Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 184239, 14 pages
http://dx.doi.org/10.1155/2015/184239

Research Article

Optimal Report Strategies for WBANs Using a Cloud-Assisted IDS

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 20 May 2015; Accepted 28 October 2015

Academic Editor: Marcello Cinque

Applying an Intrusion Detection System (IDS) to Wireless Body Area Networks (WBANs) becomes a costly task for body sensors due to their limited resources. To solve this problem, a cloud-assisted IDS framework is proposed. We adopt a new distributed-centralized mode, where IDS agents residing in body sensors will be triggered to launch. All IDS agents are only responsible for reporting the monitored events, not intrusion decision that is processed in the cloud platform. We then employ the signaling game to construct an IDS Report Game (IDSRG) depicting interactions between a body sensor and its opponent. The pure- and mixed-strategy Bayesian Nash Equilibriums (BNEs) of the stage IDSRG are achieved, respectively. As two players interact continually, we develop the stage IDSRG into a dynamic multistage game in which the belief can be updated dynamically. Upon the current belief, the Perfect Bayesian Equilibrium (PBE) of the dynamic multistage IDSRG is attained, which helps the IDS-sensor select the optimal report strategy. We afterward design a PBE-based algorithm to make the IDS-sensor decide when to report the monitored events. Experiments show the effectiveness of the dynamic multistage IDSRG in predicting the type and optimal strategy of a malicious body sensor.

1. Introduction

Recently, a specific class of Wireless Sensor Networks, known as Wireless Body Sensor Networks (WBSNs) or Wireless Body Area Networks (WBANs), has been developed as physiological sensors and low power integrated circuits are rapidly evolving. A WBAN is generally composed of some miniaturized and intelligent sensors attached on or implanted in the body, which are able to establish wireless communication links. Such networks have attracted considerable attention since they are capable of allowing for many human-central applications such as health monitoring, sports training, interactive gaming, and personal information sharing [1–5]. However, applying WBANs has to face many issues and challenges due to limited resources of body sensors [6]. One challenge in a common healthcare scenario is how to process, store, and manage the huge amount of data gathered by body sensors. Another challenge is how to meet the strict security requirement of WBANs applications [7, 8]. The openness of the wireless media of WBANs makes a malicious attacker easy to launch various attacks. Moreover, data collected by body sensors are health related and highly sensitive. Security threats may result in a patient in a hazardous situation and even death in the case of medical applications of WBANs. Therefore, Intrusion Detection System (IDS) is required to prevent body sensors from malicious actions. However, employing IDS is a costly task for body sensors due to their limited computation capability and storage capability. Moreover, these body sensors usually hold limited power while approaches to realizing IDS are computationally expensive in general. To solve these problems, cloud computing can be seen as a good remedy.

As infrastructure, cloud computing provides various services in fields of computation, storage, data access, security, and software [9, 10]. This computing model is therefore

expected to play a significant role to make up for the deficiencies of body sensors. Combining WBANs with cloud computing will provide an integrated platform that realizes combination of different WBANs, scalability of data storage, and scalability of power for processing various data analyses [11]. The concept of *Software as a Service*, especially *Security as a Service* (SECaaS) [12] that represents the provision of security applications and services via the cloud platform to the customers' systems, changes the method of protecting body sensors. Through such a cloud-assisted IDS, we are able to detect misbehavior in WBANs and send back the response commands that isolate malicious body sensors. As a result, computation cost is no longer a critical factor influencing the effectiveness of security for body sensors, since security analyses and decisions are performed in the cloud platform.

Different decisions are then emerging along with the application of a cloud-assisted IDS to body sensors. Generally, IDS agents should be initially deployed in body sensors that are referred to as IDS-sensors. After these IDS-sensors have collected other body sensors' events, a problem exists in optimizing their strategies to decide whether to report events involving malicious or normal behavior. Obviously, this problem is caused by limited resources of body sensors. On the one hand, if an IDS-sensor makes a choice not to report any events, it conserves its power and bandwidth, but no malicious body sensors will be captured. However, if an IDS-sensor reports each event it detects, the probability of capturing malicious body sensors will be increased, but the IDS-sensor will run out of its power much faster. To solve this dilemma, we are motivated to employ game theory to seek the optimal strategies.

By supplying a rich set of mathematical tools for exploring the strategic decision-making, game theory has been widely employed in different fields [13–21]. These typical applications exist in optimizing the strategy of launching IDS [22], seeking autonomously stable adaptation decisions [23], minimizing power resource allocation for interference mitigation [24], optimizing service deployment in cloud computing [25], and predicting malicious behavior of attackers [26]. Among various game types, the signaling game is profitable to depict interactions between a body sensor and its corresponding IDS-sensor. In a signaling game, one player called *Sender* has private information about its type set while the other called *Receiver* is public in its type set. Thus, we can relate a body sensor, which attempts to send messages, to *Sender* since it may be normal or malicious so that its type is unknown to IDS-sensors. On the other hand, the corresponding IDS-sensor is related to *Receiver* as it only has one type.

Our interest is then to seek the optimal report strategies for body sensors using a cloud-assisted IDS to save their limited power. We deploy IDS agents to each of the body sensors. However, only those body sensors that are chosen as relays will be triggered to launch. Their responsibility is whether to report monitored events and is not to perform intrusion decisions that are analyzed and processed in the cloud platform for utilizing its powerful capabilities of computation and storage. Thus, we address the issue that a body sensor is too limited in its resources to execute the intrusion detection task that is computationally expensive in general. Using the signaling game, we address the other issue: when should an IDS-sensor report the monitored events? We reflect economic interactions between a body sensor and its corresponding IDS-sensor by constructing an IDS Report Game (IDSRG). We gradually explore the pure- and mixed-strategy BNEs (Bayesian Nash Equilibriums) of the stage IDSRG. As two players play the game continually, we develop the stage IDSRG into a dynamic multistage IDSRG and attain the mixed-strategy PBE (Perfect Bayesian Equilibrium) of the dynamic game. Upon the advantage of PBE, we design an algorithm to guide the IDS-sensor with the optimal report strategy. In this manner, the IDS-sensor is able to prolong its battery life while reporting an acceptable amount of monitored events.

Our contributions are summarized as follows:

(1) We propose a cloud-assisted IDS framework for WBANs, in which intrusion analyses and decisions are performed in the cloud platform. Thus, a body sensor is no longer concerned about its limited computation for realizing its security.

(2) We construct the IDSRG based on the signaling game, which satisfies the actual environment where an IDS-sensor does not know the type of its opponent and is able to properly depict economic interactions between an IDS-sensor and its opponent.

(3) We attain equilibrium theorems of the stage IDSRG as well as the dynamic multistage IDSRG, which disclose the rational behavior of the IDS-sensor and its opponent.

(4) We design a report algorithm based on PBE, which provides an IDS-sensor with the optimal strategy to decide whether to take the action *Report* or not. In other words, an IDS-sensor does not always report monitored events, and thus its energy is saved.

The rest of this paper is organized as follows. In Section 2, we overview related works and highlight our particular aspects. In Section 3, we illustrate our network model and construct the stage and dynamic multistage IDSRG. In Section 4, we present a cloud-assisted IDS framework for WBANs and design a report algorithm based on PBE. In Section 5, we perform experiments to show the characteristics of the dynamic multistage IDSRG. Finally, conclusions are provided in Section 6.

Notations used in this paper are mainly listed in the Notations.

2. Related Work

Integration of cloud computing and WBANs is particularly attractive as it is able to expand the computation paradigm of WBANs. This infrastructure overcomes several shortfalls of WBANs like the storage capacity of data collected by body sensors and the ability to process these data. In spite of the above benefits, their emerging influences could be hindered by various security threats. Body sensors are susceptible to attacks, including node capturing and compromising. Patient's privacy may be lost in the cloud platform or may not

be correctly supervised. For solving these issues, a protocol to attain storage and computation security in cloud computing is proposed in [27]. Zhang et al. [28] presented a key agreement scheme that provides neighboring body sensors with a common key generated by electrocardiogram signals, in order to preserve the integrity and privacy of medical data. The authors in [29] proposed a combined framework for reliable and secure data transmission in WBANs. In addition, the method of establishing trust among body sensors has been regarded as efficient implement to improve the security and performance of WBANs, in which trust evaluation [30] and trust management [31] always should be performed.

Different from the above prevention-based mechanisms to guarantee network security, an IDS, as the second line of defense, is regarded as a detection-based approach that is a necessary tool for realizing security of networks [32]. Typical techniques such as the swarm based rough set [33], Kalman filter [34], support vector machine [35], and unsupervised anomaly detection [36] are applied to IDSs in different networks. Since malicious body sensors usually disrupt the normal operation of WBANs and waste limited resources of normal body sensors, an IDS is required for WBANs to detect malicious body sensors that have broken down the prevention-based mechanisms. Using the IDS, WBANs will be capable of reacting with and isolating intruders to ensure body sensors' normal operation. However, there only exist a few studies of intrusion detection towards WBANs although many intrusion detection studies [37, 38] have been done for Wireless Sensor Networks. In [39], the authors gave a security framework of WBANs for monitoring ambulatory health status. They then proposed an IDS, which is inspired by the biological immune system using the negative selection algorithm, to maintain performance of WBANs in the presence of malicious body sensors. Wu et al. [40] proposed an intrusion-tolerant scheme for WBANs, which is able to dynamically detect intrusions and provide an adaptive strategy with passive replication via the combination of threshold-based intrusion detection and replicas classification. Unfortunately, these works [39, 40] do not consider the computation cost incurred by launching IDS agents. The emergence of cloud computing allows us to tackle this burden by applying its powerful computing ability. Through IDS services, IDS-sensors can transfer the cost of analyzing and processing suspicious data into the cloud platform. Thus, the rest of the problem of IDS-sensors is whether or not to report the monitored events.

Up to now, several works have been concerned about the utilities of employing an IDS via game theory. In [41], Otrok et al. proposed a cooperative game model for catching a misbehaving cluster head through checkers, which can analyze interactions among checkers to decrease the false positive rate. Moreover, a noncooperative zero-sum game between the cluster head and malicious node is formulated to maximize the probability of detection for an elected head. They [42] also conducted a noncooperative game between the intruders and IDS to guide the IDS to select an optimal sampling strategy in order to effectively reduce the success chances of intruders. Zhu et al. [43] combined game-theoretic modeling and trust management to design an intrusion detection network. With a noncooperative N-person continuous-kernel game model, each IDS seeks reciprocal incentive-based optimal resource allocation to maximize the aggregated satisfaction levels of its neighbors. Huang et al. [44] proposed a new IDS called Markovian IDS, which is able to select the optimal defense strategy of misuse detection with noncooperative game theory and to determine the weakest nodes representing potential security risks via a Markov decision process. Zonouz et al. [45] proposed a response and recovery engine based on a two-player Stackelberg stochastic game, which applies attack-response trees to analyze undesired system-level security events and to choose optimal response actions by solving a partially observable competitive Markov decision process. Shamshirband et al. [46] introduced a method called cooperative game-based fuzzy Q-learning to implement cooperative defense counterattack scenarios for the sink node and the base station. Using the signaling game, Shen et al. [22] constructed an intrusion detection game, which is able to depict interactions between the sensor node and IDS agent. The PBE attained is applied to obtain the optimal strategy determining when to launch the IDS agent. Thus, the IDS agent is not always in work and the sensor's power required to detect malicious behavior is saved. They [47] also obtain optimal strategies to save IDS agents' power, through Quantal Response Equilibrium (QRE) that is more realistic than Nash Equilibrium. In addition, Liu et al. [48] investigated the security and dependability mechanism when service providers are facing service attacks of software and hardware and proposed a stochastic evolutionary coalition game (SECG) framework for secure and reliable defenses in Sensor-Cloud.

Our work is distinguished in some aspects compared to the related works above. We adopt an IDS to detect malicious body sensors in WBANs so as to protect patients' privacy. We integrate cloud computing into WBANs to extend body sensors' abilities of computation and storage. Thus, plenty of computation cost incurred by IDS agents can be migrated from body sensors to the cloud platform. We construct an IDSRG in which the game type and corresponding equilibriums are different from [41–44], in order to seek the optimal strategy to decide when to report events monitored by IDS-sensors. The signaling game used in our work properly depicts the actual situation in which an IDS-sensor is uncertain about the type of its opponent. Our work is especially motivated by [22]. However, when analyzing the payoffs of two players, we consider the factors, including the channel reliability, attack success rate, detection rate, and false alarm rate, while only the detection rate and the false alarm rate are considered in [22]. Consequently, we attain the optimal strategies that are more adequate than those in [22].

3. A Report Game for WBANs Using a Cloud-Assisted IDS

3.1. Network Model. In [49], Farooqi and Khan have overviewed that there are three different ways of installing IDS agents in Wireless Sensor Networks. These are purely centralized, purely distributed, and mixed. In the purely centralized mode, an IDS agent is installed in the sink or base station. For realizing this way, an additional special routing protocol that collects information from sensor nodes is required so

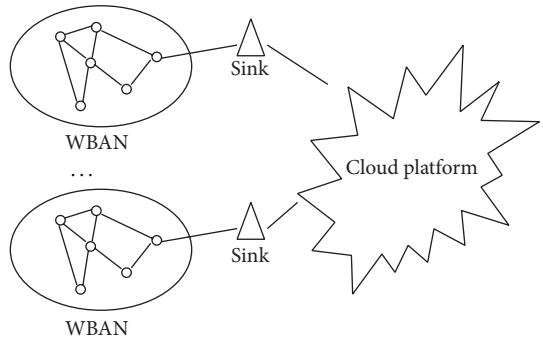

Figure 1: Network model of WBANs using a cloud-assisted IDS.

that the IDS agent can evaluate the behavior of sensor nodes according to the collected information. On the contrary, an IDS agent is installed in every sensor node in the purely distributed mode. It checks the data received in its communication range and declares whether a sensor node is compromised or not. Different from the two modes above, in the mixed mode IDS agents are only installed in monitor sensor nodes that are initially assigned. These monitor sensor nodes not only perform activities like normal sensor nodes but also check for intrusion detection.

To exert the powerful storage and computation capability of cloud computing, we adopt a new hybrid mode to realize a cloud-assisted IDS for WBANs, as depicted in Figure 1. In our mode, we deploy IDS agents in each body sensor, unlike the traditional case that the IDS agent is only installed in monitor sensor nodes. However, not all IDS agents work continuously; only IDS agents residing in body sensors that are selected as relays to forward information will be triggered to launch. Another different aspect is that the IDS agent in our network is only responsible for the monitor task, not including intrusion decisions that are made by the IDS in the cloud platform.

In Figure 1, the IDS-sensor audits data coming from those body sensors that lie inside its radio range or are its neighbors. It produces alert events if any body sensor works abnormally and may report them through the sink to the detection engine that exists in the cloud platform.

Now, a problem that will arise is how to select the optimal report strategy when a cloud-assisted IDS is applied to WBANs. The optimal strategy to be attained should maximize the probability of capturing malicious body sensors but minimize the report cost. To solve this dilemma, we next employ a dynamic multistage signaling game to model interactions between a body sensor and its corresponding IDS agent.

3.2. A Stage IDS Report Game

Definition 1. The stage IDS Report Game (IDSRG) for WBANs using a cloud-assisted IDS is a 5-tuple $(\mathcal{N}, \mathcal{T}, \mathcal{A}, P, \mathcal{U})$, where

(i) $\mathcal{N} = \{\text{Body sensor } S, \text{IDS-sensor } I\}$ is a set of players;

(ii) $\mathcal{T} = \mathcal{T}_S \times \mathcal{T}_I$, where $\mathcal{T}_S = \{\tau_S^0, \tau_S^1\}$ is the type set of player S and $\mathcal{T}_I = \{\tau_I\}$ is the type set of player I;

(iii) $\mathcal{A} = \mathcal{A}_S \times \mathcal{A}_I$, where $\mathcal{A}_S = \{\mathcal{A}_S(\tau_S^0), \mathcal{A}_S(\tau_S^1)\} = \{\{a_{\tau_S^0} \mid Cooperate\}, \{a_{\tau_S^1} \mid Attack, Cooperate\}\}$ is the action set of player S and $\mathcal{A}_I = \{a_I \mid Report, Not\text{-}report\}$ is the action set of player I;

(iv) P: $\mathcal{T} \mapsto [0, 1]$ is a prior probability distribution over types drawn by *Nature* (in game theory, *Nature* randomly chooses a type for each player according to the probability distribution across each player's type space), and $P = (p, 1 - p)$, where p is referred to as the probability of a body sensor being malicious and then $1 - p$ is the probability of a body sensor being normal;

(v) $\mathcal{U} = \{(u_S, u_I)\}$, where u_S: $\mathcal{A} \times \mathcal{T} \mapsto \mathbb{R}$ and u_I: $\mathcal{A} \times \mathcal{T} \mapsto \mathbb{R}$ are the payoff functions of players S and I, respectively.

In the stage IDSRG, we consider there are two players, that is, body sensor S and IDS-sensor I. Body sensor S has private information about its type, which may be normal, denoted by τ_S^0, or malicious, denoted by τ_S^1. That is, the type of body sensor S is unknown to IDS-sensor I. On the contrary, IDS-sensor I has only one regular type denoted by τ_I, and its type information is common knowledge to two players.

At each time slot, each player selects its action from its action space. If body sensor S is normal, it always cooperates. Its action denoted by $a_{\tau_S^0}$ is therefore *Cooperate*. That is, τ_S^0 has one pure strategy: *Cooperate*. On the other hand, if body sensor S is malicious, it may attack for attaining potential profits or cooperate for disguising itself so that the IDS will be misled and is unable to distinguish its maliciousness. Therefore, the action of τ_S^1, denoted by $a_{\tau_S^1}$, may be *Attack* or *Cooperate*. That is, τ_S^1 has two pure strategies: *Attack* and *Cooperate*. For IDS-sensor I, it may report the monitored events that come from body sensors in its radio range or not report these events for saving its energy to prolong its lifetime. Therefore, the action of τ_I, denoted by a_{τ_I}, is either *Report* or *Not-report*. That is, τ_I has two pure strategies: *Report* and *Not-report*.

To express the payoff matrix of the stage IDSRG, we introduce some parameters. A malicious body sensor can select the action *Attack* to waste the limited resources of WBANs and disrupt normal network operations. Such an attack can result in, for example, a failure of communication between two neighbors. The malicious body sensor, however, gets a gain from the attack while it has to pay the cost of consuming power to launch the attack. We therefore present g_A and c_A to denote the attack gain and cost, respectively. When a malicious or normal body sensor selects the action *Cooperate* that means it makes itself available for communication, the packet can be then forwarded successfully through a link including this body sensor. Thus, the normal body sensor benefits from good network operations. In addition, the malicious body sensor gets a gain due to its disguise that helps itself avoid the IDS detection. However, receiving and forwarding packets during the cooperation communication will incur a cost of consuming power. We assume that, for simplicity, both the malicious and normal body sensors get the same gain and pay the same cost when selecting the action

Table 1: Payoff matrix of the stage IDSRG.

(a) Body sensor S is malicious

	Report	*Not-report*
Attack	$(1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A$, $\alpha\lambda g_R - (1-\alpha)\lambda\gamma g_A - c_R$	$\lambda\gamma g_A - c_A$, $-\lambda\gamma g_A$
Cooperate	$\lambda g_C - c_C$, $-\beta\lambda l_F - c_R$	$\lambda g_C - c_C$, 0

(b) Body sensor S is normal

	Report	*Not-report*
Cooperate	$\lambda g_C - c_C$, $-\beta\lambda l_F - c_R$	$\lambda g_C - c_C$, 0

Cooperate. We therefore present g_C and c_C to denote the cooperation gain and cost, respectively. For an IDS-sensor, when it selects the action *Report*, it gets a gain denoted by g_R once the cloud platform detects the malicious body sensor due to its report. At the same time, it suffers a cost c_R from energy consumption used to transmit the monitored events. Moreover, like any general IDS, the IDS service in the cloud platform has false positive rate (i.e., false alarm rate) β, $\beta \in [0,1]$. The existence of false alarms, meaning that body sensors in normal communication are detected in error as malicious ones, will result in a loss l_F to the IDS-sensor due to its report. Besides the false positive rate, there exists the true positive rate (i.e., detection rate) α, $\alpha \in [0,1]$, during the process of intrusion detection. In addition, we introduce λ, $\lambda \in [0,1]$ as the channel reliability reflecting the actual communication environments in a cloud-assisted IDS for WBANs. In addition, we present γ, $\gamma \in [0,1]$, as the attack success rate satisfying the case that a malicious body sensor does not always attack successfully.

We can next analyze various payoffs under different action profiles of two players, which are shown in Table 1. For the action profile $(a_{\tau_S^1} = Attack, a_{\tau_I} = Report)$, in Table 1(a), the payoff of malicious body sensor τ_S^1 is the gain of failing to be detected minus the loss of being detected minus the attack cost, that is, $(1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A$, where $1-\alpha$ is the false negative rate in fact. In contrast, the payoff of IDS-sensor τ_I is the gain of detecting successfully a malicious body sensor minus the loss of failed detection minus the report cost, that is, $\alpha\lambda g_R - (1-\alpha)\lambda\gamma g_A - c_R$. For the action profile $(a_{\tau_S^1} = Attack, a_{\tau_I} = Not\text{-}Report)$, the payoff of τ_S^1 is the attack gain minus the attack cost, that is, $\lambda\gamma g_A - c_A$, while the payoff of τ_I is the loss of being attacked, that is, $-\lambda\gamma g_A$. For the action profile $(a_{\tau_S^1} = Cooperate, a_{\tau_I} = Report)$, the payoff of τ_S^1 is the cooperation gain minus the cooperation cost, that is, $\lambda g_C - c_C$, while the payoff of τ_I is the loss of false alarm minus the report cost, that is, $-\beta\lambda l_F - c_R$. For the action profile $(a_{\tau_S^1} = Cooperate, a_{\tau_I} = Not\text{-}Report)$, the payoff of τ_S^1 is the same as one in the action profile $(a_{\tau_S^1} = Cooperate, a_{\tau_I} = Report)$ while the payoff of τ_I is 0. In Table 1(b), the payoff of normal body sensor τ_S^0 is always $\lambda g_C - c_C$. The payoff of τ_I is $-\beta\lambda l_F - c_R$ if it reports and is 0 if it decides not to report.

3.3. Equilibrium Analyses of the Stage IDSRG. The stage IDSRG belongs to a game of incomplete information, since an IDS-sensor does not know its opponent's type during interactions. We should therefore change it into a complete but imperfect information game through the Harsanyi transformation to attain the corresponding BNE. During the process of the Harsanyi transformation, a virtual player *Nature* is introduced and moves first to choose a type of player S. Thus, the extensive form of the stage IDSRG can be constructed in Figure 2, where p chosen by *Nature* is the probability of a body sensor being malicious.

Theorem 2. *In the stage IDSRG, there exists a probability threshold of a body sensor being malicious, p_0, such that a pure-strategy BNE exists if $p < p_0$.*

Proof.

Case 1. Player S chooses the pure strategy $(a_{\tau_S^1} = Attack, a_{\tau_S^0} = Cooperate)$ meaning that a malicious body sensor always plays the action *Attack* and a normal body sensor always plays the action *Cooperate*.

Under Case 1, the expected payoffs of player I selecting actions *Report* and *Not-report* are

$$E_I(Report) = p(\alpha\lambda g_R - (1-\alpha)\lambda\gamma g_A - c_R) + (1-p)(-\beta\lambda l_F - c_R), \quad (1)$$

$$E_I(Not\text{-}report) = -p\lambda\gamma g_A, \quad (2)$$

respectively. If $E_I(Report) \geq E_I(Not\text{-}report)$, that is,

$$p \geq \frac{(\beta\lambda l_F + c_R)}{(\alpha\lambda g_R + \alpha\lambda\gamma g_A + \beta\lambda l_F)}, \quad (3)$$

then the dominant strategy for player I is *Report*. However, if player I selects the action *Report*, *Attack* will not be the dominant strategy for a malicious body sensor since

$$(1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A < \lambda g_C - c_C \quad (4)$$

is reasonable. Therefore, the pure strategy $(a_{\tau_S^1} = Attack, a_{\tau_S^0} = Cooperate)$ is not a pure-strategy BNE. If $E_I(Report) < E_I(Not\text{-}report)$, that is,

$$p < \frac{(\beta\lambda l_F + c_R)}{(\alpha\lambda g_R + \alpha\lambda\gamma g_A + \beta\lambda l_F)}, \quad (5)$$

then the dominant strategy for player I is *Not-report*. Correspondingly, *Attack* will be the dominant strategy for a malicious body sensor since

$$\lambda\gamma g_A - c_A > (1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A \quad (6)$$

is reasonable. Therefore, the action profile $((a_{\tau_S^1} = Attack, a_{\tau_S^0} = Cooperate), a_I = Not\text{-}report)$ is a pure-strategy BNE.

Case 2. Player S chooses the pure strategy $(a_{\tau_S^1} = Cooperate, a_{\tau_S^0} = Cooperate)$ meaning that it always plays the action *Cooperate* irrespective of its type. For player I, the dominant strategy to response to a normal body sensor's action

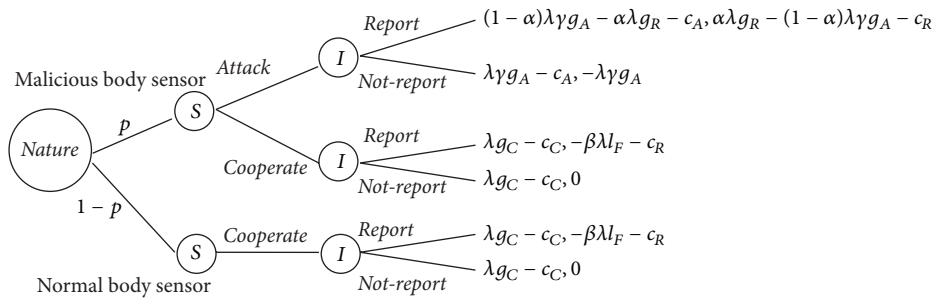

Figure 2: Extensive form of the stage IDSRG.

Cooperate is *Not-report*, whereas for a malicious body sensor, the dominant strategy to response to the action *Not-report* is *Attack*. This leads to a contradictory result. Therefore, there are not any pure-strategy BNEs when player S chooses the pure strategy $(a_{\tau_S^1} = Cooperate, a_{\tau_S^0} = Cooperate)$.

To sum up, a pure-strategy BNE $((a_{\tau_S^1} = Attack, a_{\tau_S^0} = Cooperate), a_I = Not\text{-}report)$ exists if and only if (5) is satisfied. In other words, we can find $p_0 = (\beta\lambda l_F + c_R)/(\alpha\lambda g_R + \alpha\lambda\gamma g_A + \beta\lambda l_F)$ such that a pure-strategy BNE exists if $p < p_0$. □

The pure strategy attained from Theorem 2 means that player S always plays the action *Attack* for a malicious body sensor or *Cooperate* for a normal body sensor while player I always plays the action *Not-report*. This pure strategy is not practical because the equilibrium requires player I to take the action *Not-report* at all times, and hence malicious body sensors will not be captured forever. In fact, the equilibrium attained from Theorem 2 is referred to as Pooling Equilibrium [50] in which player I has no clue about the type of player S. Therefore, it is essential to find a mixed-strategy BNE for capturing malicious body sensors.

Theorem 3. *In the stage IDSRG, there is a mixed-strategy BNE if $p \geq p_0$.*

Proof. From Theorem 2, obviously, the mixed-strategy BNE to be sought exists only if $p \geq p_0$. Let ρ be the probability with which a malicious body sensor plays the action *Attack* and let δ be the probability with which player I plays the action *Report*. We next need to find the optimal values of ρ and δ such that neither player S nor player I can increase the payoff by deviating the mixed-strategy BNE. For the mixed strategy played by player S, the expected payoffs of player I selecting actions *Report* and *Not-report* are

$$\begin{aligned} E_I(Report) &= \rho p\left(\alpha\lambda g_R - (1-\alpha)\lambda\gamma g_A - c_R\right) \\ &\quad + (1-\rho)\, p\left(-\beta\lambda l_F - c_R\right) \\ &\quad + (1-p)\left(-\beta\lambda l_F - c_R\right), \end{aligned} \tag{7}$$

$$E_I(Not\text{-}report) = -\rho p\lambda\gamma g_A, \tag{8}$$

respectively. According to the indifference between actions *Report* and *Not-report* under the optimal mixed strategy played by player I, we get

$$E_I(Report) = E_I(Not\text{-}report). \tag{9}$$

Thus, the optimal probability of a malicious body sensor selecting the action *Attack* is

$$\rho^* = \frac{(\beta\lambda l_F + c_R)}{\left[p\lambda\left(\alpha g_R + \alpha\gamma g_A + \beta l_F\right)\right]}. \tag{10}$$

For the mixed strategy played by player I, the expected payoffs of player S selecting actions *Attack* and *Cooperate* are

$$\begin{aligned} E_S(Attack) &= \delta p\left((1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A\right) \\ &\quad + (1-\delta)\, p\left(\lambda\gamma g_A - c_A\right), \end{aligned} \tag{11}$$

$$\begin{aligned} E_S(Cooperate) &= \delta p\left(\lambda g_C - c_C\right) \\ &\quad + (1-\delta)\, p\left(\lambda g_C - c_C\right) \\ &\quad + \delta(1-p)\left(\lambda g_C - c_C\right) \\ &\quad + (1-\delta)(1-p)\left(\lambda g_C - c_C\right), \end{aligned} \tag{12}$$

respectively. According to the indifference between actions *Attack* and *Cooperate* under the optimal mixed strategy played by player S, we get

$$E_S(Attack) = E_S(Cooperate). \tag{13}$$

Thus, the optimal probability of player I selecting the action *Report* is

$$\delta^* = \frac{\left[p\left(\lambda\gamma g_A - c_A\right) + c_C - \lambda g_C\right]}{\left[p\alpha\lambda\left(\gamma g_A + g_R\right)\right]}. \tag{14}$$

To sum up, given $p \geq p_0$, we can find a mixed-strategy BNE ((*Attack* with ρ^* for τ_S^1, *Cooperate* for τ_S^0), *Report* with δ^* for τ_I) that means a malicious body sensor plays the action *Attack* with probability ρ^* and a normal body sensor always plays the action *Cooperate* while player I plays the action *Report* with probability δ^*. □

Theorems 2 and 3 provide the IDS-sensor with the conditions under which the BNE can be achieved. We can

obtain the probability threshold of a body sensor being malicious, p_0, which is related to the channel reliability λ, cloud-assisted IDS' detection rate α, and false alarm rate β, as well as attack success rate γ. This threshold is extremely low since the gains of actions *Report* and *Attack*, compared to the cost of the action *Report*, are very large as $\lambda, \alpha, \beta, \gamma \in [0, 1]$. However, as the probability of a body sensor being malicious, p, grows and eventually exceeds the threshold, the mixed-strategy BNE suggested in Theorem 3 requires the malicious body sensor to be less offensive in attacking.

The advantage of applying Theorems 2 and 3 is that an IDS-sensor is not always in taking the action *Report*. As a result, the power consumption of the IDS-sensor can be conserved. However, Theorems 2 and 3 are only concerned with a slot time of interactions between an IDS-sensor and its opponent. As two players continually interact with each other, the belief (i.e., probability of a body sensor being malicious), p, which is used to compute the optimal strategy for an IDS-sensor to determine when to select the action *Report*, may be updated dynamically. Therefore, we should develop the stage IDSRG into a dynamic multistage IDSRG to dynamically present the belief of player I on the type of player S.

3.4. Dynamic Multistage IDSRG. Following interactions between players S and I, the stage IDSRG is repeatedly played at each continuous time slot t_k, where $k = 1, 2, \ldots, n$ ($n \in Z^+$). For simplicity, we assume the payoffs of players at the t_kth stage game are the same as those at the t_{k-1}th stage game; that is, there is no discount with respect to the payoffs of players in the dynamic multistage IDSRG. Besides the notations defined in the stage IDSRG, we let $h_S(t_k)$ be the historical actions of player S, let $a_S(t_k)$ be the action adopted by player S at the t_kth stage game, and let $p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$ be the posterior belief meaning the probability of a body sensor being malicious at the end of the t_kth stage IDSRG, respectively. Based on the Bayesian rule, this posterior belief can be constructed at the t_kth stage IDSRG.

Definition 4. The posterior belief hold by player I can be computed by

$$p\left(\tau_S^1 \mid a_S(t_k), h_S(t_k)\right) = \frac{p\left(\tau_S^1 \mid h_S(t_k)\right) p\left(a_S(t_k) \mid \tau_S^1, h_S(t_k)\right)}{\sum_{\widehat{\tau}_S \in \mathcal{T}_S} p\left(\widehat{\tau}_S \mid h_S(t_k)\right) p\left(a_S(t_k) \mid \widehat{\tau}_S, h_S(t_k)\right)}, \tag{15}$$

where, for any $\tau_S \in \{\tau_S^0, \tau_S^1\}$, $p(\tau_S \mid h_S(t_k))$ and $p(a_S(t_k) \mid \tau_S, h_S(t_k))$ denote, with the historical actions of player S, the prior belief hold by player I and the probability of a body sensor selecting action $a_S(t_k)$, respectively.

As described beforehand, the cloud-assisted IDS may inevitably produce detection errors and false alarms. In addition, communicating in WBANs may lose packets. Due to these factors, the actions observed by player I may not always reflect the reality accurately. We integrate these factors into computing the conditional probability $p(a_S(t_k) \mid \tau_S, h_S(t_k))$, $\tau_S \in \{\tau_S^0, \tau_S^1\}$, which can be updated as follows:

$$\begin{aligned} &p\left(Attack \mid \tau_S^1, h_S(t_k)\right) = \alpha\lambda\rho_k + \beta(1 - \lambda\rho_k), \\ &p\left(Cooperate \mid \tau_S^1, h_S(t_k)\right) \\ &\quad = (1 - \alpha)\lambda\rho_k + (1 - \beta)(1 - \lambda\rho_k), \\ &p\left(Attack \mid \tau_S^0, h_S(t_k)\right) = \beta, \\ &p\left(Cooperate \mid \tau_S^0, h_S(t_k)\right) = 1 - \beta, \end{aligned} \tag{16}$$

where $1 - \alpha$, $1 - \lambda$, $1 - \beta$, and ρ_k denote the false negative rate, the channel unreliability, the true negative rate, and the probability of player S selecting the action *Attack* at the t_kth stage IDSRG, respectively.

So far, a belief system based on (15)-(16) has been presented to describe the belief building and updating process. It is easy to see that each belief to be updated is dependent on a body sensor's action player I observes at the current stage IDSRG and the prior belief it holds. With the belief system, we can define the dynamic multistage IDSRG as follows.

Definition 5. The dynamic multistage IDSRG is a 5-tuple $(\mathcal{N}, \mathcal{T}, \mathcal{A}, \mathcal{U}, P(t_k))$, where

(i) $\mathcal{N}$, $\mathcal{T}$, $\mathcal{A}$, and $\mathcal{U}$ are the same as those defined in Definition 1;

(ii) $P(t_k) = (p(\tau_S^1 \mid h_S(t_k)), 1 - p(\tau_S^1 \mid h_S(t_k)))$, where $p(\tau_S^1 \mid h_S(t_k))$ denotes the probability of a body sensor being malicious with the historical actions $h_S(t_k)$ at the t_kth stage IDSRG, and it will be updated by $p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$ computed by (15) at the end of the t_kth stage IDSRG.

For the dynamic multistage IDSRG, Perfect Bayesian Equilibrium (PBE) can be applied to seek the optimal strategies of two players. This is because the dynamic multistage IDSRG is essentially regarded as a dynamic Bayesian game. With the aforementioned belief system, the dynamic multistage IDSRG is played in a sequential manner. Players S and I will not always select the same strategies at each stage game to attain the most expected payoffs. Their best response strategies are related to the current belief that may be changed as the dynamic multistage IDSRG evolves. This relation can be disclosed by the concept of PBE. We next illustrate that the dynamic multistage IDSRG satisfies the Bayesian conditions, which guarantee that an incomplete information game has a PBE.

Lemma 6. *The dynamic multistage IDSRG satisfies the following Bayesian conditions B(i)–B(iv) referred to in [50]:*

B(i): *the posterior beliefs are independent, and all types of player I have the same beliefs.*

B(ii): *the Bayesian rule is used to update beliefs from* $p(\tau_S \mid h_S(t_k))$ *to* $p(\tau_S \mid h_S(t_{k+1}))$ *for any* $\tau_S \in \{\tau_S^0, \tau_S^1\}$.

B(iii): *the players do not signal what they do not know.*

B(iv): *the posterior beliefs are consistent with a common joint distribution on* $\mathcal{T}$ *given* $h_S(t_k)$.

Proof. B(i) is satisfied because player I has only one type. B(ii) is satisfied because the beliefs updated in the belief system are derived from the Bayesian rule. B(iii) means $p(\tau_S^1 \mid a_S(t_k), h_S(t_k)) = p(\tau_S^1 \mid \widehat{a}_S(t_k), h_S(t_k))$ if $a_S(t_k) = \widehat{a}_S(t_k)$, which is satisfied because the signals of player S are the part of actions in the context of the dynamic multistage IDSRG. B(iv) is satisfied because only players S and I are in any stage game where no other players affect the beliefs updated by player I on its opponent. □

Theorem 7. *There is a mixed-strategy PBE in the dynamic multistage IDSRG.*

Proof. At the t_kth stage IDSRG, let ρ_k and δ_k denote the probabilities of a body sensor selecting the action *Attack* and the corresponding IDS-sensor selecting the action *Report*, respectively. For player I at the t_kth stage IDSRG, the expected payoffs of selecting actions *Report* and *Not-report* at the t_kth stage game are

$$\begin{aligned} &E_I^{t_k}(Report) \\ &= \rho_k p\left(\tau_S^1 \mid h_S(t_k)\right)\left(\alpha\lambda g_R - (1-\alpha)\lambda\gamma g_A - c_R\right) \\ &\quad + (1-\rho_k)\, p\left(\tau_S^1 \mid h_S(t_k)\right)\left(-\beta\lambda l_F - c_R\right) \\ &\quad + \left(1 - p\left(\tau_S^1 \mid h_S(t_k)\right)\right)\left(-\beta\lambda l_F - c_R\right), \end{aligned} \tag{17}$$

$$E_I^{t_k}(Not\text{-}report) = -\rho_k p\left(\tau_S^1 \mid h_S(t_k)\right)\lambda\gamma g_A, \tag{18}$$

respectively. According to the indifference between actions *Report* and *Not-report* under the optimal mixed strategy played by player I at the t_kth stage IDSRG, we get

$$E_I^{t_k}(Report) = E_I^{t_k}(Not\text{-}report). \tag{19}$$

Thus, the optimal probability of a malicious body sensor selecting the action *Attack* is

$$\rho_k^* = \frac{(\beta\lambda l_F + c_R)}{\left[p\left(\tau_S^1 \mid h_S(t_k)\right)\lambda\left(\alpha g_R + \alpha\gamma g_A + \beta l_F\right)\right]}. \tag{20}$$

For a body sensor at the t_kth stage IDSRG, the expected payoffs of selecting actions *Attack* and *Cooperate* are

$$\begin{aligned} &E_S^{t_k}(Attack) \\ &= \delta_k p\left(\tau_S^1 \mid h_S(t_k)\right)\left((1-\alpha)\lambda\gamma g_A - \alpha\lambda g_R - c_A\right) \\ &\quad + (1-\delta_k)\, p\left(\tau_S^1 \mid h_S(t_k)\right)\left(\lambda\gamma g_A - c_A\right), \end{aligned} \tag{21}$$

$$\begin{aligned} &E_S^{t_k}(Cooperate) \\ &= \delta_k p\left(\tau_S^1 \mid h_S(t_k)\right)\left(\lambda g_C - c_C\right) \\ &\quad + (1-\delta_k)\, p\left(\tau_S^1 \mid h_S(t_k)\right)\left(\lambda g_C - c_C\right) \\ &\quad + \delta_k\left(1 - p\left(\tau_S^1 \mid h_S(t_k)\right)\right)\left(\lambda g_C - c_C\right) \\ &\quad + (1-\delta_k)\left(1 - p\left(\tau_S^1 \mid h_S(t_k)\right)\right)\left(\lambda g_C - c_C\right), \end{aligned} \tag{22}$$

respectively. According to the indifference between actions *Attack* and *Cooperate* under the optimal mixed strategy played by player S at the t_kth stage IDSRG, we get

$$E_S^{t_k}(Attack) = E_S^{t_k}(Cooperate). \tag{23}$$

Thus, the optimal probability of player I selecting the action *Report* is

$$\delta_k^* = \frac{\left[p\left(\tau_S^1 \mid h_S(t_k)\right)\left(\lambda\gamma g_A - c_A\right) + c_C - \lambda g_C\right]}{\left[p\left(\tau_S^1 \mid h_S(t_k)\right)\alpha\lambda\left(\gamma g_A + g_R\right)\right]}. \tag{24}$$

To sum up, there is a mixed-strategy PBE that can be attained with the strategy profile ((*Attack* with ρ_k^* for τ_S^1, *Cooperate* for τ_S^0), *Report* with δ_k^* for τ_I) at the t_kth stage IDSRG. □

From Theorem 7, the two rational players S and I at the t_kth stage IDSRG will play with the strategy profile shown in Theorem 7. This strategy profile exhibits the so-called sequential rationality in game theory [50], which means each player's strategy is optimal whenever it has to be changed, given the belief and each other's actions. The PBE makes the IDS-sensor not always report its opponent's events while minimizing the possible damage caused by an undetected malicious body sensor. Energy that is potentially consumed by the IDS-sensor to continuously report the monitored events is therefore saved.

4. Applying PBE-Based Report Strategies to WBANs Using a Cloud-Assisted IDS

To facilitate the advantage of the above PBE, we propose and design a framework of applying IDSRG to WBANs using a cloud-assisted IDS, as illustrated in Figure 3. The framework consists of three entities: body sensor S, IDS-sensor I, and *cloud platform*. Body sensor S may be normal or malicious; it therefore signals the action *Cooperate* or *Attack* that forms *Monitored Events*. As the opponent of body sensor S, IDS-sensor I captures those *Monitored Events* and decides whether to report them to *cloud platform* through the sink. Once *cloud platform* receives the *Reported Events*, the IDS will be immediately triggered as a service and then examine the obtained record. Finally, according to alerts produced by the IDS *Administrator* may send *Control Data* to deal with a malicious body sensor.

The heart of the framework is PBE calculation whose results indict IDS-sensor I with the probability of selecting the action *Report*. This calculation starts with *Monitored Events* captured by IDS-sensor I. *Administrator* first configures the IDS agent in IDS-sensor I with *Configuration Data* for making it more reliable and accurate. He/she also defines the game parameters required, including α, β, γ, λ, g_A, g_R, g_C, c_A, c_C, c_R, l_F, and $p(\tau_S^1 \mid h_S(t_k))$. Upon these game parameters, a stage IDSRG is built up and the payoff matrix is correspondingly formulated. With the signal included in *Monitored Events* and the stage IDSRG, the IDS agent computes the probability of selecting the action *Report*, δ_k^*, according to (24). It also, according to (15), computes the

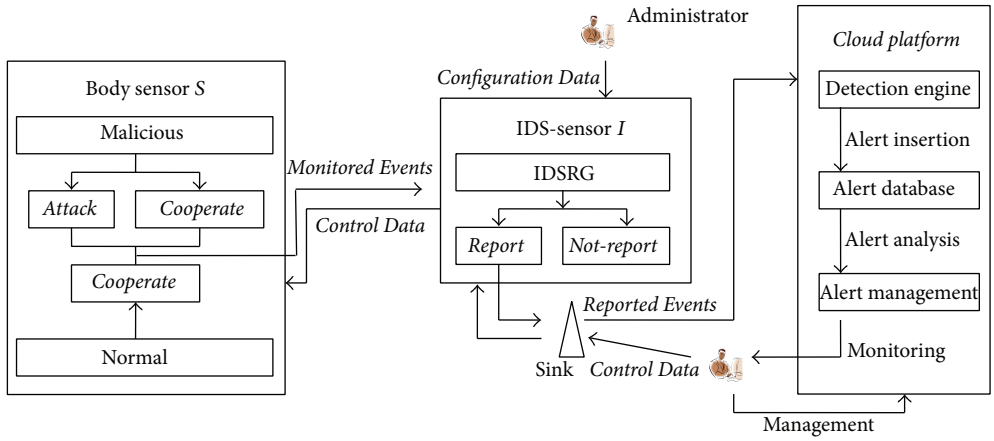

Figure 3: Framework of applying IDSRG to WBANs using a cloud-assisted IDS.

posterior belief $p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$ that is used to update $p(\tau_S^1 \mid h_S(t_k))$ for the next stage IDSRG. The process above will then be repeatedly done until the end of interactions between players S and I. The algorithm describing the PBE-based strategy to decide whether to report *Monitored Events* is given as Algorithm 1.

The other important part of the framework is the IDS in *cloud platform*. It consists of three main components: *Detection Engine*, *Alert Database*, and *Alert Management*. *Detection Engine* is the core component of the IDS, which decides whether an event sent from IDS-sensors through the sink is normal or abnormal. It may combine two of well-known detection techniques, including misuse and anomaly-based detection. It may compare the event to a predefined rule set or perform the process of multipattern matching. Upon completion, it distinguishes the event as normal or abnormal one and inserts the generated alerts into *Alert Database*. As a storage unit to maintain all the formatted events created by *Detection Engine*, *Alert Database* stores body sensor ID, the timestamp of various events, and packet information with the defined signatures. Some alert groups and statistics produced by *Alert Management* are also contained in *Alert Database*. Depending on *Alert Analysis*, *Alert Management* is applied to observe the generated alerts and relate them to previously defined attacking cases. This tool provides *Administrator* with a function to extract events and to produce reports based on source, time, and types of attacks. Finally, *Administrator* examines these findings and decides whether to send *Control Data* to those malicious body sensors.

5. Experiments

In this section, we employ MATLAB R2010a to illustrate the characteristics of the dynamic multistage IDSRG. Since we are the first to study the report game in WBANs using a cloud-assisted IDS, we do not compare our work with any prior work. Here, we explore the factors influencing a malicious body sensor to select the action *Attack*, in order to disclose its optimal attack strategies. We further, through an IDS-sensor's posterior belief computed by Algorithm 1, evaluate the performance of our proposed framework with the probability of a body sensor being malicious in terms of IDSRG parameters at the t_kth stage game.

5.1. Analyses on Optimal Attack Probabilities. We show the changeable trend of the optimal probability of a malicious body sensor selecting the action *Attack* in terms of α, β, and γ, in order to disclose the intension of a malicious body sensor. The rates of higher detection and lower false alarm make a cloud-assisted IDS easy to capture the malicious body sensors. Therefore, the optimal strategy of a malicious body sensor is to reduce the probability of selecting the action *Attack* to avoid the captured loss. On the other hand, the higher attack success rate helps a malicious body sensor attain its expected payoff more quickly. As the case we expect, the optimal probability of a malicious body sensor selecting the action *Attack*, from Figure 4, slowly decreases when the detection rate gradually increases from 0.5 to 1. A similar tendency is shown as the false alarm rate decreases from 0.1 to 0. In Figures 5 and 6, the decrement of the optimal attack probability selected by a malicious body sensor is followed with the increments of the attack success rate, detection rate, and false alarm rate. Further, the influence of the attack success rate is lower than that of the other two factors. When $\alpha = 0.9$ in Figure 5, for example, the optimal attack probability decreases from 0.1547 to 0.1239 as γ changes from 0.6 to 1. It reduces by 19.91% or so. However, when $\gamma = 0.92$, the optimal attack probability decreases from 0.2316 to 0.1162, producing 49.83% or so decrements. These results indicate we should improve the detection rate and reduce the false alarm rate for lowering the attack probability of a malicious body sensor.

5.2. Performance Analyses. At the t_kth stage IDSRG, an IDS-sensor updates its belief on the type of its opponent using (15). Without loss of generality, we assume the initial belief of each IDS-sensor is 0.5. That is, the probability of a body sensor being malicious is the same as that of a body sensor being normal. Figure 7 demonstrates the convergence of an IDS-sensor's posterior belief when different detection rates are presented. We see that the higher the detection rate is, the quicker the posterior belief converges to 1. The convergence requires about 12 times of playing the stage IDSRG if $\alpha = 0.9$,

(1) $k \leftarrow 1$;
(2) Initialize game parameters α, β, γ, λ, g_A, g_R, g_C, c_A, c_C, c_R, l_F, and $p(\tau_S^1 \mid h_S(t_k))$;
(3) Select the action *Not-report*;
(4) Do UNTIL the end of interactions between an IDS-sensor and its opponent
(5) Waked by Monitored Events;
(6) IF the IDSRG is not existed
(7) Construct a game;
(8) ELSE
(9) Get the stored game;
(10) ENDIF
(11) Compute δ_k^* according to (24);
(12) Compute $p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$ according to (15);
(13) Update $p(\tau_S^1 \mid h_S(t_k))$ with $p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$ and store it;
(14) Select the action *Report* with probability δ_k^*;
(15) $k \leftarrow k + 1$;
(16) ENDDO

Algorithm 1: PBE-based report algorithm for an IDS-sensor.

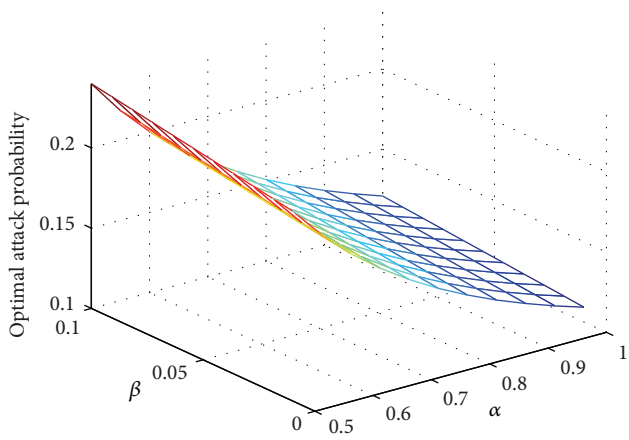

Figure 4: Optimal attack probabilities in terms of α and β.

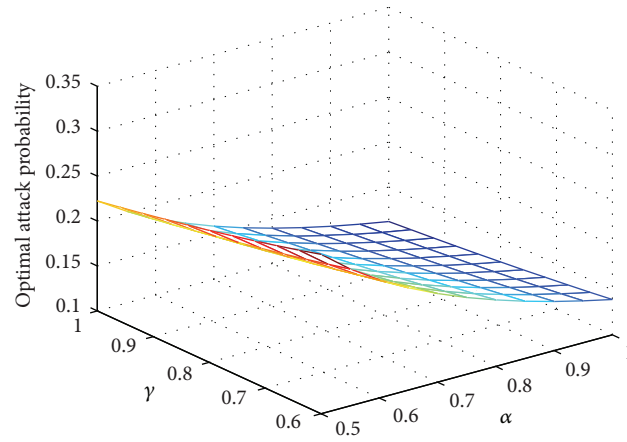

Figure 5: Optimal attack probabilities in terms of α and γ.

15 times if $\alpha = 0.7$, and 20 times if $\alpha = 0.5$, respectively. When different false alarm rates are considered in Figure 8, we see that the lower the false alarm rate is, the quicker the posterior belief converges to 1. It requires about 6 times of playing the stage IDSRG if $\beta = 0.01$, 11 times if $\beta = 0.05$, and 21 times if $\beta = 0.1$, respectively. From Figures 7 and 8, the convergence speed of an IDS-sensor's posterior belief increases as the detection rate goes up and the false alarm rate goes down. That is, the speed to judge whether a body sensor is malicious depends on the detection accuracy of the cloud-assisted IDS.

Figure 9 compares the convergence of an IDS-sensor's posterior belief when different actual-attack-gains denoted by g_A/c_A are given. We see that the lower the actual-attain-gain is, the quicker the posterior belief converges to 1. This phenomenon may be explained as follows. With a smaller actual-attack-gain, a malicious body sensor must take the action *Attack* more frequently to get its expected payoff. This increasing frequency raises the probability that the IDS-sensor successfully observes the action *Attack* launched by the malicious body sensor. Thus, the posterior belief is updated more successfully and converges to 1 more quickly.

In Figure 10, we let g_R/c_R be the actual-report-gain. It shows that a smaller actual-report-gain leads the belief system to converge to 1 more quickly. This is because the IDS-sensor should report more often to attain its expected payoff. Thus, quicker convergence of the posterior belief is achieved, leading to quicker detection of a malicious body sensor.

In what follows, we analyze how the historical actions taken by a malicious body sensor influence the convergence speed of the posterior belief, as shown in Figure 11. We assume two observation sequences: [0 0 0 0 0 1 1 1 1 1 0 0 1 0 1 0 1 1 1 0 0 0 0 0 0] and [1 1 1 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0], where 1 represents the action *Attack* and 0 represents the action *Cooperate* in the corresponding stage IDSRG. If 1 or 0 is continuous, then the malicious body sensor takes the action *Attack* or *Cooperate* repeatedly. The other important parameter considered in Figure 11 is $\alpha = 0.9$, which means a higher detection rate. We see the posterior belief converges

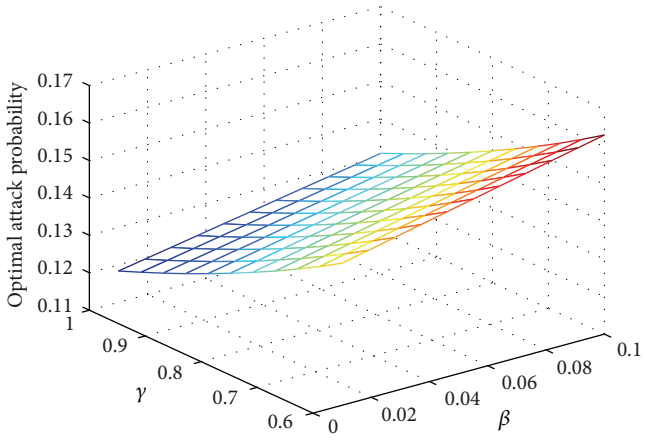

Figure 6: Optimal attack probabilities in terms of β and γ.

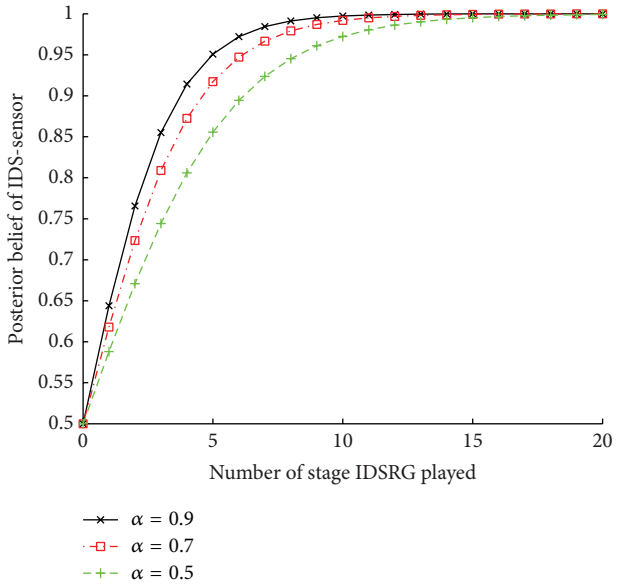

Figure 7: Probability of successfully detecting a malicious body sensor under different detection rates.

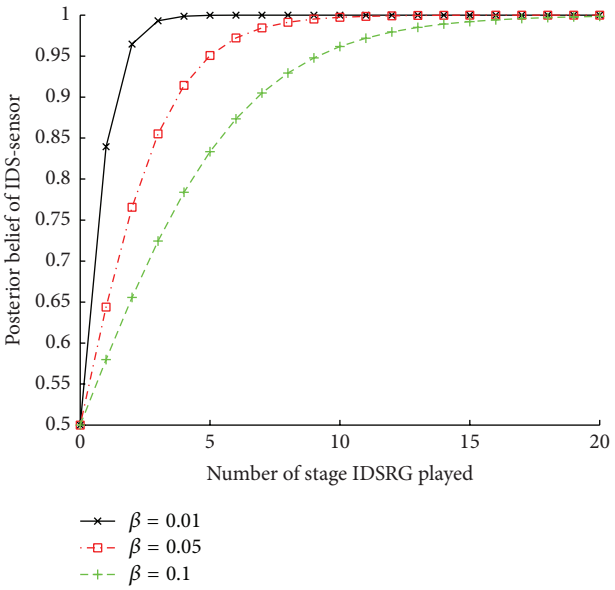

Figure 8: Probability of successfully detecting a malicious body sensor under different false alarm rates.

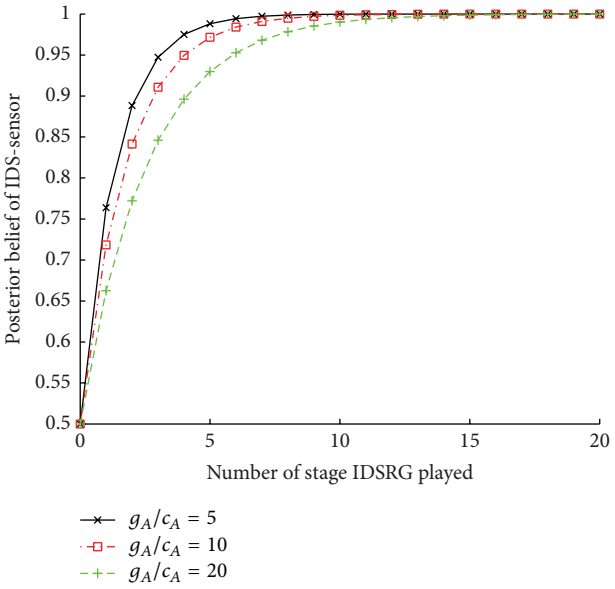

Figure 9: Probability of successfully detecting a malicious body sensor under different actual-attack-gains.

to 1 quickly when a malicious body sensor takes continuous action *Attack*. Once the IDS-sensor considers a body sensor to be malicious, the posterior belief cannot be decreased adaptively to a lower value even if the IDS-sensor observes the action *Cooperate* taken by the malicious body sensor. This means that the IDS-sensor has to always take the action *Report* and consume its energy rapidly. To avoid this case, IDS agents in IDS-sensors should initially deploy an association-rule module that can reset the posterior belief.

6. Conclusion

We have presented an IDS framework with the help of cloud computing, in order to quest for security of WBANs. It extends WBANs to an integrated platform that offers scalability of data storage and computation for launching an IDS. With this framework, IDS-sensors are only responsible for whether or not to report the monitored events, not for performing the costly task of intrusion detection. Thus, the deficiency of limited resources in WBANs is no longer a problem to guarantee security of WBANs. Moreover, to solve the IDS-sensors' dilemma between saving energy and reporting the monitored events to increase the probability of capturing the malicious body sensor, we have proposed a dynamic multistage IDSRG using the signaling game. Our game is able to depict interactions between a malicious/normal body sensor and its opponent IDS-sensor and is able to reflect their payoffs. We have proven that the stage IDSRG has a pure-strategy BNE or mixed-strategy BNE under different conditions of the probability of a body sensor being malicious.

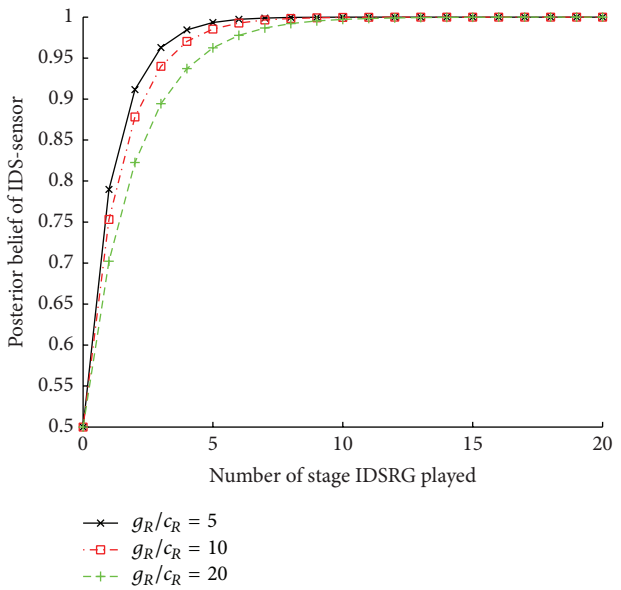

Figure 10: Probability of successfully detecting a malicious body sensor under different actual-report-gains.

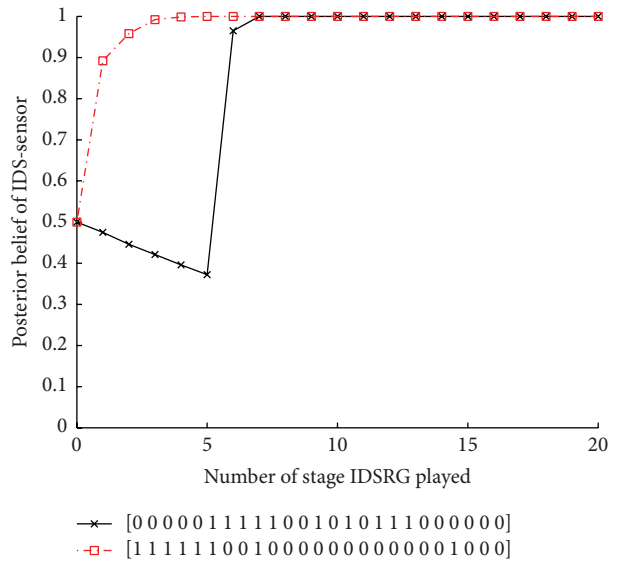

Figure 11: Probability of successfully detecting a malicious body sensor under historical actions.

As the game evolves, we have extended the stage IDSRG to a dynamic multistage IDSRG, where the belief hold by IDS-sensors can be updated rationally and dynamically according to the current and historical actions of malicious body sensors. We have also proven the existence of the mixed-strategy PBE in the dynamic IDSRG. This mixed-strategy PBE helps IDS-sensors select an optimal strategy that will prolong their lifespan while allowing them to report an acceptable amount of monitored events. A report strategy algorithm is designed to implement the mixed-strategy PBE. Experiments have shown, based on the optimal report strategies computed by the proposed algorithm, that the type and optimal strategy of a malicious body sensor can be predicted. Thus, body sensors are capable of saving their energy while the cloud-assisted IDS is able to actively defend malicious body sensors.

While the proposed approach works in principle, we plan to implement it by developing a cloud-assisted IDS testbed via Castalia 3.2, a simulator based on OMNeT++ 4.3.1. Depending on the future experiment results, a more accurate IDSRG to further enhance its decision-making capability in order to prevent body sensors from malicious attacks maybe will be attained.

Notations

S: Body sensor that is normal or malicious, namely, player S
I: Body sensor that involves an IDS agent and is chosen as a relay, namely, IDS-sensor (player I)
τ_S^0: One type of player S; a body sensor belonging to this type is normal
τ_S^1: One type of player S; a body sensor belonging to this type is malicious
$\mathcal{T}_S$: Type set of player S
τ_I: Type of player I
$\mathcal{T}_I$: Type set of player I
$a_{\tau_S^0}$: Action taken by a normal body sensor
$a_{\tau_S^1}$: Action taken by a malicious body sensor
$\mathcal{A}_S(\tau_S^0)$: Action space of a normal body sensor
$\mathcal{A}_S(\tau_S^1)$: Action space of a malicious body sensor
a_I: Action taken by an IDS-sensor
$\mathcal{A}_I$: Action space of an IDS-sensor
p: Probability of a body sensor being malicious
g_A: Attack gain of a malicious body sensor
c_A: Attack cost for a malicious body sensor
g_C: Cooperation gain of a malicious/normal body sensor
c_C: Cooperation cost for a malicious/normal body sensor
g_R: Report gain of an IDS-sensor
c_R: Report cost for an IDS-sensor
l_F: False alarm loss of an IDS-sensor
α: Detection rate of the IDS residing in the cloud platform
β: False alarm rate of the IDS residing in the cloud platform
γ: Attack success rate
λ: Channel reliability
ρ: Probability of a malicious body sensor selecting the action *Attack*
ρ^*: Optimal probability of a malicious body sensor selecting the action *Attack*
δ: Probability of an IDS-sensor selecting the action *Report*

δ^*: Optimal probability of an IDS-sensor selecting the action *Report*

$h_S(t_k)$: Historical actions adopted by a body sensor before the t_kth stage IDSRG

$a_S(t_k)$: Action adopted by a body sensor at the t_kth stage IDSRG

$p(\tau_S^1 \mid a_S(t_k), h_S(t_k))$: Posterior belief meaning the probability of a body sensor being malicious at the end of the t_kth stage IDSRG

$p(a_S(t_k) \mid \tau_S, h_S(t_k))$: Probability of a body sensor selecting action $a_S(t_k)$ at the t_kth stage IDSRG

ρ_k: Probability of a malicious body sensor selecting the action *Attack* at the t_kth stage IDSRG

ρ_k^*: Optimal probability of a malicious body sensor selecting the action *Attack* at the t_kth stage IDSRG

δ_k: Probability of an IDS-sensor selecting the action *Report* at the t_kth stage IDSRG

δ_k^*: Optimal probability of an IDS-sensor selecting the action *Report* at the t_kth stage IDSRG.

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 the 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 Grant no. 20145021.

References

[1] M. Chen, S. Gonzalez, A. V. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: a survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, 2011.

[2] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[3] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of IEEE 802.15.6 MAC, PHY, and security specifications," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 950704, 12 pages, 2013.

[4] W.-T. Sung and K.-Y. Chang, "Health parameter monitoring via a novel wireless system," *Applied Soft Computing*, vol. 22, pp. 667–680, 2014.

[5] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. Vasilakos, "Securing m-healthcare social networks: challenges, countermeasures and future directions," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 12–21, 2013.

[6] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[7] S. Saleem, S. Ullah, and K. S. Kwak, "A study of IEEE 802.15.4 security framework for wireless body area networks," *Sensors*, vol. 11, no. 2, pp. 1383–1395, 2011.

[8] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2193–2204, 2014.

[9] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 843–859, 2013.

[10] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1299–1314, 2015.

[11] G. Fortino, M. Pathan, and G. Di Fatta, "BodyCloud: integration of cloud computing and body sensor networks," in *Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '12)*, pp. 851–856, Taipei, Taiwan, December 2012.

[12] V. Getov, "Security as a service in smart clouds—opportunities and concerns," in *Proceedings of the 36th IEEE Annual International Computer Software and Applications Conference (COMPSAC '12)*, pp. 373–379, Izmir, Turkey, July 2012.

[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] S. Moretti and A. V. Vasilakos, "An overview of recent applications of game theory to bioinformatics," *Information Sciences*, vol. 180, no. 22, pp. 4312–4322, 2010.

[15] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012.

[16] 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.

[17] 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, 2013.

[18] L. D. H. Sampaio, T. Abrão, B. A. Angélico, M. F. Lima, M. L. Proença Jr., and P. J. E. Jeszensky, "Hybrid heuristic-waterfilling game theory approach in MC-CDMA resource allocation," *Applied Soft Computing*, vol. 12, no. 7, pp. 1902–1912, 2012.

[19] 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.

[20] 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.

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

[22] 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.

[23] P. Champrasert, J. Suzuki, and C. Lee, "Exploring self-optimization and self-stabilization properties in bio-inspired autonomic cloud applications," *Concurrency Computation Practice and Experience*, vol. 24, no. 9, pp. 1015–1034, 2012.

[24] D. López-Pérez, X. Chu, A. V. Vasilakos, and H. Claussen, "Power minimization based resource allocation for interference mitigation in OFDMA femtocell networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 2, pp. 333–344, 2014.

[25] H. Wada, J. Suzuki, Y. Yamano, and K. Oba, "Evolutionary deployment optimization for service-oriented clouds," *Software—Practice and Experience*, vol. 41, no. 5, pp. 469–493, 2011.

[26] 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.

[27] L. Wei, H. Zhu, Z. Cao et al., "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371–386, 2014.

[28] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[29] S. K. S. Raja and T. Jebarajan, "Reliable and secured data transmission in wireless body area networks (WBAN)," *European Journal of Scientific Research*, vol. 82, no. 2, pp. 173–184, 2012.

[30] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1164–1175, 2012.

[31] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[32] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: taxonomy, solutions and open issues," *Information Sciences*, vol. 239, pp. 201–225, 2013.

[33] Y. Y. Chung and N. Wahid, "A hybrid network intrusion detection system using simplified swarm optimization (SSO)," *Applied Soft Computing*, vol. 12, no. 9, pp. 3014–3022, 2012.

[34] 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.

[35] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," *Applied Soft Computing*, vol. 18, pp. 178–184, 2014.

[36] J. Song, H. Takakura, Y. Okabe, and K. Nakao, "Toward a more practical unsupervised anomaly detection system," *Information Sciences*, vol. 231, pp. 4–14, 2013.

[37] 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.

[38] M. A. Rassam, M. A. Maarof, and A. Zainal, "A survey of intrusion detection schemes in Wireless Sensor Networks," *American Journal of Applied Sciences*, vol. 9, no. 10, pp. 1636–1652, 2012.

[39] T. V. P. Sundararajan and A. Shanmugam, "A novel intrusion detection system for wireless body area network in health care monitoring," *Journal of Computer Science*, vol. 6, no. 11, pp. 1355–1361, 2010.

[40] G. Wu, J. Ren, L. Yao, and Z. Xu, "ITFBS: adaptive intrusion-tolerant scheme for body sensor networks in smart space applications," *IET Communications*, vol. 5, no. 17, pp. 2509–2517, 2011.

[41] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications*, vol. 31, no. 4, pp. 708–721, 2008.

[42] H. Otrok, M. Mehrandish, C. Assi, M. Debbabi, and P. Bhattacharya, "Game theoretic models for detecting network intrusions," *Computer Communications*, vol. 31, no. 10, pp. 1934–1944, 2008.

[43] Q. Zhu, C. Fung, R. Boutaba, and T. Başar, "GUIDEX: a game-theoretic incentive-based mechanism for intrusion detection networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 11, pp. 2220–2230, 2012.

[44] 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*, vol. 231, pp. 32–44, 2013.

[45] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: a game-theoretic intrusion response and recovery engine," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406, 2014.

[46] 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.

[47] S. Shen, K. Hu, L. Huang, H. Li, R. Han, and Q. Cao, "Quantal response equilibrium-based strategies for intrusion detection in WSNs," *Mobile Information Systems*, vol. 2015, Article ID 179839, 10 pages, 2015.

[48] 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.

[49] 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.

[50] D. Fudenberg and J. Tirole, *Game Theory*, The MIT Press, London, UK, 1991.