious state in which Alice is vulnerable to an attack by Eve, while state 2 represents the state in which Eve is detected and is not a threat to Alice anymore. The matrix notation used for each state i is such that each entry corresponds to an action pair (E, J) of Alice and Eve. The value in the upper left corner of each entry is the instantaneous payoff (current transmission rate) to Alice in this zero-sum stochastic game, while the lower diagonal gives the probability distribution over the future states. For example, in state 1 if both Alice and Eve use their action E, then the instantaneous payoff to Alice is $u_{SC}(\mathbf{P^E})$ and the next state is state 1. On the other hand, if Alice and Eve choose the action pair (E, J), the payoff is $u(\mathbf{P^E}, \mathbf{J^J})$ and the next state is state 1 or state 2 with probabilities γ and $1-\gamma$, respectively. Note that the payoff at the next epoch is discounted with discount rate δ.

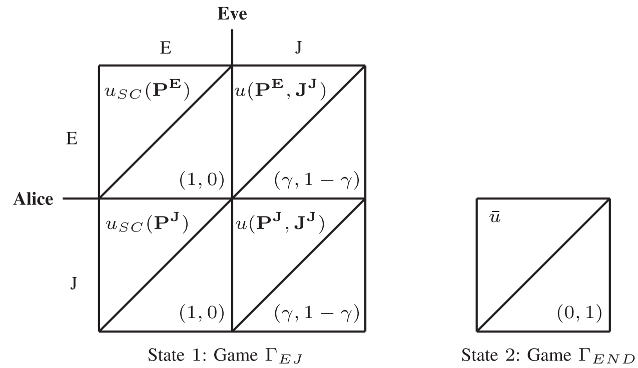


Fig. 2. State transitions and instantaneous payoffs of the stochastic game.

We denote the game played in state 1 as Γ_{EJ} and in state 2 as Γ_{END}. However, since in state 2 the game ends and Alice can continuously transmit with rate $\bar{u}$, the total discounted payoff in state 2 is equal to $(1+\delta+\delta^2+\cdots)\bar{u} = \frac{\bar{u}}{1-\delta}$. Hence from now on we will only consider the malicious state, and using the notation in [37, Chapter V.3] and [38, Part II] on page II-71 equation (8), we will denote the stochastic game Γ_{EJ} as given below.

$$\Gamma_{EJ} = \begin{array}{c} \\ E \\ \\ J \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} \qquad E \qquad\qquad & \qquad\qquad J \end{array} \\ \begin{pmatrix} u_{SC}\left(\boldsymbol{P}^E\right) + \delta\Gamma_{EJ} & u\left(\boldsymbol{P}^E, \boldsymbol{J}^J\right) + \gamma\delta\Gamma_{EJ} \\ & +(1-\gamma)\delta\frac{\bar{u}}{1-\delta} \\ u_{SC}\left(\boldsymbol{P}^J\right) + \delta\Gamma_{EJ} & u\left(\boldsymbol{P}^J, \boldsymbol{J}^J\right) + \gamma\delta\Gamma_{EJ} \\ & +(1-\gamma)\delta\frac{\bar{u}}{1-\delta} \end{pmatrix} \end{array}.$$

We are going to solve this game in stationary strategies, i.e., the strategies that are independent of history and current time. Since this game is discounted, it has an equilibrium in stationary strategies, and its solution is given as a solution to the Shapley (-Bellmann) equation [37, Chapter V.3]:

$$\begin{aligned} v &= \operatorname{val}\begin{pmatrix} v_E + \delta v & v_{EJ} + \gamma\delta v \\ v_J + \delta v & v_{JJ} + \gamma\delta v \end{pmatrix} \\ &= \max_{\boldsymbol{x}} \min_{\boldsymbol{y}} \begin{pmatrix} x_E \\ x_J \end{pmatrix}^T \begin{pmatrix} v_E + \delta v & v_{EJ} + \gamma\delta v \\ v_J + \delta v & v_{JJ} + \gamma\delta v \end{pmatrix} \begin{pmatrix} y_E \\ y_J \end{pmatrix}, \end{aligned} \tag{1}$$

where $v = \operatorname{val}(\Gamma_{EJ})$ is the value of the game, $\boldsymbol{x} = (x_E, x_J)$ is the stationary (mixed) strategy of Alice assigning the probabilities x_E and x_J to using actions E and J, $\boldsymbol{y} = (y_E, y_J)$ is the stationary (mixed) strategy of Eve assigning the probabilities y_E and y_J to using actions E and J, respectively (so, $x_E + x_J = 1$ and $y_E + y_J = 1$) and[1]

$$\begin{aligned} v_E &:= u_{SC}\left(\boldsymbol{P}^E\right) \text{ and } v_J := u_{SC}\left(\boldsymbol{P}^J\right), \\ v_{EJ} &:= u\left(\boldsymbol{P}^E, \boldsymbol{J}^J\right) + (1-\gamma)\frac{\delta\bar{u}}{1-\delta}, \\ v_{JJ} &:= u\left(\boldsymbol{P}^J, \boldsymbol{J}^J\right) + (1-\gamma)\frac{\delta\bar{u}}{1-\delta}. \end{aligned} \tag{2}$$

[1]Note that a more complete notation for these v would be v_{EE}, v_{EJ}, v_{JE} and v_{JJ}, which takes into account all pure strategies applied by the players. However, this notation makes the formulas too bulky for a two-column format. This is the reason why we have indexed only Alice's action (the first player) and active action of Eve (the second player).

Since the game is zero-sum, $\max_x \min_y$ coincides with $\min_y \max_x$ in (1).

We assume that $\boldsymbol{P}^E \neq \boldsymbol{P}^J$. Then, by the definitions of $\boldsymbol{P}^E$ and $\boldsymbol{P}^J$ the following inequalities hold:

$$\nu_E > \nu_J \text{ and } \nu_{JJ} > \nu_{EJ}. \tag{3}$$

Note that, by (2), $\frac{\nu_E}{1-\delta}$, $\frac{\nu_J}{1-\delta}$, $\frac{\nu_{EJ}}{1-\delta\gamma}$ and $\frac{\nu_{JJ}}{1-\delta\gamma}$ are the expected payoffs to Alice if the rivals employ stationary strategy pairs (E, E), (J, E), (E, J) and (J, J), respectively.

In spite of the fact that the maximin equation (1) is implicit in v, it is possible to solve it explicitly and to evaluate the stationary equilibrium strategies in closed form.

Theorem 1: The game Γ_{EJ} has a unique stationary equilibrium strategy pair $(\boldsymbol{x}, \boldsymbol{y}) = ((x, 1-x), (y, 1-y))$ and the value of the game, v, is given as follows:

(a) if the expected payoff to Alice for stationary strategy pair (E, E) is not greater than for (E, J), i.e.

$$\frac{\nu_E}{1-\delta} \leq \frac{\nu_{EJ}}{1-\delta\gamma}, \tag{4}$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (E, E)$ (so, $x = y = 1$) and $v = \frac{\nu_E}{1-\delta}$;

(b) if the expected payoff to Alice for stationary strategy pair (J, J) is not greater than for (J, E), i.e.

$$\frac{\nu_{JJ}}{1-\delta\gamma} \leq \frac{\nu_J}{1-\delta}, \tag{5}$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (J, J)$ (so, $x = y = 0$) and $v = \frac{\nu_{JJ}}{1-\gamma\delta}$;

(c) if conditions of (a) and (b) do not hold, i.e.

$$\frac{\nu_{EJ}}{1-\delta\gamma} < \frac{\nu_E}{1-\delta} \text{ and } \frac{\nu_J}{1-\delta} < \frac{\nu_{JJ}}{1-\delta\gamma}, \tag{6}$$

then a mixed stationary equilibrium arises, namely,

$$\begin{aligned}
x = X_{EJ} &:= \frac{(1-\delta)\nu_{JJ} - (1-\delta\gamma)\nu_J}{(1-\delta)(\nu_{JJ} - \nu_{EJ}) + (1-\gamma\delta)(\nu_E - \nu_J)}, \\
y = Y_{EJ} &:= \frac{\nu_{JJ} - \nu_{EJ}}{\nu_{JJ} - \nu_{EJ} + \nu_E - \nu_J}, \\
v = V_{EJ} &:= \frac{\nu_{JJ}\nu_E - \nu_{EJ}\nu_J}{(1-\delta)(\nu_{JJ} - \nu_{EJ}) + (1-\gamma\delta)(\nu_E - \nu_J)}.
\end{aligned} \tag{7}$$

It is quite interesting to note that by (2) and (7), the optimal probability, x, for Alice to communicate in eavesdropping mode is continuous in the probability, γ, of not detecting Eve, and the discount factor δ. While the optimal probability, y, for Eve to eavesdrop is piecewise constant in these parameters. Of course, the boundary of the domains, where the corresponding equilibria are applied, depends on γ and δ continuously. So, Alice is more flexible in her behavior while Eve is more straightforward. Figure 3 illustrates where domains of using pure and mixed equilibria are located.

Proof: By (3) only (E, E) and (J, J) can be pure equilibria. Also, (E, E) is an equilibrium if and only if $v = \nu_E + \delta v$ and $\nu_E + \delta v \leq \nu_{EJ} + \gamma\delta v$, and (a) follows. (J, J) is an equilibrium if and only if $v = \nu_{JJ} + \gamma\delta v$ and $\nu_J + \delta v \geq \nu_{JJ} + \gamma\delta v$, and (b) follows.

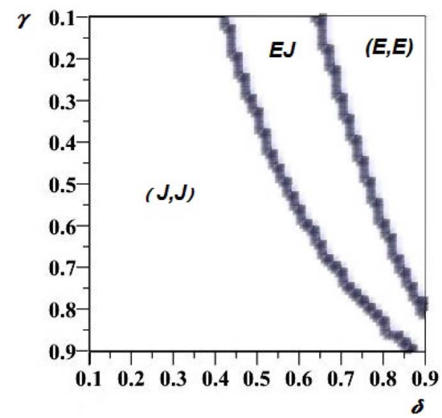


Fig. 3. Domains of using pure and mixed equilibria for $u_E = 0.8$, $u_J = 0.8$, $u_{EJ} = 0.3$, $u_{JJ} = 0.6$ and $\bar{u} = 1.1$. Here (J, J) and (E, E) are pure equilibria, while EJ is an abbreviation for the mixed equilibrium strategy, which is constructed by randomizing pure strategies E and J.

If conditions of (a) and (b) do not hold then equilibrium has to be found in mixed strategies (so, $0 < x, y < 1$). For a 2×2 matrix game such equilibrium strategies are the ones that equalize the payoffs, i.e.

$$\begin{aligned}
(\nu_E + \delta v)y + (\nu_{EJ} + \gamma\delta v)(1-y) &= v, \\
(\nu_J + \delta v)y + (\nu_{JJ} + \gamma\delta v)(1-y) &= v, \\
(\nu_E + \delta v)x + (\nu_J + \delta v)(1-x) &= v, \\
(\nu_{EJ} + \gamma\delta v)x + (\nu_{JJ} + \gamma\delta v)(1-x) &= v.
\end{aligned} \tag{8}$$

Solving these equations for x, y and v implies (7). By (3), $0 < y < 1$. While the condition that $0 < x < 1$ is equivalent to conditions (6), and the result follows. ■

IV. Extended Game

In this section, we consider an extension of the model of the previous section in which Alice can also try to trap Eve by employing an extra mode, namely, a silent mode. Thus, understanding that the communication can be corrupted motivates Alice to provoke Eve into jamming mode to detect her and remove her from intrusion, and then to switch to the most efficient way of communication. To study this problem we extend our stochastic game by allowing Alice to use an extra action denoted by S when she is in a silent or quiet mode, and not transmitting signals to Bob, in order to increase the probability that the IDS detects Eve. By using this action, Alice may lose time due to the delay in transmitting signals to Bob. However, Alice can benefit from the earlier detection of Eve and hence earlier resumption of the more efficient regime of transmission. If Alice uses such a strategy and if Eve eavesdrops, then Eve is not detected, and thus, the game is repeated again in the next time slot with discount factor δ (Figure 4). If Eve jams she can be detected with probability $1 - \gamma_S > 1 - \gamma$ (and not detected with probability $\gamma_S < \gamma$), so in the silent mode the probability of Eve's detection by the IDS is greater than in one of the other two transmission modes. This scenario can be described by a stochastic game Γ_{EJS} with one (malicious) state (i.e. when

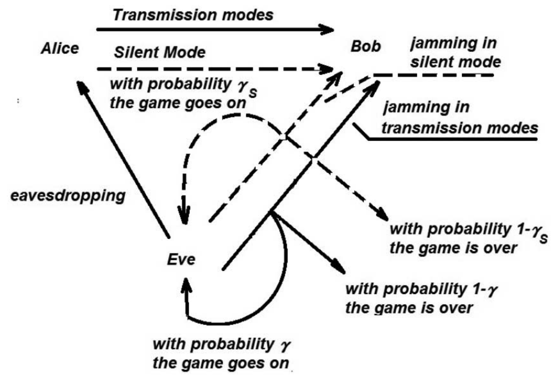


Fig. 4. Relationships between Alice, Bob and Eve in the extended stochastic game.

Alice is under malicious threat from Eve) using a matrix form as follows:

$$\Gamma_{EJS} = \begin{array}{c} \\ E \\ \\ J \\ \\ S \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} E & J \end{array} \\ \begin{pmatrix} u_{SC}(\boldsymbol{P}^E) + \delta\Gamma & u(\boldsymbol{P}^E, \boldsymbol{J}^J) + \gamma\delta\Gamma \\ & +(1-\gamma)(\delta + \delta^2 + \cdots)\bar{u} \\ u_{SC}(\boldsymbol{P}^J) + \delta\Gamma & u(\boldsymbol{P}^J, \boldsymbol{J}^J) + \gamma\delta\Gamma \\ & +(1-\gamma)(\delta + \delta^2 + \cdots)\bar{u} \\ \delta\Gamma & \gamma_S\delta\Gamma \\ & +(1-\gamma_S)(\delta + \delta^2 + \cdots)\bar{u} \end{pmatrix} \end{array}.$$

Again we are going to solve this game in stationary strategies using the Shapley (-Bellmann) equation [37]:

$$v = \max_{\boldsymbol{x}} \min_{\boldsymbol{y}} \begin{pmatrix} x_E \\ x_J \\ x_S \end{pmatrix}^T \begin{pmatrix} \nu_E + \delta v & \nu_{EJ} + \gamma\delta v \\ \nu_J + \delta v & \nu_{JJ} + \gamma\delta v \\ \delta v & \nu_S + \gamma_S\delta v \end{pmatrix} \begin{pmatrix} y_E \\ y_J \end{pmatrix}, \quad (9)$$

where $\nu_S = (1-\gamma_S)\frac{\delta\bar{u}}{1-\delta}$, $v = \mathrm{val}(\Gamma)$ is the value of the game, $\boldsymbol{x} = (x_E, x_J, x_S)$ is the stationary (mixed) strategy of Alice assigning probabilities x_E, x_J and x_S to employ strategies E, J and S respectively, and $x_E + x_J + x_S = 1$.

To solve this game we introduce two auxiliary stochastic games, Γ_{ES} and Γ_{JS}. Γ_{ES} is the 2×2 sub-game of the 3×2 game Γ_{EJS} with two strategies of Alice, E and S. Γ_{JS} is also the 2×2 sub-game of the 3×2 game Γ, with two strategies of Alice, J and S. Similar to the proof of Theorem 1 we can show the following result.

Theorem 2: The sub-game Γ_{DS}, where $D = E$ or $D = J$, has the unique stationary equilibrium strategy pair $(\boldsymbol{x}, \boldsymbol{y}) = ((x, 1-x), (y, 1-y))$ and the value of the game is v given as follows:

(a) if the expected payoff to Alice for stationary strategy pair (D, E) is not greater than for (D, J), i.e.

$$\frac{\nu_D}{1-\delta} \leq \frac{\nu_{DJ}}{1-\delta\gamma}, \quad (10)$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (D, E)$ and $v = \frac{\nu_D}{1-\delta}$;

(b) if the expected payoff to Alice for stationary strategy pair (D, J) is not greater than for (D, E) and is not less than for (S, J), i.e.

$$\frac{\nu_{DJ}}{1-\delta\gamma} \leq \frac{\nu_D}{1-\delta} \text{ and } \frac{\nu_S}{1-\delta\gamma_S} \leq \frac{\nu_{DJ}}{1-\delta\gamma}, \quad (11)$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (D, J)$ and $v = \frac{\nu_{DJ}}{1-\gamma\delta}$;

(c) if the conditions of (a) and (b) do not hold, i.e.

$$\frac{\nu_{DJ}}{1-\delta\gamma} \leq \frac{\nu_D}{1-\delta} \text{ and } \frac{\nu_{DJ}}{1-\delta\gamma} < \frac{\nu_S}{1-\delta\gamma_S}, \quad (12)$$

then an equilibrium in mixed strategies arises, namely, $x = X_{DS}$, $y = Y_{DS}$ and $v = V_{DS}$, where $y = y_{DS}$ is the unique root in (0, 1) of the quadratic equation: $F_D(y) = a_2y^2 + a_1y + a_0 = 0$, with $a_2 := (\nu_D(1-\gamma_S) + \nu_S(1-\gamma) - \nu_{DJ}(1-\gamma_S))\delta$, $a_1 := \nu_{DJ}(1+\delta(1-2\gamma_S)) - \nu_D(1-\delta\gamma_S) - \nu_S(1+\delta(1-2\gamma))$, $a_0 := \nu_S(1-\gamma\delta) - \nu_{DJ}(1-\gamma_S\delta)$, and

$$V_{DS} := \frac{\nu_{DJ}(1-y_{DS}) + \nu_E y_{DS}}{1-\delta(\gamma + (1-\gamma)y_{DS})} \text{ and } X_{DS} := \frac{1-\delta}{\nu_D}V_{DS}. \quad (13)$$

Note that, since $F_D(1) = -(1-\delta)\nu_E < 0$, $F_D(0) = a_0 > 0$ by (12), and $a_2 > 0$ by (12) such a y exists, and it is unique.

Theorem 3: The game Γ_{EJS} has the unique stationary equilibrium strategies $(\boldsymbol{x}, \boldsymbol{y}) = ((x_E, x_J, x_S), (y, 1-y))$ and the value of the game is v given as follows:

(a) if the expected payoff to Alice for stationary strategies (E, E) is not greater than for (E, J), i.e.

$$\frac{\nu_E}{1-\delta} \leq \frac{\nu_{EJ}}{1-\delta\gamma}, \quad (14)$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (E, E)$ and $v = \frac{\nu_E}{1-\delta}$;

(b) if the expected payoff to Alice for stationary strategies (J, J) is not greater than for (J, E), and is not less than for (S, J), i.e.

$$\frac{\nu_{JJ}}{1-\gamma\delta} \leq \frac{\nu_J}{1-\delta} \text{ and } \frac{\nu_S}{1-\delta\gamma_S} \leq \frac{\nu_{JJ}}{1-\delta\gamma}, \quad (15)$$

then $(\boldsymbol{x}, \boldsymbol{y}) = (J, J)$ and $v = \frac{\nu_{JJ}}{1-\gamma\delta}$;

(c_1) if

$$\frac{\nu_{EJ}}{1-\delta\gamma} < \frac{\nu_E}{1-\delta} \text{ and } \nu_J < \frac{1-\delta}{1-\gamma\delta}\nu_{JJ}, \quad (16)$$

and

$$L_S(Y_{EJ}, V_{EJ}) \leq V_{EJ}, \quad (17)$$

where $L_S(y, v) := \delta v y + (\nu_S + \delta\gamma_S v)(1-y)$, then $(\boldsymbol{x}, \boldsymbol{y}) = ((X_{EJ}, 1-X_{EJ}, 0), (Y_{EJ}, 1-Y_{EJ}))$ and the value of the game $v = V_{EJ}$;

(c_2) if (16) holds and (17) does not hold, then $(\boldsymbol{x}, \boldsymbol{y}) = ((X_{ES}, 0, 1-X_{ES}), (Y_{ES}, 1-Y_{ES}))$, and the value of the game is $v = V_{ES}$;

(d_1) if

$$\frac{\nu_{EJ}}{1-\delta\gamma} < \frac{\nu_E}{1-\delta}, \ \nu_J > \frac{1-\delta}{1-\gamma\delta}\nu_{JJ} \text{ and } \frac{1-\delta\gamma_S}{1-\delta\gamma}\nu_{JJ} \leq \nu_S \quad (18)$$

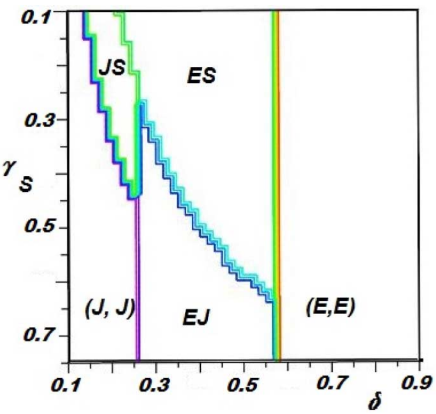


Fig. 5. Domains of using pure and mixed equilibria for $u_E = 1.3$, $u_J = 0.8$, $u_{EJ} = 0.3$, $u_{JJ} = 0.5$, $\bar{u} = 5$ and $\gamma = 0.8$. Here (J, J) and (E, E) are pure equilibria, while EJ, ES and JS are abbreviations for the mixed equilibrium strategies constructed by randomizing the corresponding pure strategies.

and

$$L_S(Y_{EJ}, V_{EJ}) \geq V_{EJ}, \tag{19}$$

then $(\boldsymbol{x}, \boldsymbol{y}) = ((X_{ES}, 0, 1 - X_{ES}), (Y_{ES}, 1 - Y_{ES}))$ and the value of the game $v = V_{ES}$;

(d_2) if (18) holds and (19) does not hold, then $(\boldsymbol{x}, \boldsymbol{y}) = ((0, X_{JS}, 1 - X_{JS}), (Y_{JS}, 1 - Y_{JS}))$ and the value of the game $v = V_{JS}$.

Proof: By (3) only (E, E), (J, J) and (S, J) can be pure equilibria. Also, (E, E) is an equilibrium if and only if $v = \nu_E + \delta v$ and $\nu_E + \delta v \leq \nu_{EJ} + \gamma\delta v$, and (a) follows. (J, J) is an equilibrium if and only if $v = \nu_{JJ} + \gamma\delta v$ and $\nu_J + \delta v \geq \nu_{JJ} + \gamma\delta v \geq \nu_S + \gamma_S\delta v$, and (b) follows.

Now we prove that (S, J) cannot be a pure equilibrium. Assume that (S, J) is an equilibrium. Then $v = \nu_S + \gamma_S\delta v$, so $v = \nu_S/(1 - \gamma_S\delta)$ and $\delta v \geq \nu_S + \gamma_S\delta v \geq \nu_{JJ} + \gamma\delta$. Substituting v into the first of these inequalities implies $\delta(1 - \gamma_S) \geq 1 - \gamma_S\delta$. This contradiction yields that (S, J) cannot be a pure equilibrium.

Suppose the conditions of (a) and (b) do not hold. Then an equilibrium exists in mixed strategies. The value of the game v is a solution to the equation $v = w(v)$, where $w(v)$ for a fixed v is a solution of the following LP (linear programming) problem:

$$\begin{aligned}
&\min w(v):\\
&\quad L_E(y, v) := (\nu_E + \delta v)y + (\nu_{EJ} + \gamma\delta v)(1 - y) \leq w(v),\\
&\quad L_J(y, v) := (\nu_J + \delta v)y + (\nu_{JJ} + \gamma\delta v)(1 - y) \leq w(v),\\
&\quad L_S(y, v) := \delta v y + (\nu_S + \delta\gamma_S v)(1 - y) \leq w(v),\\
&0 \leq y \leq 1.
\end{aligned} \tag{20}$$

Let (16) hold. Then, by Theorem 1(c), there is a mixed equilibrium in the game Γ_{EJ}. Thus, L_E is increasing and L_J is decreasing in y and these lines intersect at the point $y = Y_{EJ}$. Further, by (20) (Figure 6), the value of the game is V_{EJ} if (17) holds and it is V_{ES} if (17) does not hold, and thus (c_1) and (c_2) follow.

Let (18) hold. Then, by Theorem 1(b), (J, J) is a pure equilibrium in the game Γ_{EJ}. Then L_E and L_J are increasing in

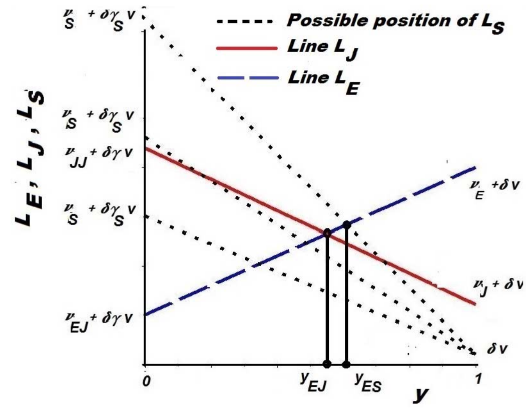


Fig. 6. Evaluation of Eve's equilibrium strategy and the value of the game. Case (c) of Theorem 3.

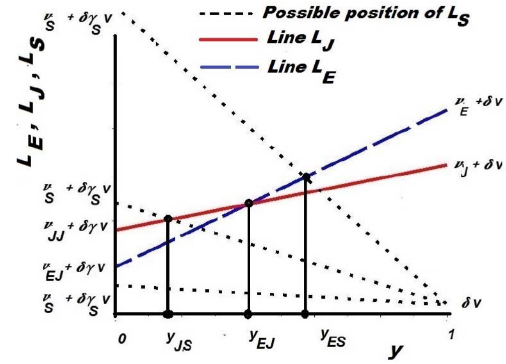


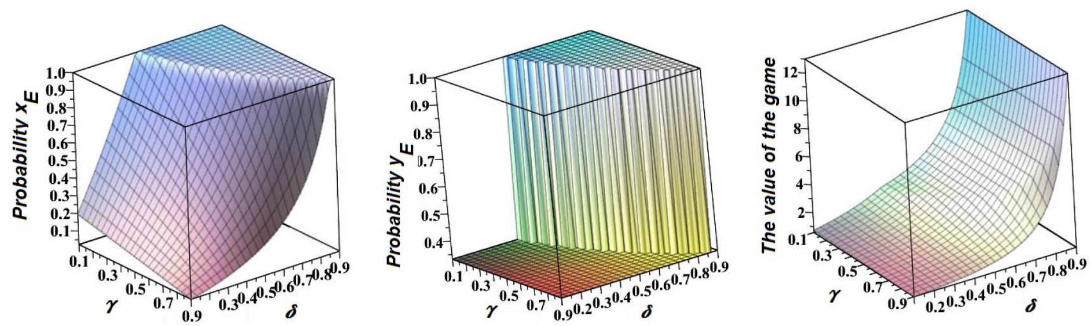
Fig. 7. Evaluation of Eve's equilibrium strategy and the value of the game. Case (d) of Theorem 3.

y, and these lines intersect at the point $y = Y_{EJ}$. So, by (20) (Figure 7), the value of the game is V_{ES} if (19) holds and it is V_{JS} if (19) does not hold, and thus (d_1) and (d_2) follow. ■

It is quite natural that there is no pure equilibrium that includes Alice's silent action as a component. Since the best response by Eve to such a strategy of Alice is to eavesdrop, Alice can never deliver any information to Bob without being eavesdropped upon and Eve is never detected. To increase the payoff by means of a new possibility made available by the silent mode, Alice has to risk losing either secrecy or reliability and jointly use silence and one of the transmission modes to provoke Eve to jam. Figure 5 illustrates how domains of using pure and mixed equilibria are located.

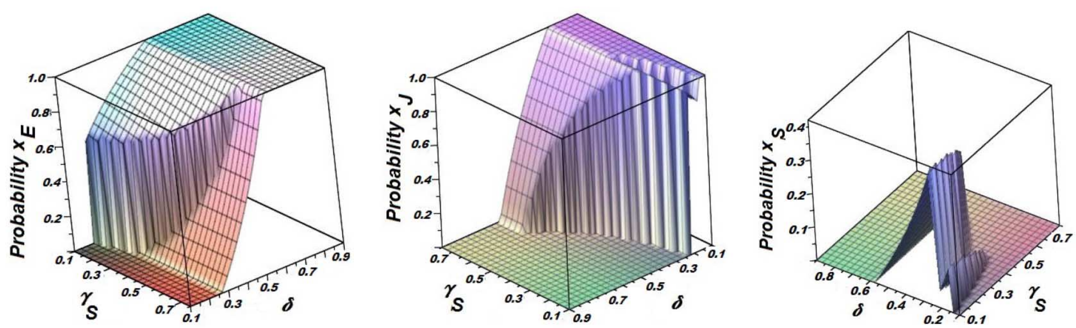
V. Numerical Illustration

We first consider the basic game in which Alice can only transmit. We investigate through numerical examples how Alice's optimal probability to transmit in eavesdropping mode, x_E, Eve's optimal eavesdropping probability, y_E, and the value of the game depend on the probability, γ, that Eve is not detected in the jamming mode and the discount factor δ. Assume $\nu_E = 1.3$, $\nu_J = 0.5$, $\nu_{EJ} = 0.1$, $\nu_{JJ} = 0.5$ and $\bar{u} = 3$ (Figure 8). The optimal probability, x_E, of Alice to transmit in eavesdropping mode is continuous and decreasing in the probability γ. This is quite reasonable since decreasing the



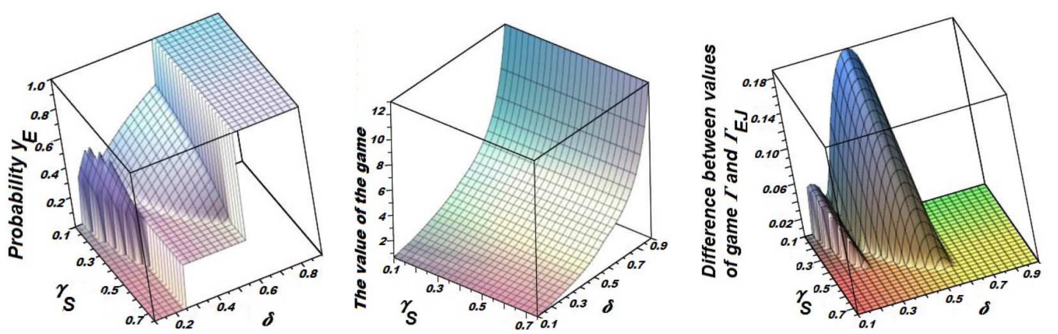
(a) (b) (c)

Fig. 8. (a) The optimal probability x_E for Alice to communicate in eavesdropping mode, (b) the optimal probability y_E for Eve to eavesdrop, and (c) the value of the game as functions of the probability γ and discount factor δ in the game Γ_{EJ}.



(a) (b) (c)

Fig. 9. The optimal probability for Alice to communicate: (a) in eavesdropping mode, (b) in jamming mode, and (c) in silent mode.



(a) (b) (c)

Fig. 10. (a) The optimal probability for Eve to eavesdrop, (b) the value of the game Γ, (c) the difference between the values of the games Γ and Γ_{EJ}.

chance of not being detected makes jamming mode safer for Eve; thus, Eve focuses on reducing reliability of the communication between Alice and Bob. This forces Alice to focus more on reliable rather than secret communications. That is why Alice increases the probability of transmitting in jamming mode. Eve's probability of eavesdropping, y_E, is piecewise constant and is a decreasing function of the probability γ. The value of the game is continuously decreasing in γ since a larger probability that Eve is not detected allows her to perform her malicious activity for longer periods and to cause greater damage to Alice's communication with Bob. An increasing discount factor δ implies reduction in the urgency of communication, and it leads to switching to more secure communication. This in turn increases the probability of using eavesdropping mode by Alice and Eve, and thus, increases the value of the game.

Let $\nu_E = 1.3$, $\nu_J = 0.8$, $\nu_{EJ} = 0.3$, $\nu_{JJ} = 0.5$, $\bar{u} = 5$ and $\gamma = 0.8$. For the game Γ, where Alice has three options, Figures 9 and 10 show that the equilibrium strategy (x_E, x_J, x_S) of Alice, the optimal probability of eavesdropping, y_E, by Eve and the value, v, of the game depend on the probability γ_S of jamming being undetected in silent mode and the discount factor δ. It is interesting that the optimal probabilities x_E, x_J, x_S and y_E are piece-wise continuous functions of γ_S and δ, while the value of the game is continuous and monotonic. Jumps in x_E, x_J, x_S and y_E can take place on the boundaries of domains (Figure 5) where one type of equilibrium switches to the other. Figure 10(c) illustrates how the silent mode incorporated in Alice's strategy can increase her payoff depending on the urgency of transmission (discount factor δ) and parameters of the IDS (the probability of not detecting γ_S). To increase her payoff by using silent mode Alice has to risk losing either secrecy or reliability jointly using silent and one of the transmission modes. So, improvement takes place in the domains ES and JS, while in the domains EJ, (E, E) and (J, J) (Figure 5) the value of the game coincides with the one in which the silent mode is not employed.

VI. Conclusions

In this paper, we have introduced and analyzed a new paradigm that can be useful for secret and reliable communication, namely, incorporating in the transmission protocol a time slot dealing only with detection of a malicious threat to improve the secrecy and reliability of communication. To deal with this problem two stochastic games have been proposed and solved explicitly. The first one extends the static game between a user and a sophisticated adversary who can execute two threats: jamming and eavesdropping ([10] and [11]) to a dynamic stochastic game, in which the adversary in jamming mode can be detected by the IDS. The second game extends the first by allowing the user to also implement a silent mode. Explicit solution of these stochastic games demonstrates that such a silent mode increases the secrecy and reliability of communication, and the resulting randomized strategy specifies the frequency of using the silent mode.

References

[1] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communications over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[3] Z. Li, R. Yates, and W. Trappe, "Secure communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2007, pp. 1296–1300.

[4] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Norwood, MA, USA: Artech House, 2006.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. MobiHoc*, 2005, pp. 46–57.

[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Veh. Technol. Conf. (VTC'05-Fall)*, 2005, vol. 3, pp. 1906–1910.

[7] W. Xu, "Jamming attack defense," in *Encyclopedia of Cryptography and Security*, Tilborg H. C. A and S. Jajodia, Eds. New York, NY, USA: Springer, 2011, pp. 655–661.

[8] Y. Wu, B. Wang, K. J. R Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 4–15, Jan. 2012.

[9] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games for power controlled medium access with dynamic traffic," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2010, pp. 1818–1822.

[10] G. T Amariucai, "Physical security in wireless networks: Intelligent jamming and eavesdropping," Ph.D. dissertation, Dept. Elect. Comput. Eng., Louisiana State University, Baton Rouge, LA, USA, 2009.

[11] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proc. Mil. Commun. Conf. (MILCOM)*, 2010, pp. 1695–1700.

[12] 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 *Proc. Mil. Commun. Conf. (MILCOM)*, 2011, pp. 119–124.

[13] A. Garnaev and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 753–757.

[14] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Ad Hoc Networks*, M. H. Sherif, A. Mellouk, J. Li, and P. Bellavista, Eds. New York, NY, USA: Springer, 2014, pp. 146–161.

[15] A. Garnaev and W. Trappe, "Secret communication when the eavesdropper might be an active adversary," in *Multiple Access Communications*, M. Jonsson, A. Vinel, B. Bellalta, and E. Belyaev, Eds. New York, NY, USA: Springer, 2014, pp. 121–136.

[16] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Survey*, vol. 45, no. 3, pp. 1–45, 2013.

[17] G. Theodorakopoulos and J. S. Baras, "Game theoretic modeling of malicious users in collaborative networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1317–1327, Sep. 2008.

[18] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "Challenges to applying game theory to the domain of information warfare," in *Proc. 4th Inf. Survivability Workshop (ISW'02)*, 2002, 4pp.

[19] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1278–1287, Aug. 2014.

[20] A. Garnaev, Y. Hayel, E. Altman, and K. Avrachenkov, "Jamming game in a dynamic slotted ALOHA network," in *Game Theory for Networks*, R. Jain and R. Kannan, Eds. New York, NY, USA: Springer, 2012, pp. 429–443.

[21] Y. E. Sagduyu and A. Ephremidess, "A game-theoretic analysis of denial of service attacks in wireless random access," *J. Wireless Netw.*, vol. 15, pp. 651–666, 2009.

[22] K. C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," in *Proc. Int. Conf. Game Theory Netw. (GameNets)*, 2009, pp. 697–703.

[23] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[24] A. Garnaev and W. Trappe, "Anti-jamming strategies: A stochastic game approach," in *Mobile Networks and Management*, R. Aguero, T. Zinner, R. Goleva, A. Timm-Giel, and P. Tran-Gia, Eds. New York, NY, USA: Springer, 2015, pp. 230–243.

[25] G. Calinescu, S. Kapoor, K. Qiao, and J. Shin, "Stochastic strategic routing reduces attack effects," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2011, pp. 1–5.

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

[27] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming game in wireless networks with transmission cost," in *Network Control and Optimization*, T. Chahed and B. Tuffin, Eds. New York, NY, USA: Springer, 2007, pp. 1–12.

[28] E. Altman, K. Avrachenkov, and A. Garnaev, "Transmission power control game with SINR as objective function," in *Network Control and Optimization*, E. Altman and A. Chaintreau, Eds. New York, NY, USA: Springer, 2009, pp. 112–120.

[29] A. Garnaev, Y. Hayel, and E. Altman, "A Bayesian jamming game in an OFDM wireless network," in *Proc. 10th Int. Symp. Model. Optim. Mobile Ad Hoc Wireless Netw. (WIOPT)*, 2012, pp. 41–48.

[30] C. Comaniciu, N. B. Mandayam, and H. V. Poor, *Wireless Networks: Multiuser Detection in Cross-Layer Design*. New York, NY, USA: Springer, 2005.

[31] S. Verdú, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[32] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York, NY, USA: Springer, 1994.

[33] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[34] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2003, pp. 3575–3579.

[35] A. Garnaev and W. Trappe, "Stationary equilibrium strategies for bandwidth scanning," in *Multiple Access Communications*, M. Jonsson, A. Vinel, B. Bellalta, N. Marina, D. Dimitrova, and D. Fiems, Eds. New York, NY, USA: Springer, 2013, pp. 168–183.

[36] A. Garnaev, W. Trappe, and C.-T. Kung, "Dependence of optimal monitoring strategy on the application to be protected," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2012, pp. 1054–1059.

[37] G. Owen, *Game Theory*. New York, NY, USA: Academic, 1982.

[38] T. S. Ferguson, *Game Theory*. Los Angeles, CA, USA: UCLA, 2008.

Andrey Garnaev received the M.Sc. degree in mathematics, the Ph.D. degree in applied mathematics, and the D.Sc. degree in computer science and applied mathematics from Saint Petersburg State University, St. Petersburg, Russia, in 1982, 1987, and 1997, respectively. He is currently a Researcher with WINLAB, Rutgers University, North Brunswick, NJ, USA, and a Professor with the Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University. His research interests include applications of game theory and optimization theory in network security, wireless communication, pricing and related fields. He has published in leading journals like IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *Telecommunication Systems Journal*, *Performance Evaluation*, *Naval Research Logistics*, *International Journal of Game Theory*, and *Journal of Optimization Theory and Applications*.

Melike Baykal-Gursoy received the Ph.D. degree in systems engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 1988. She has been on the faculty at Rutgers University, New Brunswick, NJ, USA, since then, where she is an Associate Professor of Industrial and Systems Engineering. Her research interests include stochastic modeling and optimization, Markov decision processes, stochastic games, and queueing, with applications to traffic, security, and supply chains. She has published in leading journals like *Mathematics of Operations Research, Queueing Systems: Theory and Applications*, *Mathematical Methods of Operations research*, *European Journal of Operational Research*, and has a recent book *Introduction to Probability and Statistics* (Kendall/Hunt, 2015).

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, USA, in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana-Champaign, Urbana, IL, USA. Since 1990, he has been on the faculty of Princeton University, where he is the Michael Henry Strater University Professor and the Dean of the School of Engineering and Applied Science. He has also held visiting appointments at several universities, including most recently at Stanford University, Stanford, CA, USA, and Imperial College, London, U.K. His research interests include wireless networks and related fields. Among his publications in these areas is the recent book *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor is a member of the U.S. National Academy of Engineering and the U.S. National Academy of Sciences, and is a foreign member of Academia Europaea and the Royal Society. He is also a fellow of the American Academy of Arts and Sciences, the Royal Academy of Engineering (U.K.), and the Royal Society of Edinburgh. He was the recipient of the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, and honorary doctorates from Aalborg University, Aalborg, Denmark, Aalto University, Espoo, Finland, HKUST, Clear Water Bay, Hong Kong, and the University of Edinburgh, Edinburgh, U.K.