Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 179839, 10 pages
http://dx.doi.org/10.1155/2015/179839

*Research Article*

# Quantal Response Equilibrium-Based Strategies for Intrusion Detection in WSNs

**Shigen Shen,[1,2] Keli Hu,[1] Longjun Huang,[1,3] Hongjie Li,[2] Risheng Han,[2] and Qiying Cao[4]**

[1]*Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China*
[2]*College of Mathematics, Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China*
[3]*College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China*
[4]*College of Computer Science and Technology, Donghua University, Shanghai 201620, China*

Correspondence should be addressed to Shigen Shen; shigens@126.com

Received 29 April 2015; Revised 18 July 2015; Accepted 21 July 2015

Academic Editor: Laurence T. Yang



This paper is to solve the problem stating that applying Intrusion Detection System (IDS) to guarantee security of Wireless Sensor Networks (WSNs) is computationally costly for sensor nodes due to their limited resources. For this aim, we obtain optimal strategies to save IDS agents' power, through Quantal Response Equilibrium (QRE) that is more realistic than Nash Equilibrium. A stage Intrusion Detection Game (IDG) is formulated to describe interactions between the Attacker and IDS agents. The preference structures of different strategy profiles are analyzed. Upon these structures, the payoff matrix is obtained. As the Attacker and IDS agents interact continually, the stage IDG is extended to a repeated IDG and its payoffs are correspondingly defined. The optimal strategies based on QRE are then obtained. These optimal strategies considering bounded rationality make IDS agents not always be in *Defend*. Sensor nodes' power consumed in performing intrusion analyses can thus be saved. Experiment results show that the probabilities of the actions adopted by the Attacker can be predicted and thus the IDS can respond correspondingly to protect WSNs.

## 1. Introduction

Recently, Wireless Sensor Networks (WSNs) have attracted considerable concerns owing to their broad applications. Typical examples exist in environment monitoring, health monitoring, earthquake monitoring, objects tracking, and so on [1]. One of the major issues that we must face is how to guarantee security of WSNs before they are widely applied. Similar to traditional networks, there are to realize secure WSNs and prevention- and detection-based mechanisms [2–8]. The prevention-based mechanism, which aims to prevent any attack before it occurs, includes cryptography, key management, and authentication. On the contrary, the detection-based mechanism is to identify specifically those compromised nodes after they have broken down the measures taken by the prevention step. This mechanism is generally applied using Intrusion Detection System (IDS) as the second line of defense, while the prevention-based mechanism is referred to as the first line of defense. With an IDS, key data such as intruder identification, intrusion time, and intrusion activity are provided to mitigate and remedy attack influences.

Currently, lots of IDSs [9, 10] have been proposed for various WSNs structures to provide an important security mechanism against both insider and outsider attacks. However, applying an IDS to WSNs is challenging since sensor nodes have resources limited in terms of energy, memory, computation, and communication capacities. Generally, different methods including anomaly-, misuse-, and specification-based detection are computationally expensive, which are particularly costly for small sensor nodes. This situation motivates us to seek optimal strategies of intrusion detection to possibly save sensor nodes' resources.

As a formal and mathematical tool that studies competition among involved individuals, game theory has provided us with an efficient method to explore optimal strategies in the field of intrusion detection of WSNs [11–14]. Nevertheless, game-theoretic approaches have a common assumption in which players are completely rational and the solutions

to games are based on Nash Equilibrium (NE). In real-world applications, however, all Attackers (a player in game theory) may not be always rational and they do not even care about being detected. Therefore, NE-based solutions are not suitable for such circumstances and we need a more appropriate method to solve Intrusion Detection Games.

Nowadays, Quantal Response Equilibrium (QRE) has turned into a popular alternative to the traditional NE in behavior game theory. The QRE model maintains the assumption that individuals have beliefs that are supported in equilibrium by the strategies that players choose, but with the assumption that players make systematic mistakes or deviations in their choices [15]. There are two reasons resulting in the deviation behavior. One is called bounded rationality. The other is that players' payoffs are influenced by social preference in which subjects appear altruistic or fair or seek to reciprocate fairness or seek to limit inequality in payoffs [15].

In this paper, QRE is adopted to seek optimal strategies of saving IDS agents' power in WSNs. Considering the characteristics of sensor nodes, we construct a stage Intrusion Detection Game to describe interactions between the Attacker (a player) and IDS agents (the other player). The preference structures for the Attacker and IDS agents are defined, which lead to form payoffs of players. As the stage game evolves (the Attacker and IDS agents interact continually), we extend it to a repeated game and define the corresponding payoffs. We further obtain QRE-based strategies to show how the Attacker and IDS agents will select their actions.

To the best of our knowledge, this paper is the first work to focus on exploring QRE-based strategies for intrusion detection in WSNs. The main contributions of this paper are summarized as follows:

(1) we formulate a stage Intrusion Detection Game according to Binmore's method to study strategies of malicious sensor nodes and IDS agents, which is able to reflect interactions between the Attacker and IDS agents as well as their preferences;

(2) we extend the stage Intrusion Detection Game to a repeated Intrusion Detection Game by redefining the corresponding payoffs, which is able to reflect the reality that malicious sensor nodes and IDS agents interact continually;

(3) instead of NE-based strategies, we obtain QRE-based strategies of the Attacker and IDS agents, which satisfies such a situation to the point that the Attacker and IDS agents always make their decisions with bounded rationality;

(4) we realize an implementation of applying the repeated Intrusion Detection Game to WSNs based on the algorithm of calculating QRE-based strategies that can predict the Attacker's future behavior.

The rest of this paper is organized as follows. In Section 2, we overview related work to distinguish the difference between our work and other related works. In Section 3, we construct our stage Intrusion Detection Game for WSNs and extend it to a repeated game. Further, we give a method of calculating QRE-based strategies. In Section 4, we implement an intrusion detection mechanism based on QRE-based strategies and give the corresponding algorithm. In Section 5, we perform experiments to show how the repeated Intrusion Detection Game is actually played. Finally, conclusions are provided in Section 6.

## 2. Related Work

IDSs in WSNs have attracted considerable attention. In the good survey, Butun et al. [5] presented detailed information about IDSs and the applicability of IDSs to WSNs, which are followed by the analysis and comparison of each scheme along with their advantages and disadvantages. Al-Hamadi and Chen [16] considered an optimization problem for the case where a voting-based distributed intrusion detection algorithm is employed to detect and isolate malicious nodes in WSNs. They then can dynamically determine the best redundancy level to apply to multipath routing for achieving the case of intrusion tolerance. In another paper [17], they analyzed dynamic redundancy management of integrated intrusion detection and tolerance, which is to maximize the lifetime of homogeneous clustered WSNs. To cope with potential Denial of Service attacks in WSNs, Cho et al. [18] proposed a partially distributed intrusion detection system with low memory and power requirements. In [19], Farooqi et al. proposed a novel intrusion detection mechanism including online prevention and offline detection for securing WSNs from routing attacks. To obtain efficient performance under limited computation resources of sensor nodes, Kim et al. [20] developed a Wu-Manber algorithm-based network intrusion detection system. By integrating system monitoring modules and intrusion detection modules in WSNs, Sun et al. [21] proposed an extended Kalman filter-based mechanism to detect false injected data. They further combine cumulative summation and generalized likelihood ratio to increase detection sensitivity. Shamshirband et al. [22] developed a cooperative-based fuzzy artificial immune system, in which the Cooperative-Decision-Making Module incorporates the danger detector module with the fuzzy Q-learning vaccination module to produce optimum defense strategies for detecting intrusion in WSNs. In addition, Riecker et al. [23] proposed a lightweight, energy-efficient IDS, where mobile agents are used to detect intrusions based on the energy consumption of the sensor nodes.

Since selecting the profitable detection strategy is able to lower resources consumption, game theory has been widely applied to obtain these optimal strategies. For example, the optimal strategies of launching IDS agents installed in sensor nodes are obtained by the signaling game in [24]. To determine the best defense strategies, Huang et al. [25] proposed a Markovian IDS incorporating game theory with anomaly and misuse detection, where Markov decision processes are employed with an attack-pattern-mining algorithm to predict future attack patterns. Moosavi and Bui [26] considered non-zero-sum discounted stochastic games to formally formulate and analyze the intrusion detection problem in WSNs. They assumed that the game data are not to be fully known to

the players and achieved a robust optimization approach to address this data uncertainty. On the contrary, a zero-sum stochastic game is applied in [27] to predict malicious behavior of Attackers. In [28], Shen et al. formulate a malware-defense differential game, in which the system can dynamically choose its strategies to minimize the overall cost whereas the malware intelligently varies its strategies over time to maximize this cost, to obtain optimal dynamic strategies for the system. In addition, cooperative games are also applied to formulate intrusion detection problem in WSNs. Shamshirband et al. [29] combined the game-theoretic approach and the fuzzy Q-learning algorithm to implement cooperative defense counter-attack scenarios for the sink node and the base station. The game is composed of three players consisting of sink nodes, a base station, and an Attacker and performs when a victim node in WSNs receives a flooding packet as a DDoS attack beyond a specific alarm event threshold. To obtain secure and reliable defenses of virtual sensor services in cloud-assisted WSNs, Liu et al. [30] proposed a stochastic evolutionary coalition game which is able to decide how evolutionary coalitions should be dynamically formed for reliable virtual-sensor-service composites to deliver data and how to adaptively defend in the face of uncertain attack strategies.

Among various game types, a repeated game consists of some number of repetitions of a stage game. Such a game is generally divided into two categories: finitely and infinitely repeated game, depending on whether interactions among players are finite or infinite. Players in a repeated game must consider the effects produced by their current chosen strategies on the opponents' strategies in subsequent rounds [31]. The same stage game, when played repeatedly, may result in different equilibriums. Therefore, each player must take optimal reactions against the opponent, which will affect one's payoffs in future.

Some applications of repeated game have been devoted to various aspects in wireless networks. Agah and Das [32] formulated a repeated game between IDS and sensor nodes to prevent Denial of Service (DoS) attacks in WSNs. Upon their proposed game, a protocol was proposed to category different sensor nodes based on their behavior. In [33], Pandana et al. proposed a self-learning repeated game framework to overcome selfishness and noncooperation of autonomous nodes in wireless ad hoc networks. The framework ensures the cooperation among nodes for the current packet forwarding and finds the better cooperation probabilities by self-learning algorithms. Chen et al. [34] constructed a repeated game model based on reputation for wireless networks to fully utilize the scarce spectrum resource. The model is able to help multiple primary and secondary users coexist and share the spectrum. Using a repeated game to enforce cooperation among nodes in wireless networks, Kong and Kwok [35] proposed an efficient packet-scheduling algorithm that leads to an equilibrium. Upon the algorithm, the wireless channel resources are fully utilized. The other typical cooperation applications of repeated game are composed of cooperative multicast [36], network selection [37], and power trading [38]. In addition, Sagduyu et al. [39] formulated a repeated game under network uncertainty to deal with jamming attacks in wireless networks. A multiattacker repeated colluding game is proposed in [40] to find subgame equilibriums that indicate the optimal strategies of Attackers. Upon these equilibriums, a security policy is established to detect malicious nodes that collude with each other to launch the selective forwarding attacks. Moreover, cognitive radio users, using a repeated game in [41], can adapt their power by observing the interference from the feedback signals of primary users and transmission rates obtained in the previous stage. Zhu and Martínez [42] developed a repeated game to solve the coverage optimization problem of mobile sensors. To defend against multistage attacks, Luo et al. [43] modeled a two-player non-zero-sum noncooperative dynamic multistage game with incomplete information to find the best actions for defenders. Sun et al. [44], considering inherent uncertainty of nodes in ad hoc networks, proposed a power control mechanism with a dynamic repeated game-theoretic framework. Smith et al. [45] proposed a dynamic noncooperative repeated game for transmitting power control across multi-source-destination distributed wireless networks. Recently, the "zero-determinant strategies" [46–50] of a repeated game have attracted much attention in scientific world. In particular, Farraj et al. [48] employed a repeated game-theoretic formulation to describe the interactions of the parties in cyber-enabled power systems. Transient stabilization over time using zero-determinant strategies is obtained to indicate the potential of the constrained controller.

Based on the repeated game, QRE developing the concept of NE considers bounded rationality and thus is profitable to describe the dilemma of security source allocation. To fit the bounded rationality of human adversaries in security game, Yang et al. [51] modeled human behavior of adversaries and provided new mathematical models based on prospect theory and stochastic discrete choice model. A modification of QRE is proposed to develop algorithms that are efficient to compute the best response of the security forces when playing against the different adversaries. In [52], QRE is used to capture players' bounded rationality and to model internal Attackers' behavior. The results are able to predict how an internal Attacker will act in future. Then, a detailed game-based detection algorithm taking advantage of these results is described in detail.

## 3. Constructing Intrusion Detection Game for WSNs

*3.1. Network Model.* According to classification based on the installation location of IDS agents, there are purely distributed, purely centralized, and distributed-centralized structures [53]. For the purely distributed situation, each sensor node has been equipped with an IDS agent that locally examines malicious actions from neighboring sensor nodes. On the contrary, for the purely centralized situation, the base station (BS) has been equipped with the IDS agent, where a special protocol is necessary to gather information from sensor nodes to examine the behavior of sensor nodes. In addition, for the distributed-centralized situation, monitor sensor nodes are introduced and have been equipped with

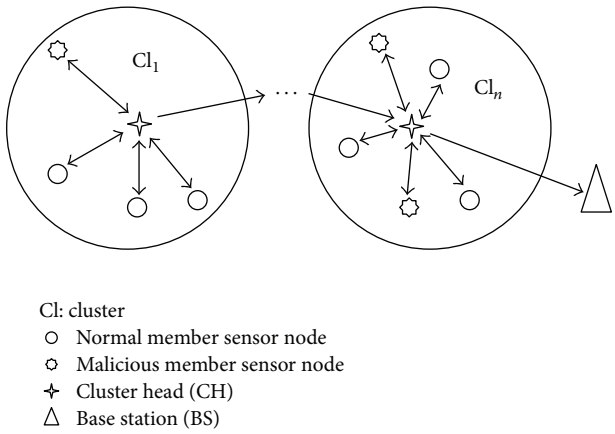


Figure 1: Network model [24].

IDS agents. Not only do these monitor nodes perform activities like normal nodes, but also they check for intrusion detection.

Our network model adopts the same one in [24], as depicted in Figure 1. This model belongs to the distributed-centralized case. However, under clustering hierarchy, each sensor node has been equipped with an IDS agent, which is not the same as the situation where IDS agents are only installed in monitor sensor nodes. When an energy-abundant sensor node is elected as a cluster head (CH), the deployed IDS agent will launch simultaneously while the IDS agents in member sensor nodes are in sleep. Therefore, a CH executes the task of intrusion detection by the IDS agent in addition to aggregating and sending data.

### 3.2. Stage Intrusion Detection Game

*Definition 1.* The stage Intrusion Detection Game (IDG) is a 3-tuple $\mathbb{G} = (\mathcal{N}, \mathcal{A}, \mathcal{U})$, where

(1) $\mathcal{N} = \{\text{Attacker } i, \text{IDS agent } j\}$ is a set of players;

(2) $\mathcal{A} = \mathcal{A}_i \times \mathcal{A}_j$, where $\mathcal{A}_i = \{Cooperate\ (C), Preattack\ (P), Attack\ (A)\}$ and $\mathcal{A}_j = \{Sleep\ (S), Grant\ (G), Defend\ (D)\}$ are the sets of actions adopted by players $i$ and $j$, respectively;

(3) $\mathcal{U} = \mathcal{U}_i \times \mathcal{U}_j$, where $\mathcal{U}_i = \{u_i(s_i) : \mathcal{A}_i \mapsto \mathbb{R}\}$ and $\mathcal{U}_j = \{u_j(s_j) : \mathcal{A}_j \mapsto \mathbb{R}\}$ are the sets of payoffs of players $i$ adopting strategy $s_i$ and $j$ adopting strategy $s_j$, respectively.

In Definition 1, we consider that the game is played by the Attacker ($i$) versus the IDS agents ($j$). Player $i$ is in fact referred to malicious sensor nodes that have such purposes as to listen to sensor information, devastate a sensor node's communication abilities, or entirely disable a sensor node. On the other hand, player $j$ is referred to IDS agents that are initially installed in CHs. The goal of our Intrusion Detection Game is, from the view of game theory, to supply optimal strategies for IDS agents in response to the Attacker selecting its strategies dynamically.

As an Attacker, player $i$ has three possible actions. It may take the action *Cooperate* ($C$), meaning that it acts normally during communications among other sensor nodes. This action disguises it to avoid being captured by its opponent. However, the intentions of player $i$ are hostile, and therefore its aim is to systematically arrange methods so that it can attack other sensor nodes for its own profits. Generally, it might disclose private information of other sensor nodes for obtaining other information required for it to finish an attack. These actions are known as reconnaissance attacks and can be summarized as the action *Preattack* ($P$). Moreover, an Attacker finally achieve the phase in which the action *Attack* ($A$) is made to obtain its expected profit. This action is without doubt the most threatening action among all. It raises and strengthens the seriousness of the problem and leads to many unexpected results such as a network unavailable for its legitimate sensor nodes, inaccurate sensing information, and leaking private data. In summary, the set of actions of player $i$ is $\{C, P, A\}$.

To confront Attackers, player $j$ also has three actions. Due to limited resources in sensor nodes, the strategy that IDS agents are always in *Defend* is not optimal. Otherwise, cluster heads installed IDS agents will consume their power quickly since processing intrusion detection is generally costly. Player $j$ may therefore take the action *Sleep* ($S$) for saving energy. After launching IDS agents, it may grant sensor nodes to continue when no malicious behavior has been discovered. Note that two cases result in the fact that player $j$ takes this action *Grant* ($G$). One case is that the Monitored Events are truly normal. The other is that IDS agents cannot detect the malicious events since any IDS has the false negative rate. In addition, player $j$ will take the action *Defend* ($D$) to stop the work of malicious sensor nodes once violations are detected. In a summary, the set of actions of player $j$ is $\{S, G, D\}$.

Based on the above analyses, there are nine possible combinations between the Attacker's actions and the IDS agent's actions. For example, strategy profile $(C, S)$ means that player $i$ acts normally and player $j$ is in sleep for saving energy. $(P, G)$ means that player $i$ acts in a preattack step and player $j$ grants its opponent to continue for not detecting reconnaissance attacks. $(A, D)$ means that player $i$ performs attacking behavior and player $j$ prevents its opponent from its malicious work to protect sensor nodes.

Finally, let us quantify preferences and payoffs of players in the stage IDG. Let the symbols $\succ$ and $\sim$ be the preference and indifference, respectively. For example, if $x \succ y$, then it is said that $x$ is preferred to $y$.

For the player Attacker, it is most profitable to attack successfully the WSNs without being defended. Since the IDS agents taking the action *Sleep* or *Grant* cannot defend the Attacker, the preference of strategy profile $(A, G)$ is indifferent to that of $(A, S)$. Its next choice is to take the action *Cooperate* without being defended. The following preference action is *Preattack* without any deterrence. The action *Attack* that is defended follows the Attacker's favorite, which is more preferable than the action *Cooperate* that is defended. Finally, the worst choice is the action *Preattack* responded by the

Table 1: Payoff matrix.

| | $S$ | $G$ | $D$ |
|---|---|---|---|
| $C$ | (6, 8) | (6, 7) | (1, 4) |
| $P$ | (4, 3) | (4, 2) | (0, 5) |
| $A$ | (8, 1) | (8, 0) | (2, 6) |

action *Defend*. The above analyses result in the following preference structure:

$$(A,S) \sim (A,G) \succ (C,S) \sim (C,G) \succ (P,S) \sim (P,G) \succ (A,D) \succ (C,D) \succ (P,D). \quad (1)$$

With respect to the player IDS agents, the most preferable profile is the action *Cooperate* followed by the action *Sleep*. The following is the action *Cooperate* followed by the action *Grant* since taking the action *Grant* spends more power for detection than taking *Sleep*. When it takes the action *Defend*, it prefers orderly the actions *Attack*, *Preattack*, and *Cooperate*. It next prefers the action *Preattack* followed orderly by the actions *Sleep* and *Grant*. The least preferable profile is the action *Attack* followed by the action *Grant*. Therefore, the preference structure attained is

$$(C,S) \succ (C,G) \succ (A,D) \succ (P,D) \succ (C,D) \succ (P,S) \succ (P,G) \succ (A,S) \succ (A,G). \quad (2)$$

According to Binmore's method [54], rational numbers are assigned to reflect players' preferences ranked in (1) and (2). Then, after being multiplied with their least common factor, the values of payoff functions $u_i$ and $u_j$, free of fractions, can be formed in Table 1.

*3.3. Repeated Intrusion Detection Game.* In the realistic WSNs, interactions between players Attacker and IDS agents are continually performed. Therefore, the stage IDG will be played more than once and it is reasonable to model these interactions as a repeated game. Generally, a repeated game is a particular style of an extensive form game in which each stage is a repetition of the same strategic-form game. The times of playing a repeated game may be finite or infinite. If the game never ends (Attacker and IDS agent interact forever) or players (Attacker and IDS agent) do not know when the game ends, it is called an infinitely repeated game, which will be employed in this paper. In a repeated game, a strategy is an entire plan of action described in the stage game. When each stage ends, all players are able to observe the consequence of the stage game and make a choice to select the future actions depending on the history of actions. The overall payoff in a repeated game is denoted by a normalized discounted aggregate of the payoff at each stage game. Our repeated Intrusion Detection Game (RIDG) can be defined as follows.

*Definition 2.* The infinite $\delta$-discounted RIDG is composed of repeated game $\mathbb{G}$, which is denoted by $\mathbb{G}(\infty, \delta)$, where

(1) the set of players is $\mathcal{N}$ defined in Definition 1;

(2) for every player $x \in \{i, j\}$, its overall strategy at the $t$th stage IDG is $s_x^t = [s_x(h_0), s_x(h_1), \ldots, s_x(h_t)]$, where $h_y$, $y \in \{0, 1, \ldots, t\}$, denotes the $y$th history stage and $s_x(h_y)$ denotes the strategy adopted by player $x$ at the $y$th history stage;

(3) for every player $x \in \{i, j\}$, its overall payoff is the $\delta$-discounted average of instant payoffs from each round of the repeated Intrusion Detection Game.

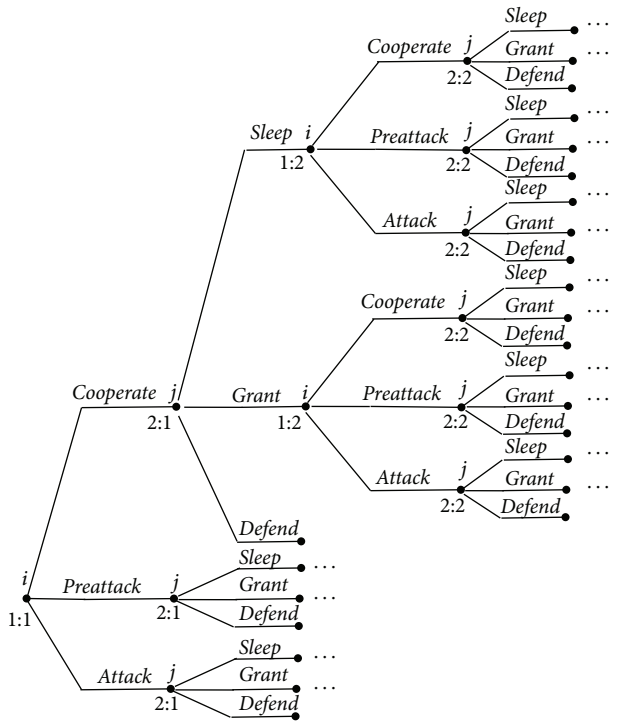


Figure 2: Repeated Intrusion Detection Game.

Figure 2 shows a representation of the RIDG in extensive form. In fact, an Attacker is perfectly aware of IDS agents' past actions because IDS agents exert actions on the Attacker. In other words, player $j$'s (IDS agents') actions are perfectly known by player $i$ (Attacker). On the other hand, player $j$ is imperfectly aware of player $i$'s past choices because player $j$ judges its opponent's actions with uncertainty. Consequently, the RIDG belongs to a repeated dynamic game with imperfect information.

From Figure 2, player $i$ first takes an action at the beginning node. It may select action *Cooperate*, *Preattack*, or *Attack*. Next, player $j$ responds to its opponent with action *Sleep*, *Grant*, or *Defend*. As soon as it selects action *Defend*, the game ends. Except for this case, the game will be played repeatedly.

Now, let us define players' payoffs for the repeated IDG. Players Attacker and IDS agents strive to maximize their expected payoffs over multiple rounds of the stage IDG. The expected payoff is generally described as a sum of per-period payoffs, multiplied by a discount factor $\delta$, $\delta \in [0, 1)$. If the discount factor is not too high, the players then are interested enough in future outcomes of the game. Both players therefore put more weight on the current payoff than

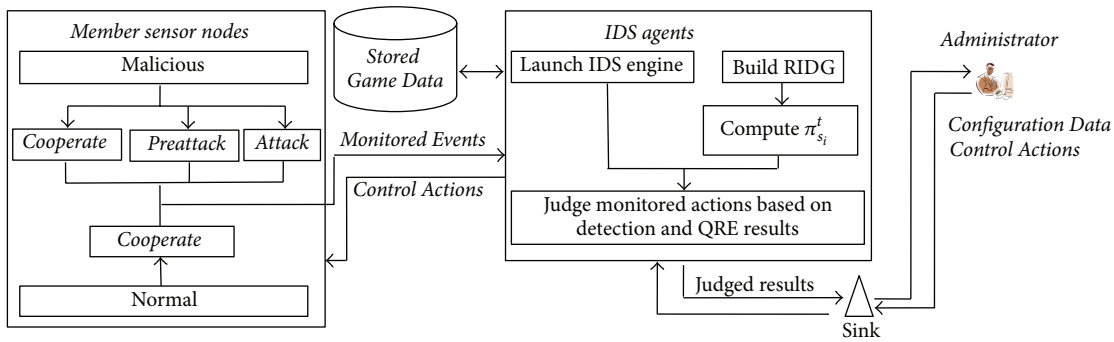


Figure 3: Implementation of applying our RIDG to WSNs.

on the future payoffs. The total payoff for player $x$, $x \in \{i, j\}$, is given as

$$u_x^t(s_x) = \sum_{y=0}^{t} \delta^y u_x^y(s_x), \tag{3}$$

where $u_x^y(s_x)$ denotes the payoff obtained by player $x$, $x \in \{i, j\}$, adopting strategy $s_x$ at slot time, $y$, $y = 0, 1, 2, \ldots, t$. Further, in the repeated game with infinite rounds, the total payoff in (3) is often averaged. Therefore, the average discounted payoff for player $x$, $x \in \{i, j\}$, can be expressed as

$$\overline{u}_x^t(s_x) = (1-\delta) \sum_{y=1}^{t} \delta^y u_x^y(s_x). \tag{4}$$

Next let us analyze the total number of strategy profiles in our RIDG. Generally, as an infinitely repeated game, the total number of strategy profiles at the $t$th stage is computed by multiplying the number of history strategy profiles at all stages $0, 1, \ldots, t-1$, with the number of actions to be played at the $t$th stage. However, in our RIDG, the action *Defend* adopted by player $j$ means that the game ends. In this sense, the number of combined actions excluding the terminal action *Defend* is $3 \times 2 = 6$. Therefore, the total number of strategy profiles at the $t$th stage, $n_t$, can be computed as

$$n_t = 6 \times n_{t-1}, \quad t = 1, 2, 3, \ldots, \tag{5}$$

where $n_0 = 9$.

From (5), we can see that the total number of strategy profiles of our RIDG will increase quickly as the number of all repeated stage IDGs grows. As a result, complexity to predict the future behavior of player $i$ by computing the NE of a subgame becomes higher and higher, which motivates us to find an optimal alternative, QRE.

*3.4. QRE-Based Strategies.* QRE for extensive form games is first defined by McKelvey and Palfrey [55], which provides an equilibrium notion with bounded rationality. QRE is not an equilibrium refinement, and it can obtain significantly different results from NE. It is only defined for games with separate strategies, regardless of the fact that there are repeated-strategy analogues. In particular, it is developed as a probabilistic extension of NE and can be used to give reasons why players might systematically deviate from the NE path. This is because players in QRE are assumed to make errors in selecting which strategy to play. The probability of any particular strategy being picked is positively related to the highest expected payoff from that strategy. Therefore, strategy choices in QRE are probabilistic rather than deterministic.

The characteristic that QRE provides equilibrium with bounded rationality is realized by introducing a rationality parameter to the payoff. The rationality parameter denoted by $\lambda$ is changed during the process of QRE converging to the NE. When $\lambda = 0$, players are completely irrational. This case means that even though a player cannot obtain greater payoff, players Attacker and IDS agents will select another strategy other than the one indicated by NE. On the contrary, when $\lambda \to \infty$, players will follow NE since they become completely rational in this case. So far, the QRE can be calculated by

$$\pi_{s_x}^t = \frac{\exp(\lambda \cdot \overline{u}_x^t(s_x))}{\sum_{y \in \mathscr{A}_x} \exp(\lambda \cdot \overline{u}_x^t(y))}, \tag{6}$$

where $\pi_{s_x}^t$ is in fact the probability of player $x$, $x \in \{i, j\}$, selecting strategy $s_x$. From (6), QRE-based strategies of players Attacker and IDS agents can be obtained, respectively. In essence, QRE-based strategies are based on the introduction of payoff perturbations associated with actions adopted by players Attacker and IDS agents. The probability of a strategy profile is positively related to the average discounted payoffs held by players. The set of QRE can be regarded as a correspondence mapping the rationality parameter $\lambda$ into a set of mixed strategy (the probability that each action of IDS agents will be selected by IDS agents) in $\mathscr{A}$.

## 4. QRE-Based Intrusion Detection for WSNs

As given in Figure 3, we realize an implementation of applying our RIDG to WSNs. The data flow begins with member sensor nodes that are being monitored by the IDS agents installed in the corresponding CH. These member sensor nodes may be normal or malicious, so they take possible actions including *Cooperate*, *Preattack*, and *Attack*. As soon as the IDS agent is woken by events of member sensor nodes,

(1) $t \leftarrow 1$;
(2) Initialize game parameters required in Definition 2;
(3) Do UNTIL the end of interactions between players Attacker and the corresponding IDS agent
(4) Woken by *Monitored Events*;
(5) Judge whether *Monitored Events* are normal or malicious with the known intrusion detection techniques;
(6) IF the output of detection is malicious THEN
(7) IF the RIDG is not existed THEN
(8) Construct the first stage RIDG with game parameters including $\mathcal{N}$, $\mathcal{A}$, and $\mathcal{U}$;
(9) ELSE
(10) Obtain the current stage RIDG from the *Stored Game Data*;
(11) ENDIF
(12) Compute $\pi^t_{s_x}$ according to (6);
(13) Compute $\overline{u}^t_x(s_x)$ according to (4) and store it into the *Stored Game Data* for the next stage RIDG;
(14) Combine IDS results and $\pi^t_{s_x}$, and send them to *Administrator*;
(15) ENDIF
(16) $t \leftarrow t + 1$;
(17) ENDDO

Algorithm 1: QRE-based intrusion detection algorithm for IDS agents.

it filters the Monitored Events and employs an IDS engine to judge whether an event is normal or not.

Generally, IDS agents have been previously configured to make them more accurate and reliable, through Configuration Data sent by *Administrator*. Upon completion of events detection, the relevant results will be temporarily stored for the final decision. On the other hand, the IDS agent starts to initialize game parameters required in Definition 2. It accepts the results of events detection and formulates the RIDG. When the RIDG is constructed at the first stage, preferences and payoffs of two players, which have been stored in the *Stored Game Data*, are manually set by *Administrator*. The IDS agent then, employing (6), calculates the QRE probabilities with the events detection results and the stage RIDG. The QRE probabilities attained will be combined with the IDS results, and this combination will be sent to Administrator who may take Control Actions on member sensor nodes through the IDS agent. After one round of RIDG is played, the game parameters will be updated to the *Stored Game Data*. In particular, the payoffs of two players are adjusted according to (4), which will be used in the next stage RIDG. The above process will then be repeated until the IDS agent selects action *Defend*. In fact, reaching this point means the end of interactions between players Attacker and IDS agents. Next, we describe the algorithm for the process of QRE-based intrusion detection (Algorithm 1).

## 5. Experiments

With Gambit [56], QRE-based strategies are calculated to show us how the RIDG is actually played, as illustrated in Table 2 and Figures 4 and 5. These illustrations show that we are able to predict the Attacker's actions, so that the corresponding IDS agent can adopt the appropriate action in advance. Calculations begin with equal probabilities for each action. In this manner, every action has a probability of 0.3333

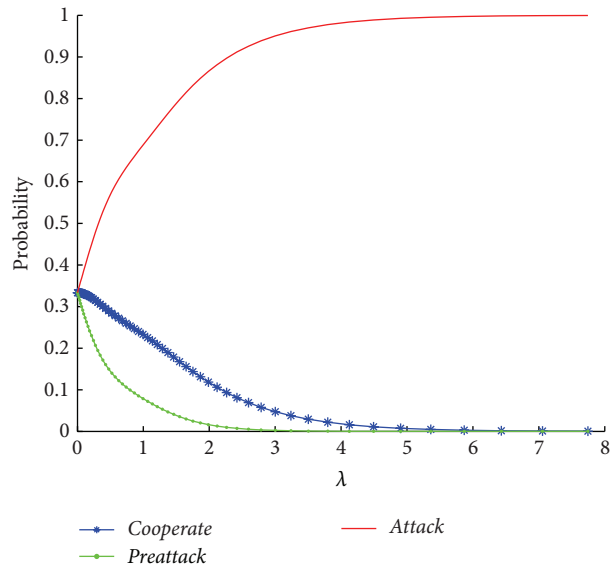


Figure 4: QRE-based strategies for the player Attacker.

or so, since there are three actions for each player. In addition, the rationality parameter $\lambda$ starts with $\lambda = 0$ at step 1.

The trend of actions adopted by the Attacker is shown in Figure 4, where $y$-axis represents the probability the Attacker will select a certain strategy for a given $\lambda$. It is remarkable that the probability of the Attacker adopting the action *Cooperate* or *Preattack* is gradually decreasing while the probability of the action *Attack* is increasing. From Table 2, when $\lambda \approx 3.238326$, the probability of the action *Preattack* becomes zero approximately. This case means the action *Preattack* has been eliminated from this step. Adapting the Attacker's strategies continually, it is $\lambda \approx 161.049147$, when the selection by the Attacker of the action *Attack* becomes certain. This means

Table 2: QRE calculations for the players Attacker and IDS agents in the RIDG.

| Step | $\lambda$ | Attacker | | | IDS agents | | |
|---|---|---|---|---|---|---|---|
| | | *Cooperate* | *Preattack* | *Attack* | *Sleep* | *Grant* | *Defend* |
| 1 | 0 | 0.333333 | 0.333333 | 0.333333 | 0.333333 | 0.333333 | 0.333333 |
| 2 | 0.010248 | 0.333301 | 0.327668 | 0.339031 | 0.333302 | 0.329903 | 0.336795 |
| 3 | 0.021502 | 0.333192 | 0.321514 | 0.345294 | 0.333192 | 0.326104 | 0.340703 |
| 4 | 0.033854 | 0.332985 | 0.314843 | 0.352172 | 0.332978 | 0.321894 | 0.345128 |
| 5 | 0.047402 | 0.332655 | 0.307631 | 0.359715 | 0.332625 | 0.317226 | 0.35015 |
| 6 | 0.062251 | 0.332172 | 0.299857 | 0.367971 | 0.332088 | 0.312046 | 0.355866 |
| 7 | 0.078512 | 0.331504 | 0.291508 | 0.376987 | 0.331314 | 0.306297 | 0.36239 |
| 8 | 0.0963 | 0.330612 | 0.28258 | 0.386808 | 0.330231 | 0.299913 | 0.369856 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 47 | 3.238326 | 0.0376928 | 0.00147867 | 0.960829 | $2.83E-07$ | $1.11E-08$ | 1 |
| 48 | 3.502404 | 0.0292182 | 0.000880193 | 0.969902 | $6.29E-08$ | $1.89E-09$ | 1 |
| 49 | 3.797081 | 0.021933 | 0.000492093 | 0.977575 | $1.21E-08$ | $2.71E-10$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 89 | 161.049147 | $1.14E-70$ | $1.30E-140$ | 1 | 0 | 0 | 1 |
| 90 | 177.142263 | $1.17E-77$ | $1.37E-154$ | 1 | 0 | 0 | 1 |
| 91 | 194.844691 | $2.40E-85$ | $5.76E-170$ | 1 | 0 | 0 | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 104 | 672.367387 | $9.88E-293$ | 0 | 1 | 0 | 0 | 1 |
| 105 | 739.592327 | $6.27463E-322$ | 0 | 1 | 0 | 0 | 1 |
| 106 | 813.539761 | 0 | 0 | 1 | 0 | 0 | 1 |

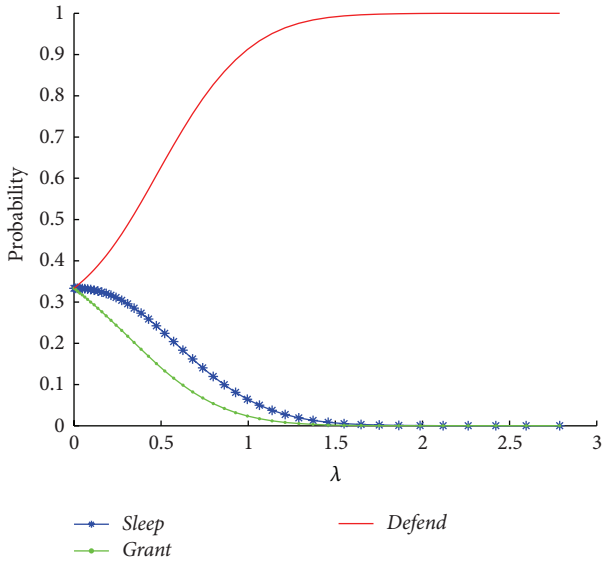


Figure 5: QRE-based strategies for the player IDS agents.

that if $\lambda$ is greater than 161.049147, then the Attacker always selects the action *Attack* that is in fact the NE of the stage IDG.

Figure 5 shows the trend of actions adopted by IDS agents, where the probability of the action *Sleep* or *Grant* is decreasing and the probability of the action *Defend* is increasing. However, compared to the changeable trend of the selection by the Attacker, the action adopted by the IDS agents converges quickly to the action *Defend* that is the NE of the stage IDG. This point, from Table 2, is obtained when $\lambda \approx 3.238326$ for the IDS agents while $\lambda$ is 161.049147 or so for the Attacker.

## 6. Conclusion

To save sensor nodes' power, we have put forward a method based on QRE to make IDS agents not always be in *Defend*. A stage IDG that is able to reflect interactions between the Attacker and IDS agents has been formulated, where we have thoroughly considered players' preferences and have assigned payoffs of players according to Binmore's method. To reflect the reality that the Attacker and IDS agents interact continually, we have extended the stage IDG to a repeated IDG and have defined the corresponding payoffs. Further, we have given the method of calculating QRE-based strategies that predict the Attacker's future behavior. As a result, optimal reactions can be suggested to the IDS agents to protect WSNs.

In the future, to extend the current game model RIDG when taking into account multiple Attackers that may collude is an interesting work.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## Acknowledgments

This work was supported by National Natural Science Foundation of China under Grant no. 61272034, by Zhejiang Provincial Natural Science Foundation of China under Grants LY13F030012 and LY13F020035, and by Science Foundation of Shaoxing University under Grants 20145021 and 2014LG1009.

## References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] A. Ramos and R. H. Filho, "Sensor data security level estimation scheme for wireless sensor networks," *Sensors*, vol. 15, no. 1, pp. 2104–2136, 2015.

[3] A. Derhab, A. Bouras, M. R. Senouci, and M. Imran, "Fortifying intrusion detection systems in dynamic Ad Hoc and wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 608162, 15 pages, 2014.

[4] R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[5] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[6] C.-F. Hsieh, R.-C. Chen, and Y.-F. Huang, "Applying an ontology to a patrol intrusion detection system for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 634748, 14 pages, 2014.

[7] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 371–383, 2015.

[8] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 375–385, 2014.

[9] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[10] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[11] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, article 25, 39 pages, 2013.

[12] S. Shen, G. Yue, Q. Cao, and F. Yu, "A survey of game theory in wireless sensor networks security," *Journal of Networks*, vol. 6, no. 3, pp. 521–532, 2011.

[13] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 472–486, 2013.

[14] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, "Game theory for wireless sensor networks: a survey," *Sensors*, vol. 12, no. 7, pp. 9055–9097, 2012.

[15] M. D. McCubbins, M. Turner, and N. Weller, "Testing the foundations of quantal response equilibrium," in *Social Computing, Behavioral-Cultural Modeling and Prediction*, vol. 7812 of *Lecture Notes in Computer Science*, pp. 144–153, Springer, Berlin, Germany, 2013.

[16] H. Al-Hamadi and I.-R. Chen, "Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks," *IEEE Transactions on Network and Service Management*, vol. 10, no. 2, pp. 189–203, 2013.

[17] H. Al-Hamadi and I. R. Chen, "Integrated intrusion detection and tolerance in homogeneous clustered sensor networks," *ACM Transactions on Sensor Networks*, vol. 11, no. 3, article 47, 24 pages, 2015.

[18] E. J. Cho, C. S. Hong, S. Lee, and S. Jeon, "A partially distributed intrusion detection system for wireless sensor networks," *Sensors*, vol. 13, no. 12, pp. 15863–15879, 2013.

[19] A. H. Farooqi, F. A. Khan, J. Wang, and S. Lee, "A novel intrusion detection framework for wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 907–919, 2013.

[20] I. Kim, D. Oh, M. K. Yoon, K. Yi, and W. W. Ro, "A distributed signature detection method for detecting intrusions in sensor systems," *Sensors*, vol. 13, no. 4, pp. 3998–4016, 2013.

[21] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 13–25, 2013.

[22] S. Shamshirband, N. B. Anuar, M. L. M. Kiah et al., "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–117, 2014.

[23] M. Riecker, S. Biedermann, R. El Bansarkhani, and M. Hollick, "Lightweight energy consumption-based intrusion detection system for wireless sensor networks," *International Journal of Information Security*, vol. 14, no. 2, pp. 155–167, 2015.

[24] S. Shen, Y. Li, H. Xu, and Q. Cao, "Signaling game based strategy of intrusion detection in wireless sensor networks," *Computers & Mathematics with Applications*, vol. 62, no. 6, pp. 2404–2416, 2011.

[25] J.-Y. Huang, I.-E. Liao, Y.-F. Chung, and K.-T. Chen, "Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining," *Information Sciences. An International Journal*, vol. 231, pp. 32–44, 2013.

[26] H. Moosavi and F. M. Bui, "A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1367–1379, 2014.

[27] S. Shen, R. Han, L. Guo, W. Li, and Q. Cao, "Survivability evaluation towards attacked WSNs based on stochastic game and continuous-time Markov chain," *Applied Soft Computing*, vol. 12, no. 5, pp. 1467–1476, 2012.

[28] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, pp. 1962–1973, 2014.

[29] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, vol. 32, pp. 228–241, 2014.

[30] J. Liu, S. Shen, G. Yue, R. Han, and H. Li, "A stochastic evolutionary coalition game model of secure and dependable virtual service in Sensor-Cloud," *Applied Soft Computing*, vol. 30, pp. 123–135, 2015.

[31] A. B. MacKenzie and L. A. DaSilva, *Game Theory for Wireless Engineers*, Morgan & Claypool Publishers, San Rafael, Calif, USA, 2006.

[32] A. Agah and S. K. Das, "Preventing DoS attacks in wireless sensor networks: a repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[33] C. Pandana, Z. Han, and K. J. R. Liu, "Cooperation enforcement and learning for optimizing packet forwarding in autonomous wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 3150–3163, 2008.

[34] J. Chen, S. Lian, C. Fu, and R. Du, "A hybrid game model based on reputation for spectrum allocation in wireless networks," *Computer Communications*, vol. 33, no. 14, pp. 1623–1631, 2010.

[35] Z. Kong and Y.-K. Kwok, "Efficient wireless packet scheduling in a non-cooperative environment: game theoretic analysis and algorithms," *Journal of Parallel and Distributed Computing*, vol. 70, no. 8, pp. 790–799, 2010.

[36] B. Niu, H. V. Zhao, and H. Jiang, "A cooperation stimulation strategy in wireless multicast networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2355–2369, 2011.

[37] R. Trestian, O. Ormond, and G.-M. Muntean, "Reputation-based network selection mechanism using game theory," *Physical Communication*, vol. 4, no. 3, pp. 156–171, 2011.

[38] S. Kandeepan, S. K. Jayaweera, and R. Fedrizzi, "Power-trading in wireless communications: a cooperative networking business model," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1872–1880, 2012.

[39] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112–118, 2011.

[40] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, "A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks," *Computer Communications*, vol. 35, no. 17, pp. 2125–2137, 2012.

[41] P. Zhou, Y. Chang, and J. A. Copeland, "Reinforcement learning for repeated power control game in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 54–69, 2012.

[42] M. Zhu and S. Martínez, "Distributed coverage games for energy-aware mobile sensor networks," *SIAM Journal on Control and Optimization*, vol. 51, no. 1, pp. 1–27, 2013.

[43] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "A fictitious play-based response strategy for multistage intrusion defense systems," *Security and Communication Networks*, vol. 7, no. 3, pp. 473–491, 2014.

[44] Y. Sun, Y. Guo, Y. Ge, S. Lu, J. Zhou, and E. Dutkiewicz, "Improving the transmission efficiency by considering non-cooperation in ad hoc networks," *Computer Journal*, vol. 56, no. 8, pp. 1034–1042, 2013.

[45] D. B. Smith, M. Portmann, W. L. Tan, and W. Tushar, "Multi-source-destination distributed wireless networks: pareto-efficient dynamic power control game with rapid convergence," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2744–2754, 2014.

[46] A. A. Daoud, G. Kesidis, and J. Liebeherr, "Zero-determinant strategies: a game-theoretic approach for sharing licensed spectrum bands," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2297–2308, 2014.

[47] D. Hao, Z.-H. Rong, and T. Zhou, "Zero-determinant strategy: an underway revolution in game theory," *Chinese Physics B*, vol. 23, no. 7, Article ID 078905, 2014.

[48] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Transactions on Smart Grid*, 2015.

[49] H. Zhang, N. Dusit, L. Song, T. Jiang, and Z. Han, "Zero-determinant strategy in cheating management of wireless cooperation," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '14)*, pp. 4382–4386, Austin, Tex, USA, December 2014.

[50] D. Hao, Z. Rong, and T. Zhou, "Extortion under uncertainty: zero-determinant strategies in noisy games," *Physical Review E—Statistical, Nonlinear, and Soft Matter Physics*, vol. 91, no. 5, Article ID 052803, 8 pages, 2015.

[51] R. Yang, C. Kiekintveld, F. Ordóñez, M. Tambe, and R. John, "Improving resource allocation strategies against human adversaries in security games: an extended study," *Artificial Intelligence*, vol. 195, pp. 440–469, 2013.

[52] I. Kantzavelou and S. Katsikas, "A game-based intrusion detection mechanism to confront internal attackers," *Computers & Security*, vol. 29, no. 8, pp. 859–874, 2010.

[53] A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 9, no. 2, pp. 69–83, 2012.

[54] K. Binmore, *Playing for Real : A Text on Game Theory*, Oxford University Press, New York, NY, USA, 2007.

[55] R. D. McKelvey and T. R. Palfrey, "Quantal response equilibria for extensive form games," *Experimental Economics*, vol. 1, no. 1, pp. 9–41, 1998.

[56] R. D. McKelvey, A. M. McLennan, and T. L. Turocy, "Gambit: Software Tools for Game Theory," Version 14.1.0, 2014, http://www.gambit-project.org/.