Security Games With Unknown Adversarial Strategies

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

***Abstract*—The security community has witnessed a significant increase in the number of different types of security threats. This situation calls for the design of new techniques that can be incorporated into security protocols to meet these challenges successfully. An important tool for developing new security protocols as well as estimating their effectiveness is game theory. This game theory framework usually involves two players or agents: 1) a protector and 2) an adversary, and two patterns of agent behavior are considered: 1) selfish behavior, where each of the agents wants to maximize his payoff; and 2) leader and follower behavior, where one agent (the leader) expects that the other agent (the follower) will respond to the leader's strategy. Such an approach assumes that the agents agree on which strategy to apply in advance. In this paper, this strong assumption is relaxed. Namely, the following question is considered: what happens if it is unknown *a priori* what pattern of behavior the adversary is going to use, or in other words, it is not known, what game he intends to play? Using a simple game-theoretic model, it is shown that the protector can lose if he does not take into account the possibility that the adversary can play a game other than the one the protector has in mind. Further considered is a repeated game in which the protector can learn about the presence of an adversary, and the behavior of belief probabilities is analyzed in this setting.**

***Index Terms*—Bayesian equilibrium, Bayesian learning, Nash equilibrium, network protection, Stackelberg equilibrium.**

I. Introduction

THE INCREASE in Web services and online operations for various industries and critical businesses has led to an increase in different threats and malicious activities. For example, the financial system might suffer such threats, as was pointed out by Treasury Secretary J. Lew in a speech at the hedge-fund-focused Delivering Alpha Conference [1]. In addition to direct damage such successful cyberattacks against the financial sector can also cause long-term problems by reducing confidence in the market and creating economic instability. Not only the financial system can suffer from cyberattacks. For example, cyberattacks on electric utilities can be devastating, since "taking down an electric grid, especially one that serves a major city, could do real damage to the economy and may indirectly cost lives" [2]. Even the U.S. government can suffer such attacks. "The USIS (U.S. Investigations Services), which provides background checks for the U.S. government was recently hacked. This is the second data breach in a few months that threaten the U.S. government" [3].

These increasing threats call for designing new paradigms that can be incorporated into security protocols. An important tool for designing security protocols as well as estimating their effectiveness is game theory. This is due to the fact that, in general in security problems, there are two groups of agents having opposing goals. Say, in a network, the first groups of agents are the protectors (such as intruder detection systems), who aim to protect the network. The second groups of agents are the adversaries (or adversary) who intend to intrude on or damage the network. Surveys of research contributions that analyze and solve security and privacy problems in computer networks via game-theoretic approaches can be found in [4] and [5]. A survey paper [6] on security games describes the research challenges for applying game theoretic methods in security systems. Among such research, for example, Sagduyu *et al.* [7] suggested a jamming game for power-controlled medium access with dynamic traffic, a game-theoretic approach for eavesdropping and jamming in next-generation wireless networks was suggested in [8], malicious users in collaborative networks are modeled in [9], challenges in applying game theory to the domain of information warfare are discussed in [10], static and dynamic games for infrastructure security are suggested in [11], stochastic games for security in networks with interdependent nodes were investigated in [12], and bandwidth scanning strategies to detect illegal intrusion in a network are described in [13] and [14]. Also, game theory has been applied to fight jamming with jamming [15], for resource allocation in wireless networks between users [16] and channels [17] in the presence of a jammer, to ad hoc networks [18] and for node protection [19].

In such settings usually two patterns of the agents' behavior are considered: 1) selfish, or Nash, behavior, in which each of the agents wants to maximize his payoff and 2) leader and follower, or Stackelberg, behavior, when one agent (the leader)

Manuscript received November 7, 2014; revised April 5, 2015 and June 8, 2015; accepted August 17, 2015. Date of publication September 23, 2015; date of current version September 14, 2016. This work was supported by the National Science Foundation under Grant CMMI-1436288 and Grant CMMI-1435778. This paper was recommended by Associate Editor J. Shamma.

A. Garnaev is with the Center for Advanced Infrastructure and Transportation, Rutgers University, Piscataway, NJ 08854-8018 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, Rutgers Center for Operations Research, Rutgers University, Piscataway, NJ 08854-8018 USA, and also with the Center for Advanced Infrastructure and Transportation, 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/TCYB.2015.2475243

expects that the other agent (the follower) will apply his best response to maximize his payoff for each fixed leader's strategy. Then, in turn, the leader maximizes his payoff after incorporating the follower's best response strategy. This approach assumes that the agents agree on the mode of decision-making in advance.

The main contribution of this paper is to analyze scenarios that relax the assumption that the players always have to follow the same pattern of behavior. Taking into account the possibility of diversionary tactics by the adversary from his expected pattern of behavior can be considered as taking into account the human factor. For example, as it is now realized, the economic turmoil of the previous decade [20] may have been due in part to reliance on economic models that did not take into account that the participants of the market might not behave as predicted by standard game models. In a Stackelberg duopoly model, it is assumed that the first player is the leader, while the second player is the follower. This model works nicely while both players assume such a relationship. If one day the second player changes his mind in committing to the best response policy, and instead plays selfishly, the first player's payoff might be effected negatively by such an unexpected behavior.

Using a simple game-theoretic model, we first show that the protector can lose if he does not take into account the possibility that the adversary can play a game other than the one the protector has in mind. We further show that incorporating into the protector's strategy, the possibility that the adversary might play another game allows the protector to increase his payoff. We note that such an approach can be useful in a wide spectrum of problems, even, for example, analyzing such problems as the starting point of the Ukrainian crisis of 2014. Namely, Cohen in *The Nation* [21] wrote that since the 1990s Russia was treated as a follower in decision-making. So, it was not taken into account that in some situations it might prefer not to play as a follower, but rather would prefer to play its own Nash equilibrium strategy. If the possibility of such a situation had been taken into consideration from the beginning, as we suggest, it could be possible to gain in payoff compared to considering only the Stackelberg scenario, or the Nash scenario.

Since our model involves incomplete information about what kind of game the adversary means to play, we will apply a Bayesian approach, which has been widely used for modeling network security problems, such as intrusion detection in wireless ad hoc networks [22]–[24], attack-type uncertainty on a network [25], the effects on an unknown eavesdropper on a wireless transmitter [26], or allocation of limited resources for critical infrastructure protection [27], [28].

A Bayesian approach is characterized by asymmetric information the agent may have. Comprehensive analyses of various asymmetric-information zero-sum repeated games are given in [29]. A game theoretic model of an attacker against an intelligent network, where the attacker seeks to degrade network operations while the network adapts its operations to counteract the effects of the attacker is investigated in [30]. A general approach to solve two-player zero-sum stochastic games where only one of the players is informed of the state at each stage is discussed in [31].

The organization of this paper is as follows. In Section II, we first formulate the considered problem in selfish and leader–follower scenarios. In Section III, we formulate and solve a Bayesian game, in which the game the adversary will play is random. In Section IV, we solve the repeated version of the considered game in which the belief about the opponent's game is adapted. In Section V, the conclusions are presented. Proofs of the obtained results are contained in an appendix.

II. Basic Security Model

In this section, we formulate a basic security model. A network may be under attack by an adversary attempting to intrude on it in order to perform a damaging action, say, to steal data. We consider the network as an abstract one, not specifying its topology. There is a protector (owner, or manager of the network), who wants to protect the network. Also, an adversary may be present, and if so, wants to intrude on the network. We assume that the protector cannot observe the intrusion, but can suffer from the effects of a successful intrusion. The *a priori* probability that the adversary is present is given by q^1, and with probability $q^0 = 1-q^1$ he is not present. To increase the protection level of the network, the protector has some resources. To intrude into the network, the adversary also has some resources. We consider these protection and intrusion resources to be abstract ones, not specifying how they can be allocated within the network. Let x be the resource effort the protector applies to protect the network, and y be the resource effort applied by the adversary to intrude into the network. Let $P(x, y)$ be the probability of successful intrusion into the network, when protection effort x and intrusion effort y are employed. In this paper, we assume that this probability is proportional to the fraction of effort put forth into the attack, that is

$$P(x, y) = \frac{y}{d + x + y} \tag{1}$$

where d is an initial level of network security. This is the ratio-form contest success function commonly used in the attack-defense literature [32], [33], corresponding to the scenario for $d > 0$, where inherent protection is allowed [34]. If $d = 0$, there is no inherent (or free) protection [35]. It is clear that $P(x, y)$ is monotonically increasing in y from 0 at $y = 0$ to 1 as y tends to infinity, and it is decreasing in x from $y/(d + y)$ at $x = 0$ to zero as x tends to infinity.

Furthermore, let R_P be the value of protected assets in the network and C_P be the protection cost per unit protection effort. Similarly, let R_A be the adversary's reward for a successful intrusion and C_A be the intrusion cost per unit of applied intrusion effort. The expected payoff to the protector is the difference between the value of the protected assets and protection cost, that is

$$v_P^S(x, y) = q^1 v_P(x, y) + q^0 v_P(x, 0) \tag{2}$$

with

$$v_P(x, y) = R_P(1 - P(x, y)) - C_P x.$$

The payoff to the adversary is the difference between the value of a successful intrusion and the intrusion cost, that is

$$v_A(x, y) = R_A P(x, y) - C_A y. \tag{3}$$

A. Selfish Pattern of Behavior

In this section, we deal with a selfish pattern of behavior, in which each player designs his optimal behavior as the best response to his rival's strategy. Namely, x_* and y_* form a (Nash) equilibrium if and only if

$$x_* = \mathrm{BR}_P^S(y_*) = \arg_x \max v_P^S(x, y_*)$$
$$y_* = \mathrm{BR}_A(x_*) = \arg_y \max v_A(x_*, y)$$

or, equivalently, the following inequalities hold for any pair of strategies (x, y):

$$v_P^S(x, y_*) \le v_P^S(x_*, y_*)$$
$$v_A(x_*, y) \le v_A(x_*, y_*). \tag{4}$$

Since the payoff v_P^S is concave in x and v_A is concave in y, the game has an equilibrium [36]. The following theorem gives the equilibrium explicitly.

Theorem 1: The considered (Nash) game has a unique equilibrium (x^S, y^S) given as follows:

$$x^S = \begin{cases} 0, & \frac{d}{\overline{R}_A} \ge 1 \\ 0, & \frac{d}{\overline{R}_A} < 1, \frac{\overline{R}_P}{\overline{R}_A}\frac{\sqrt{d}}{\sqrt{\overline{R}_A} - \sqrt{d}} \ge q^1 \\ \overline{R}_A\left(\frac{q^1\overline{R}_P}{\overline{R}_A + q^1\overline{R}_P}\right)^2 - d, & \frac{d}{\overline{R}_A} < 1, \frac{\overline{R}_P}{\overline{R}_A}\frac{\sqrt{d}}{\sqrt{\overline{R}_A} - \sqrt{d}} < q^1 \end{cases} \tag{5}$$

$$y^S = \begin{cases} 0, & 1 \le \frac{d}{\overline{R}_A} \\ \sqrt{\overline{R}_A d} - d, & \frac{d}{\overline{R}_A} < 1, \frac{\overline{R}_P}{\overline{R}_A}\frac{\sqrt{d}}{\sqrt{\overline{R}_A} - \sqrt{d}} \ge q^1 \\ q^1\overline{R}_P\left(\frac{\overline{R}_A}{\overline{R}_A + q^1\overline{R}_P}\right)^2, & \frac{d}{\overline{R}_A} < 1, \frac{\overline{R}_P}{\overline{R}_A}\frac{\sqrt{d}}{\sqrt{\overline{R}_A} - \sqrt{d}} < q^1 \end{cases} \tag{6}$$

where $\overline{R}_P = R_P/C_P$ is the asset value to protection cost ratio, and $\overline{R}_A = R_A/C_A$ is the adversary's benefit to intrusion cost ratio.

Thus, if the adversary's benefit to cost ratio is smaller than the initial level of security d, there is no reason for the adversary to intrude and for the protector to increase the level of security. Otherwise, if the probability that the intruder is present in the network is small, that is, $q^1 \le (\overline{R}_P/\overline{R}_A)(\sqrt{d}/(\sqrt{\overline{R}_A} - \sqrt{d}))$, then the protector does not consider such a threat as essential, and keeps on maintaining the initial level of security. As q^1 increases further, the protector begins increasing its level of security.

B. Leader–Follower Pattern of Behavior

In the leader–follower pattern of behavior, one of the rivals is a leader, and the other is a follower. In our case, the protector is a leader, and the adversary is a follower. We assume that with probability q^2 such an adversary is present in the network and with probability $q^0 = 1 - q^2$ he is not present. For a fixed x, the adversary designs his strategy as the best response to x, i.e., $y = \mathrm{BR}_A(x)$. The protector, taking into account such adversarial behavior, assigns his strategy to maximize his expected payoff, that is

$$x = \arg_x \max v_P^L(x, \mathrm{BR}_A(x))$$

where

$$v_P^L(x, y) = q^2 v_P(x, y) + q^0 v_P(x, 0).$$

Note that, we use the term "pattern of behavior" on purpose, as we do not split the game into two steps. We assume that all actions are taken simultaneously based on *a priori* knowledge (say, from previous experience) that this adversary always acts as a follower. This assumption is natural for problems such as network security, in which the protector cannot observe the intrusion itself, but can suffer its consequences (say, as in the theft of credit card numbers [37]).

For the considered model, the best response strategy $\mathrm{BR}_A(x)$ is given as follows:

$$y = \mathrm{BR}_A(x) = \begin{cases} \sqrt{\overline{R}_A(d + x)} - d - x, & x < \overline{R}_A - d \\ 0, & x \ge \overline{R}_A - d. \end{cases} \tag{7}$$

Thus

$$v_P^L(x, \mathrm{BR}_A(x)) = R_P - C_P x + \begin{cases} q^2 R_P\left(\frac{\sqrt{d + x}}{\sqrt{\overline{R}_A}} - 1\right), & x < \overline{R}_A - d \\ 0, & x \ge \overline{R}_A - d. \end{cases} \tag{8}$$

Note that $v_P^L(x, \mathrm{BR}_A(x))$ is continuous in x, concave for $x \le \overline{R}_A - d$, and linearly decreasing for $x \ge \overline{R}_A - d$. Also, $v_P^L/(dx)|_{x \uparrow \overline{R}_A - d} > -C_p = v_P^L/(dx)|_{x \downarrow \overline{R}_A - d}$. Thus, $v_P^L(x, \mathrm{BR}_A(x))$ is concave in x, the game has a unique (Stackelberg) equilibrium, and the following theorem gives it explicitly.

Theorem 2: The considered leader–follower game has a unique equilibrium (x^L, y^L), where

$$x^L = \begin{cases} 0, & \frac{d}{\overline{R}_A} \ge 1 \\ 0, & \frac{d}{\overline{R}_A} < 1, q^2 \le \frac{2\sqrt{\overline{R}_A d}}{\overline{R}_P} \\ \frac{\left(q^2\overline{R}_P\right)^2}{4\overline{R}_A} - d, & \frac{d}{\overline{R}_A} < 1, \frac{2\sqrt{\overline{R}_A d}}{\overline{R}_P} < q^2 < \frac{2\overline{R}_A}{\overline{R}_P} \\ \overline{R}_A - d, & \frac{d}{\overline{R}_A} < 1, \frac{2\overline{R}_A}{\overline{R}_P} \le q^2 \end{cases} \tag{9}$$

$$y^L = \mathrm{BR}_A\left(x^L\right) = \begin{cases} 0, & \frac{d}{\overline{R}_A} \ge 1 \\ \sqrt{\overline{R}_A d} - d, & \frac{d}{\overline{R}_A} < 1, q^2 \le \frac{2\sqrt{\overline{R}_A d}}{\overline{R}_P} \\ \frac{q^2\overline{R}_P}{2}\left(1 - \frac{q^2\overline{R}_P}{2\overline{R}_A}\right), & \frac{d}{\overline{R}_A} < 1, \frac{2\sqrt{\overline{R}_A d}}{\overline{R}_P} < q^2 < \frac{2\overline{R}_A}{\overline{R}_P} \\ 0, & \frac{d}{\overline{R}_A} < 1, \frac{2\overline{R}_A}{\overline{R}_P} \le q^2. \end{cases} \tag{10}$$

Similar to the selfish pattern of behavior, if the adversary's benefit to cost ratio is smaller than the initial level of security d, then there is no reason for the adversary to intrude and

for the protector to increase the level of security. Otherwise, there is a threshold value of the probability for the adversary to be in the network, $q^2 = (2\sqrt{\overline{R}_A d})/\overline{R}_P$ such that for smaller probabilities the protector does not consider such a threat as critical and keeps on maintaining the initial level of security. Meanwhile for higher probabilities, the protector applies extra security effort. There is also a difference with the selfish pattern of behavior. Namely, if the benefit to cost ratio of the protected assets is larger than twice the adversary's benefit to cost ratio, i.e., $\overline{R}_P > 2\overline{R}_A$, and if the probability that the adversary is present is large enough, then the protector increases the protection effort, thereby scaring the adversary away.

III. Unknown Adversarial Intensions

In this section, we assume that it is unknown to the protector what game the adversary intends to play. It is only known that with probability q^1, he can act as a selfish player, and with probability q^2, he can act as a follower, with $q^1 + q^2 \leq 1$. So, $q^0 = 1 - q^1 - q^2$ gives the probability that the adversary is not present. To deal with this situation, we have to apply a Bayesian approach, introducing two types of adversaries according to the game the adversary plays. Denote by y^1 and y^2, the strategies employed by the adversary according to his type. Then, if the protector employs strategy x, we have that $y^2 = \mathrm{BR}_A(x)$. Thus, the expected payoff to the protector is

$$Ev_P\Big(x, y^1\Big) = q^1 v_P\Big(x, y^1\Big) + q^2 v_P(x, \mathrm{BR}_A(x)) + q^0 v_P(x, 0) \tag{11}$$

where $q^0 = 1 - q^1 - q^2$.

The payoff to the adversary of type 1 is $v_A(x, y^1)$.

We look for equilibrium strategies. Note that, in general, the payoff (11) can be nonconcave in x, and so the game may not have an equilibrium [36]. In the considered model, however, using (1), (2), and (8), this payoff becomes

$$\begin{aligned} Ev_P\Big(x, y^1\Big) = {} & q^1\left(R_P\frac{d+x}{d+x+y^1} - C_P x\right) \\ & + q^2\begin{cases}\left(\dfrac{R_P\sqrt{d+x}}{\sqrt{\overline{R}_A}} - C_P x\right), & x < \overline{R}_A - d \\ (R_P - C_P x), & x \geq \overline{R}_A - d\end{cases} \\ & + q^0(R_P - C_P x). \end{aligned} \tag{12}$$

It is clear that the payoff Ev_P is now concave in x as the sum of two concave functions. Since $v_A(x, y^1)$ is concave in y^1, the game has an equilibrium [36]. The following theorem gives this equilibrium explicitly.

Theorem 3: The considered game has a unique equilibrium (x, y^1, y^2).

1) If

$$1 \leq \frac{d}{\overline{R}_A} \tag{13}$$

then $(x, y^1, y^2) = (0, 0, 0)$.

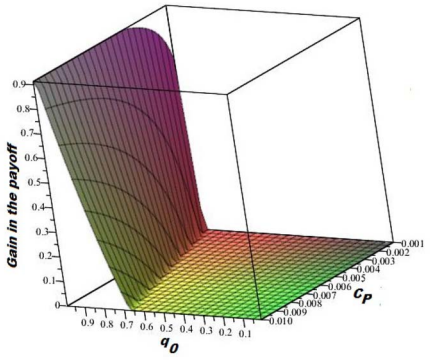

Fig. 1. Possible gain in the protector's payoff as the function $\max\{E_P((1-q_0)/2,\ (1-q_0)/2, q_0) - R_P(1 - P(x^L, y^L)) - C_P x^L, 0\}$.

2) If

$$\frac{d}{\overline{R}_A} < 1 < \frac{\big(q^1 + q^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1} \tag{14}$$

then $(x, y^1, y^2) = (\overline{R}_A - d, 0, 0)$.

3) If

$$\frac{\big(q^1 + q^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1} < \sqrt{\frac{d}{\overline{R}_A}} < 1 \tag{15}$$

then $(x, y^1, y^2) = (0, \sqrt{\overline{R}_A d} - d, \sqrt{\overline{R}_A d} - d)$.

4) If

$$\sqrt{\frac{d}{\overline{R}_A}} < \frac{\big(q^1 + q^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1} < 1 \tag{16}$$

then

$$\begin{aligned} x &= \overline{R}_A\left(\frac{\big(q^1 + q^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1}\right)^2 - d \\ y^1 = y^2 &= \frac{\big(q^1 + q^2/2\big)\overline{R}_A\overline{R}_P\big(\overline{R}_A - q^2\overline{R}_P/2\big)}{\big(\overline{R}_A + \overline{R}_P q^1\big)^2}. \end{aligned} \tag{17}$$

Note that the equilibrium strategies of both adversary types, y^1 and y^2, coincide. This can be explained by the fact that both of them are the best response strategies to the protector's strategy x. However, the intuitions behind these strategies are different. For the second adversary type, due to its follower nature, y^2 is just the best response strategy to x. Meanwhile for the first adversary type, due to its selfish nature, it is a solution to the best response equations.

Note that such strategies equalize the probability of protection against each type of adversary. This phenomena is typical for search games where an equalizing protection level strategy quite often turns out to be an equilibrium strategy [38]–[40]. Also, as is shown in the next section, in spite of this similarity, in the repeated version of the game, the protector can improve his belief about the adversary's presence of the corresponding type in an attempt to understand the exact type of the adversary.

Denote by $E_P(q_1, q_2, q_0)$, the optimal payoff to the protector. As a numerical illustration to compare these payoffs for this equilibrium, we consider $R_A = 1$, $R_P = 1$, $C_P = 0.01$, $C_A = 0.05$, and $d = 0.1$. Fig. 1 illustrates the gain in the

protector's payoffs $\max\{E_P((1-q_0)/2, (1-q_0)/2, q_0) - R_P(1-P(x^L, y^L)) - C_P x^L, 0\}$, if the protector takes into account that the adversary sometimes might prefer to divert from a role as a follower in a Stackelberg pattern of behavior.

IV. Adapting Belief on Malicious Threat

In this section, we consider the protection problem as a game that is played repeatedly at time slots $t = 1, 2, \ldots$. Thus, it is not a sequential game, but rather it is the same game played repeatedly. We examine two scenarios to build protection.

1) Inherent protection is constant, i.e., the initial level d_i of security for each time slot i is the same, i.e., $d_i = d$ for each i. Thus, the current level of protection is the sum of the initial level d and current protection effort x_i.
2) Inherent protection is cumulative, i.e., the initial level d_i of security for each time slot i is the initial level of security at the beginning plus the accumulated protection efforts for all the previous time slots, $d_i = d + \sum_{j=1}^{i-1} x_j$, where x_j is the protection effort at time t.

At the beginning of each time slot, the protector adapts his belief regarding the adversary's presence in the network. Namely, the protector adjusts his protection strategy to an adapted belief on the existence of the threat. The adversary, if he is present in the network, can adjust also his intrusion efforts at the beginning of the next time slot after taking into account any perception he might have regarding the adjusted protector's belief. If the adversary performs a successful attack, the game is over. To gain insight into the problem here, we consider the rule in which the adaptation takes into account the result of the protection only in the previous time slot (i.e., not upon any other previous time slot). Since q^m is the probability that the adversary of the corresponding type (m) is present in the network, then at the beginning of the first time slot the protector's belief about the adversary's presence of the corresponding type will be denoted as $q_1^m = q^m$ for $m = 1, 2$, and the belief that the adversary is not in the network will be denoted as $q_1^0 = 1 - q_1^1 - q_1^2 = q^0$. In the first time slot, the rivals apply the equilibrium strategies x_1 and (y_1^1, y_1^2) given by Theorems 1–3 according to the original belief. The probability that the adversary type m fails to intrude is $1 - P_1(x_1, y_1^m)$ with $P_1(x_1, y_1^m) = P(x_1, y_1^m)$ and $m = 1, 2$. In deriving the revised probabilities that the adversary is in the network if the attack was unsuccessful, we use the same approach as in obtaining the posterior probability after an unsuccessful search of an object in a box that might be hidden [11], [41]. Then, by Bayes' formula, the revised probability that the adversary is in the network is given as follows:

$$q_2^m = \frac{q_1^m\big(1 - P_1\big(x_1, y_1^m\big)\big)}{q_1^0 + q_1^1\big(1 - P_1\big(x_1, y_1^1\big)\big) + q_1^2\big(1 - P_1\big(x_1, y_1^2\big)\big)}.$$

Thus, here we deal with the simplest learning mechanism. For examples of more advanced learning mechanisms, say, multiple-instance learning and reinforcement learning see [42] and [43].

It is clear that $q_2^m < q_1^m$. Taking into account this adapted belief, the rivals repeat the game in the second time slot, if the attack on the first time slot was not successful, and the game is repeated until the attack is successful.

Let x_k, (y_k^1, y_k^2) and q_k^m be the equilibrium strategies and the adapted belief for time slot k. Then

$$q_{k+1}^m = \frac{q_k^m\big(1 - P_k\big(x_k, y_k^m\big)\big)}{q_k^0 + q_k^1\big(1 - P_k\big(x_k, y_k^1\big)\big) + q_k^2\big(1 - P_k\big(x_k, y_k^2\big)\big)} \tag{18}$$

with

$$P_k\big(x_k, y_k^m\big) = \begin{cases} \dfrac{y_k^m}{d + x_k + y_k^m}, & \text{for scenario 1)} \\ \dfrac{y_k^m}{d + \sum_{i=1}^{k} x_i + y_k^m}, & \text{for scenario 2).} \end{cases}$$

Since $q_1^m > q_2^m > q_3^m > , \ldots,$ while either $P_k < 1$ or $q_k^1 > 0$ and $q_k^2 > 0$, this belief learning process continues until the first successful attack or creating the ideal protection when the adversary stops his attempt to break through the established protection.

Since $y_k^1 = y_k^2$, it follows that $P(x_k, y_k^1) = P(x_k, y_k^2)$. Hence the posterior probabilities do not allow us to identify the adversary's type. However, we can still obtain the posterior probabilities of the presence of each adversary type, and, by (18), their convergence rates remain the same

$$\frac{q_{k+1}^2}{q_k^2} = \frac{q_{k+1}^1}{q_k^1}. \tag{19}$$

Then, based on Theorem 3, the following results are obtained.

1) If the initial condition is

$$1 \le \frac{d_1}{\overline{R}_A} \tag{20}$$

then $y_1^1 = y_1^2 = x_1 = 0$. So, $d_2 = d$, and (20) also holds with d_2 instead of d_1. Thus, $y_i^1 = y_i^2 = x_i = 0$ and the initial protection is perfect in that there is no reason to improve it or to attempt to break through it.

2) If the initial condition is

$$\frac{d_1}{\overline{R}_A} < 1 < \frac{\big(q_1^1 + q_1^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1} \tag{21}$$

then

$$\Big(x_1, y_1^1, y_1^2\Big) = \big(\overline{R}_A - d, 0, 0\big). \tag{22}$$

Thus, $q_2^m = q_1^m$ for $m \in [0, 2]$. Then:

   a) for scenario 1), the condition (15) holds with q_2^m instead of q_1^m. So, the protector applies a constant protection effort, and it keeps the adversary away from intrusion;
   b) for scenario 2), by (22), $d_2 = \overline{R}_A$. Thus, the condition (20) holds with d_2 instead of d_1. Thus, $y_i^1 = y_i^2 = x_i = 0$ for $i \ge 2$ and the perfect protection is achieved in that there is no reason to improve it or to attempt to break through it.

3) If the initial condition is

$$\frac{\big(q_1^1 + q_1^2/2\big)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1} < \sqrt{\frac{d_1}{\overline{R}_A}} < 1 \tag{23}$$

then

$$\left(x_1, y_1^1, y_1^2\right) = \left(0, \sqrt{\overline{R}_A d_1} - d_1, \sqrt{\overline{R}_A d_1} - d_1\right). \quad (24)$$

Thus, $d_2 = d_1 = d$ for both scenarios. Then, due to the monotonically decreasing nature of q_i^m for $m = 1, 2$, (23) also holds with q_2^m and d_2 instead of q_1^m and d_1. This makes this case different from (b_i). The protector believes that the adversary might be present in the network, and still it might be expensive for him to increase the protection. Meanwhile the adversary, if he is present, applies a constant intrusion effort, until he succeeds.

4) If the initial condition is

$$\sqrt{\frac{d_1}{\overline{R}_A}} < \frac{\left(q_1^1 + q_1^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1} < 1 \quad (25)$$

then

$$x_1 = \overline{R}_A\left(\frac{\left(q_1^1 + q_1^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1}\right)^2 - d_1$$
$$y_1^1 = y_1^2 = \frac{\left(q_1^1 + q_1^2/2\right)\overline{R}_A\overline{R}_P\left(\overline{R}_A - q_1^2\overline{R}_P/2\right)}{\left(\overline{R}_A + \overline{R}_P q_1^1\right)^2}. \quad (26)$$

a) for scenario 1), i.e., $d_i = d$, the right inequality of (25) is equivalent to

$$q_1^2 < 2\overline{R}_A/\overline{R}_P$$

and the left inequality of (25) is equivalent to

$$\sqrt{\overline{R}_A d} < q_1^1\overline{R}_P\left(1 - \sqrt{d/\overline{R}_A}\right) + q_1^2\overline{R}_P/2.$$

Thus, due to the monotonically decreasing nature of q_i^1 and q_i^2 and the fact that $d/\overline{R}_A < 1$, the equilibrium strategies are given as follows:

$$x_i = \overline{R}_A\left(\frac{\left(q_i^1 + q_i^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_i^1}\right)^2 - d_i$$
$$y_i^1 = y_i^2 = \frac{\left(q_i^1 + q_i^2/2\right)\overline{R}_A\overline{R}_P\left(\overline{R}_A - q_i^2\overline{R}_P/2\right)}{\left(\overline{R}_A + \overline{R}_P q_i^1\right)^2} \quad (27)$$

for $i \le k-1$, where k is an integer such that

$$q_k^1\overline{R}_P\left(1 - \sqrt{d/\overline{R}_A}\right) + q_k^2\overline{R}_P/2 \le \sqrt{\overline{R}_A d}$$
$$< q_{k-1}^1\overline{R}_P\left(1 - \sqrt{d/\overline{R}_A}\right) + q_{k-1}^2\overline{R}_P/2 \quad (28)$$

and

$$\left(x_i, y_i^1, y_i^2\right) = \left(0, \sqrt{\overline{R}_A d} - d, \sqrt{\overline{R}_A d} - d\right) \text{ for } i \ge k$$

until the first successful attack;

b) for scenario 2)

$$d_2 = d_1 + x_1 = \overline{R}_A\left(\frac{\left(q_1^1 + q_1^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1}\right)^2.$$

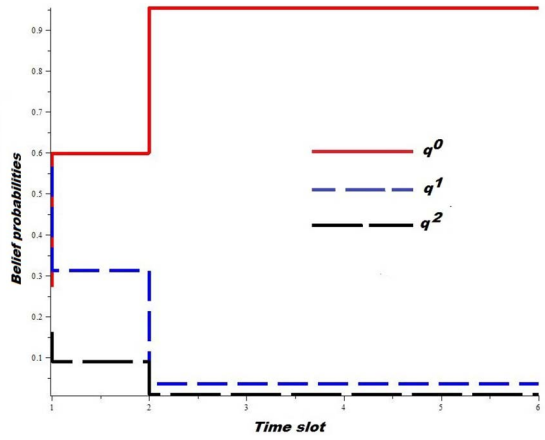

Fig. 2. Illustration of the monotone convergence of the belief probabilities over time slots in scenario 1).

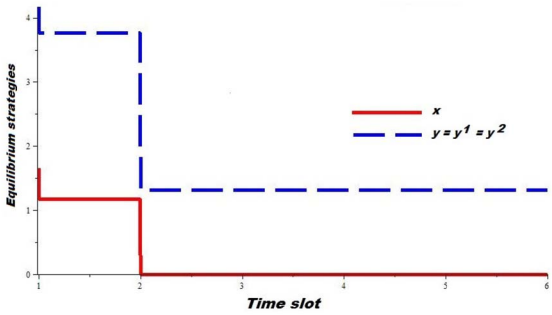

Fig. 3. Convergence of equilibrium strategies x_i and $y_i^1 = y_i^2 = y_i$ over time slots in scenario 1).

Thus, the inequality

$$\sqrt{\frac{d_2}{\overline{R}_A}} < \frac{\left(q_2^1 + q_2^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_2^1}$$

is equivalent to

$$\frac{\left(q_1^1 + q_1^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_1^1} < \frac{\left(q_2^1 + q_2^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q_2^1}.$$

This implies that the following inequality has to hold:

$$\frac{1 + q_1^2/\left(2q_1^1\right)}{\overline{R}_A/q_1^1 + \overline{R}_P} < \frac{1 + q_2^2/\left(2q_2^1\right)}{\overline{R}_A/q_2^1 + \overline{R}_P}.$$

The last inequality cannot hold due to the monotonically decreasing nature of q_i^1 and (19).

Thus, the equilibrium strategies are $(x_i, y_i^1, y_i^2) = (0, \sqrt{\overline{R}_A d_2} - d_2, \sqrt{\overline{R}_A d_2} - d_2)$ for any $i \ge 2$ until the first successful attack.

Fig. 2 illustrates the monotone convergence of the belief probabilities and Fig. 3 illustrates the equilibrium strategies x_i and $y_i^1 = y_i^2 = y_i$ for $R_A = 2$, $R_P = 1$, $C_P = 0.1$, $C_A = 0.1$, $d = 0.1$, $q_1^0 = 0.1$, $q_1^1 = 0.7$, and $q_2^1 = 0.2$ for scenario 1).

V. Conclusion

In this paper, we have considered the following question: what happens if it is unknown *a priori* what pattern of behavior

an adversary is going to use, or in other words, what game he intends to play (Nash or Stackelberg)? Using a simple game-theoretic model, we have shown that the protector can lose if he does not take into account that the adversary can play a game other than the one the protector has in mind. We have further shown that incorporating into the protector's strategy the possibility that the adversary might play another game allows the protector to increase his payoff. One of our goals for the future is to develop a dynamic version of the current analysis, based on the stochastic game approach, with a more sophisticated adversary, who can combine an attacking mode with silent modes.

APPENDIX

Proof of Theorem 1: Note that

$$\frac{d\,v_P^S}{d\,x} = \frac{q^1 R_P y}{(d+x+y)^2} - C_P \tag{29}$$

$$\frac{d\,v_A}{d\,y} = \frac{R_A(d+x)}{(d+x+y)^2} - C_A. \tag{30}$$

To find an equilibrium, by (4), (29), and (30), we have to solve the equations

$$\frac{q^1 R_P y}{(d+x+y)^2} = C_P \tag{31}$$

$$\frac{R_A(d+x)}{(d+x+y)^2} = C_A. \tag{32}$$

Dividing (31) by (32), and solving the obtained equation for y implies

$$y = \frac{\overline{R}_A}{q^1 \overline{R}_P}(d+x). \tag{33}$$

Substituting this y into (32) yields

$$d+x = \overline{R}_A\left(\frac{q^1\overline{R}_P}{\overline{R}_A + q^1\overline{R}_P}\right)^2.$$

This, jointly with (33), implies (5) and (6), and the result follows. ∎

Proof of Theorem 2: By (8), $v_P(x, \mathrm{BR}_A(x))$ is decreasing for $x \geq \overline{R}_A - d$.

For $x < \overline{R}_A - d$ we have that

$$\frac{d\,v_P^L}{d\,x} = \frac{q^2 R_P}{2\sqrt{\overline{R}_A(d+x)}} - C_P.$$

Thus, if

$$\frac{d\,v_P^L}{d\,x}(0) = \frac{q^2 R_P}{2\sqrt{\overline{R}_A d}} - C_P \leq 0 \tag{34}$$

then v_P^L is also decreasing for $x < \overline{R}_A - d$, and the optimal x equals to zero.

If (34) does not hold and

$$\frac{d\,v_P^L}{d\,x}\Big|_{x=\overline{R}_A-d} = \frac{q^2 R_P}{2\overline{R}_A} - C_P \geq 0 \tag{35}$$

then v_P^L is increasing for $x > \overline{R}_A - d$, and the optimal $x = \overline{R}_A - d$.

If (34) and (35) do not hold, then $\arg_x \max v_P$ is the unique root of the equation $(d\,v_P)/(d\,x)(x) = 0$, and the result follows. ∎

Proof of Theorem 3: Note that

$$\frac{d\,v_A}{d\,y^1} = \frac{R_A(d+x)}{\left(d+x+y^1\right)^2} - C_A \tag{36}$$

and

$$\frac{d\,Ev_P}{d\,x} = \frac{q^1 R_P y^1}{\left(d+x+y^1\right)^2} - C_P + \begin{cases} \dfrac{q^2 R_P}{2\sqrt{\overline{R}_A(d+x)}}, & x < \overline{R}_A - d \\ 0, & x \geq \overline{R}_A - d. \end{cases} \tag{37}$$

Thus, by (36) and (37), 1) follows.

It is clear that for a fixed y^1, $(d\,Ev_P/d\,x)(x, y^1)$ is strictly decreasing in x, continuous on $[0,\infty)\backslash\{\overline{R}_A - d\}$, and discontinuous at the unique point $x = \overline{R}_A - d$. Thus:

1) if

$$\frac{q^1 R_P y^1}{\left(d+y^1\right)^2} \leq C_P - \frac{q^2 R_P}{2\sqrt{\overline{R}_A d}} \tag{38}$$

then

$$\mathrm{BR}_P\left(y^1\right) = 0 \tag{39}$$

2) if

$$C_P - \frac{q^2 R_P}{2\sqrt{\overline{R}_A d}} < \frac{q^1 R_P y^1}{\left(d+y^1\right)^2} \tag{40}$$

and

$$\frac{q^1 R_P y^1}{\left(\overline{R}_A+y^1\right)^2} \leq C_P - \frac{q^2 R_P}{2\overline{R}_A} \tag{41}$$

then $\mathrm{BR}_P(y^1) = x$, where x is the unique root of the equation

$$\frac{q^1 R_P y^1}{\left(d+x+y^1\right)^2} = C_P - \frac{q^2 R_P}{2\sqrt{\overline{R}_A(d+x)}} \tag{42}$$

3) if (40) holds and

$$\frac{q^1 R_P y^1}{\left(\overline{R}_A+y^1\right)^2} > C_P - \frac{q^2 R_P}{2\overline{R}_A} \tag{43}$$

and

$$\frac{q^1 R_P y^1}{\left(\overline{R}_A+y^1\right)^2} < C_P \tag{44}$$

then

$$\mathrm{BR}_P\left(y^1\right) = \overline{R}_A - d \tag{45}$$

4) if (40) and (43) hold and

$$\frac{q^1 R_P y^1}{\left(\overline{R}_A + y^1\right)^2} \geq C_P \tag{46}$$

then $\mathrm{BR}_P(y^1) = x$ is the unique root of the equation

$$\frac{q^1 \overline{R}_P y^1}{\left(d + x + y^1\right)^2} = C_P. \tag{47}$$

Since at least one equilibrium (x, y) exists, to find an equilibrium explicitly by 1)–4) we have to consider separately four cases: 1) $x > \overline{R}_A - d$; 2) $0 < x < \overline{R}_A - d$; 3) $x = \overline{R}_A - d$; and 4) $x = 0$.

1) By (36) and (37), the inequality

$$x > \overline{R}_A - d \tag{48}$$

holds for an (interior) equilibrium (x, y^1) if and only if (x, y^1) is a solution of (47) and

$$\frac{\overline{R}_A(d + x)}{\left(d + x + y^1\right)^2} = 1. \tag{49}$$

Following the proof of Theorem 1 implies that the equilibrium x has to be given by

$$x = \overline{R}_A \left(\frac{q^1 \overline{R}_P}{\overline{R}_A + q^1 \overline{R}_P} \right)^2 - d.$$

Thus, $x < \overline{R}_A - d$. This contradiction to (48) proves that there is no equilibrium such that (48) holds.

2) By (36) and (37), the inequalities $0 < x < \overline{R}_A - d$ hold for an (interior) equilibrium (x, y^1) if and only if (x, y^1) is a solution of (42) and (49). Solving (49) by y^1 implies

$$y^1 = \sqrt{\overline{R}_A(d + x)} - d - x. \tag{50}$$

Substituting this y^1 into (42) yields

$$\frac{q^1 \overline{R}_P \left(\sqrt{\overline{R}_A(d + x)} - d - x \right)}{\overline{R}_A(d + x)} = 1 - \frac{q^2 \overline{R}_P}{2\sqrt{\overline{R}_A(d + x)}}. \tag{51}$$

Solving this equation for $d + x$ yields

$$d + x = \overline{R}_A \left(\frac{\left(q^1 + q^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1} \right)^2. \tag{52}$$

Substituting $d + x$ into (50) implies

$$y^1 = \frac{\left(q^1 + q^2/2\right)\overline{R}_A \overline{R}_P \left(\overline{R}_A - q^2 \overline{R}_P/2\right)}{\left(\overline{R}_A + \overline{R}_P q^1\right)^2}. \tag{53}$$

Thus, there is an interior equilibrium if and only if $0 < x < \overline{R}_A$ and $y^1 > 0$. These conditions, by (52) and (53), are equivalent to

$$\frac{d}{\overline{R}_A} < \left(\frac{\left(q^1 + q^2/2\right)\overline{R}_P}{\overline{R}_A + \overline{R}_P q^1} \right)^2 < 1 \tag{54}$$

and

$$q^2 \overline{R}_P / 2 < \overline{R}_A. \tag{55}$$

Since the right-hand inequality of (54) is equivalent to (55), 2) follows. Cases 3) and 4) are obvious, and the result follows. ■

REFERENCES

[1] Media Center. (Jul. 18, 2014). *Treasury Secretary Calls for Greater Financial Sector Cyber Security, Merlin Secure Peformance*. [Online]. Available: http://www.merlin-intl.com/treasury-secretary-calls-for-greater-financial-sector-cyber-security/

[2] S. Magnuson. (Mar. 2014). *Power Companies Struggle to Maintain Defenses Against Cyber-Attacks, National Defense NDIA's Business and Technology Magazine*. [Online]. Available: http://www.nationaldefensemagazine.org/archive/2014/March/Pages/PowerCompaniesStruggletoMaintainDefensesAgainstCyber-Attacks.aspx

[3] P. Paganini. (Aug. 12, 2014). *The Network of USIS Compromised by a Cyber Attack, Security Affairs*. [Online]. Available: http://securityaffairs.co/wordpress/27499/cyber-crime/network-usis-compromised-cyber-attack.html

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacsar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, pp. 1–39, Jun. 2013.

[5] S. Roy *et al.*, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci. (HICSS)*, Honolulu, HI, USA, 2010, pp. 1–10.

[6] M. Tambe, A. X. Jiang, B. An, and M. Jain, "Computational game theory for security: Progress and challenges," in *Proc. AAAI Spring Symp. Appl. Comput. Game Theory*, Stanford, CA, USA, Mar. 2012, pp. 1–6. [Online]. Available: http://teamcore.usc.edu/papers/2014/AAAISS14.pdf

[7] 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)*, Austin, TX, USA, 2010, pp. 1818–1822.

[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 *Proc. Military Commun. Conf. (MILCOM)*, Baltimore, MD, USA, 2011, pp. 119–124.

[9] 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.

[10] 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. Surviv. Workshop (ISW)*, Vancouver, BC, Canada, 2002.

[11] M. Baykal-Gursoy, Z. Duan, H. V. Poor, and A. Garnaev, "Infrastructure security games," *Eur. J. Oper. Res.*, vol. 239, no. 2, pp. 469–478, Dec. 2014.

[12] 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)*, Istanbul, Turkey, 2009, pp. 697–703.

[13] 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)*, Anaheim, CA, USA, 2012, pp. 1054–1059.

[14] A. Garnaev, W. Trappe, and C.-T. Kung, "Optimizing scanning strategies: Selecting scanning bandwidth in adversarial RF environments," in *Proc. 8th Int. Conf. Cogn. Radio Orient. Wireless Netw. (CROWNCOM)*, Washington, DC, USA, 2013, pp. 148–153.

[15] L. Chen and J. Leneutreb, "Fight jamming with jamming—A game theoretic analysis of jamming attack in wireless networks and defense strategy," *Comput. Netw.*, vol. 55, no. 9, pp. 2259–2270, Jun. 2011.

[16] E. Altman, K. Avrachenkov, and A. Garnaev, "Fair resource allocation in wireless networks in the presence of a jammer," *Perform. Eval.*, vol. 67, no. 4, pp. 338–349, Apr. 2010.

[17] 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)*, Paderborn, Germany, 2012, pp. 41–48.

[18] X. Liao, D. Hao, and K. Sakurai, "Classification on attacks in wireless ad hoc networks: A game theoretic view," in *Proc. 7th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM)*, Gyeongju, Korea, 2011, pp. 144–149.

[19] V. J. Baston and A. Y. Garnaev, "A search game with a protector," *Nav. Res. Logist.*, vol. 47, no. 2, pp. 85–96, Mar. 2000.

[20] S. Lohr. (Nov. 4, 2008). *In Modeling Risk, the Human Factor was Left Out, The New York Times*. [Online]. Available: http://www.nytimes.com/2008/11/05/business/05risk.html?pagewanted=all&_r=0
[21] S. F. Cohen. (Aug. 12, 2014). *The New Cold War and the Necessity of Patriotic Heresy, The Nation*. [Online]. Available: http://www.thenation.com/article/180942/new-cold-war-and-necessity-patriotic-heresy#
[22] Y. Liu, C. Comaniciu, and H. Mani, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. Int. Conf. Perform. Eval. Methodol. Tools Proc. (Valuetools)*, Nantes, France, 2006.
[23] H. Wei and H. Sun, "Using Bayesian game model for intrusion detection in wireless ad hoc networks," *Int. J. Commun., Netw. Syst. Sci.*, vol. 3, no. 7, pp. 602–607, Jul. 2010.
[24] A. Agah, S. K. Das, K. Basu, and M. Asadi, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. 3rd IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, 2004, pp. 243–346.
[25] 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.
[26] A. Garnaev and W. Trappe, "Secret communication when the eavesdropper might be an active adversary," in *Multiple Access Communications* (LNCS 8715), M. Jonsson, A. Vinel, B. Bellalta, and E. Belyaev, Eds. Cham, Switzerland: Springer, 2014, pp. 121–136.
[27] B. An, M. Brown, Y. Vorobeychik, and M. Tambe, "Security games with surveillance cost and optimal timing of attack execution," in *Proc. 12th Int. Joint Conf. Auton. Agents Multi-Agent Syst. (AAMAS)*, St. Paul, MN, USA, 2013, pp. 223–230.
[28] B. An *et al.*, "Security games with limited surveillance," in *Proc. 26th AAAI Conf. Artif. Intell. (AAAI)*, Toronto, ON, Canada, 2012, pp. 1241–1248.
[29] S. Zamir, "Repeated games of incomplete information: Zero-sum," in *Handbook of Game Theory*, R. J. Aumann and S. Hart, Eds. Amsterdam, The Netherlands: Elsevier, 1992, pp. 110–154.
[30] J. Zheng and D. A. Castanon, "Stochastic dynamic network interdiction games," in *Proc. Amer. Control Conf. (ACC)*, Montreal, QC, Canada, 2012, pp. 1838–1844.
[31] L. Li and J. Shamma, "LP formulation of asymmetric zero-sum stochastic games," in *Proc. IEEE 53rd Annu. Conf. Decis. Control (CDC)*, Los Angeles, CA, USA, 2014, pp. 1930–1935.
[32] G. Tullock, "Efficient rent-seeking," in *Towards a Theory of the Rent-Seeking Society*, J. M. Buchanan and R. D. Tollison, and G. Tullock, Eds. College Station: Texas A&M Univ. Press, 1980, pp. 97–112.
[33] S. Skaperdas, "Contest success functions," *Econ. Theory*, vol. 7, no. 2, pp. 283–290, Feb. 1996.
[34] J. Zhuang and V. M. Bier, "Balancing terrorism and natural disasters—Defensive strategy with endogenous attack effort," *Oper. Res.*, vol. 55, no. 5, pp. 976–991, 2007.
[35] K. Hausken, "Information sharing among firms and cyber attacks," *J. Account. Public Policy*, vol. 26, no. 6, pp. 639–688, Nov./Dec. 2007.
[36] D. Fudenberg and J. Tirole, *Game Theory*. Boston, MA, USA: MIT Press, 1991.
[37] J. Callaham. (Dec. 28, 2011). *50,000 Credit Card Numbers Stolen in Stratfor Cyber Attack*. [Online]. Available: http://www.neowin.net/news/50000-credit-card-numbers-stolen-in-stratfor-cyber-attack
[38] K. Iida, R. Hohzaki, and K. Sato, "Hide-and-search game with the risk criterion," *J. Oper. Res. Soc. Jpn.*, vol. 37, no. 3, pp. 287–296, 1993.
[39] M. F. Neuts, "A multistage search game," *J. Soc. Ind. Appl. Math.*, vol. 11, no. 2, pp. 502–507, Jun. 1963.
[40] A. Garnaev, G. Garnaeva, and P. Goutal, "On the infiltration game," *Int. J. Game Theory*, vol. 26, no. 2, pp. 215–221, Jan. 1997.
[41] M. H. DeGroot, *Optimal Statistical Decisions*. Hoboken, NJ, USA: Wiley, 2004.
[42] Y. Xiao, B. Liu, Z. Hao, and L. Cao, "A similarity-based classification framework for multiple-instance learning," *IEEE Trans. Cybern.*, vol. 44, no. 4, pp. 500–515, Apr. 2014.
[43] K. Senda, S. Hattori, T. Hishinuma, and T. Kohda, "Acceleration of reinforcement learning by policy evaluation using nonstationary iterative method," *IEEE Trans. Cybern.*, vol. 44, no. 12, pp. 2696–2705, Dec. 2014.

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 the Center for Advanced Infrastructure and Transportation, Rutgers University, Piscataway, NJ, USA, and a Professor with the Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University, Russia. He has published in leading journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the *Telecommunication Systems Journal*, *Performance Evaluation*, *Naval Research Logistics*, the *International Journal of Game Theory*, and the *Journal of Optimization Theory and Applications*. His current research interests include the applications of game theory and optimization theory in network security, wireless networks, pricing, and related fields.

Melike Baykal-Gursoy received the Ph.D. degree in systems engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 1988.

Since then, she has been on the faculty of Rutgers University, Piscataway, NJ, USA, where she is currently an Associate Professor of Industrial and Systems Engineering. She has published in leading journals, such as *Mathematics of Operations Research*, *Queueing Systems: Theory and Applications*, *Mathematical Methods of Operations Research*, and the *European Journal of Operational Research*, and has a recent book entitled *Introduction to Probability and Statistics* (Kendall Hunt, 2015). Her current research interests include stochastic modeling and optimization, Markov decision processes, stochastic games, and queueing, with applications to traffic, security, and supply chains.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science 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 currently the Michael Henry Strater University Professor of Electrical Engineering and the Dean of the School of Engineering and Applied Science. His current research interests include stochastic analysis, statistical signal processing, and information theory, and their applications in wireless networks and related fields, such as social networks and smart grid. Among his publications in these areas is the recent book entitled *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor received a Guggenheim Fellowship in 2002, and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2014 International Scientific Radio Union Booker Gold Medal, and honorary doctorates from Aalborg University, Aalto University, the Hong Kong University of Science and Technology, and the University of Edinburgh. In 1990, he served as the President of the IEEE Information Theory Society, and from 2004 to 2007, he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He is a member of the National Academy of Engineering and the National Academy of Sciences, and 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.