Bayesian Rules Based Optimal Defense Strategies for Clustered WSNs

Weiwei Zhou[1*], Bin Yu[1]
[1] Zhengzhou Institute of Information Science and Technology
Zhengzhou - CHINA
[e-mail: zww15238060801@163.com; 13083602007@163.com]
*Corresponding author: Weiwei Zhou

Received August 16, 2017; revised March 7, 2018; accepted May 25, 2018; published December 31, 2018

Abstract

Considering the topology of hierarchical tree structure, each cluster in WSNs is faced with various attacks launched by malicious nodes, which include network eavesdropping, channel interference and data tampering. The existing intrusion detection algorithm does not take into consideration the resource constraints of cluster heads and sensor nodes. Due to application requirements, sensor nodes in WSNs are deployed with approximately uncorrelated security weights. In our study, a novel and versatile intrusion detection system (IDS) for the optimal defense strategy is primarily introduced. Given the flexibility that wireless communication provides, it is unreasonable to expect malicious nodes will demonstrate a fixed behavior over time. Instead, malicious nodes can dynamically update the attack strategy in response to the IDS in each game stage. Thus, a multi-stage intrusion detection game (MIDG) based on Bayesian rules is proposed. In order to formulate the solution of MIDG, an in-depth analysis on the Bayesian equilibrium is performed iteratively. Depending on the MIDG theoretical analysis, the optimal behaviors of rational attackers and defenders are derived and calculated accurately. The numerical experimental results validate the effectiveness and robustness of the proposed scheme.

Keywords: wireless sensor networks (WSNs); multi-stage intrusion detection game (MIDG); intrusion detection system (IDS); posterior probability; Bayesian equilibrium

1. Introduction

With the characteristics of high redundancy, low power consumption, self-organization and fast deployment, wireless sensor networks (WSNs) have broad application prospects in various fields such as battlefield environment reconnaissance, target tracking, and situational awareness, etc [1]. However, today's advanced mobile computing and wireless communication technology, combined with the complexity of open and bandwidth-constrained channels, increases significantly the security risk by making the data monitoring and intrusion detection more and more challenging than before. Consequently, WSNs are becoming much more vulnerable to various threats, which include MAC flooding, nodes replication, and replay attack, etc [2].

As a distributed and heterogeneous computing network, WSNs have been extensively explored in many countries. The perimeter security is an important guarantee to ensure the internal data security and the topology integrity, which provides the theoretical basis for the applications of WSNs in high security fields [3]. Generally, the perimeter security mechanisms in WSNs can be divided into two main families: Prior defense mechanism (PDM) and ex-post detection mechanism (EDM) [4]. PDM refers to relative cryptographic algorithms, verification codes and signature algorithms to ensure the confidentiality, completeness, availability, controllability and non-repudiation in the data processing [5]. To the contrary, EDM detects and restrains the invasion through intrusion detection technology. As a whole, prior defense is the first line of defense for the network security. When the malicious nodes decipher the internal key and cryptographic algorithm through node replication or capture, PDM in WSNs will be invalid immediately [6]. Even worse, malicious nodes can intercept the crucial information transmitted to other sensor nodes. Sustained attack can exhaust the network resource promptly and therefore severely threats the network security. Thus, the intrusion detection mechanism (IDM) should be widely deployed as a complementary line of defense to the high-reliability security approaches aiming at eliminating the underlying threats [7]. Since the perimeter security of WSNs is equal to "the detection and suppression of illegal behaviors", many researchers pay much attention to the abnormal detection and misuse detection in recent years, which belong to the classical IDM [8]. By means of the detecting and filtering function in IDM, the system can check and quarantine the illegal behaviors to guarantee the perimeter security in WSNs [9].

The existing intrusion detection methods are principally based on the assumptions that sensor nodes' resource is relatively sufficient and security weights possessed by sensor nodes are identical [10]. However, sensor nodes usually have different security levels or possess different security weights depending on the information they possess. Thus, the proposed IDS schemes cannot be adopted directly in WSNs [11]. It is seriously urgent to design an intrusion detection scheme to take into consideration both the security weights and the resource constraints [12]. As a mathematical method to formulate the solution of the participants under the assumptions, game theory provides a possible way to analyze the optimal defense strategy for the IDS. The intrusion detection game is divided into different stages in WSNs. Depending on the behaviors of external node and parameter settings in previous stage, IDS can infer and modify the probability that external node outside the cluster is a malicious node in the next stage [13].

In the multi-stage intrusion detection game, IDS in WSNs shows that cluster head and sensor nodes cooperate with each other in the cluster [14, 15]. The malicious node and IDS

constitute the roles of the signal sender and receiver in WSNs. Thus, the game between IDS and external node can be regarded as signal game in each stage.

Some sensor nodes are more “attractive” to attackers than others. Such targets belong to the nodes containing more sensible information and lower security intensity. When attack cost is greater than the revenue, the malicious node will not choose to attack the sensor node. Similarly, IDS tends to perform a defense strategy if and only if the defense revenue is greater than the payment. Therefore, how to calculate the security-weight threshold of sensor nodes is the key to solve the game model of IDM.

The rest of this paper is organized as follows: In Section 2, a review of the IDS in WSNs is presented. Besides, the advantages and disadvantages of existing IDM are compared in different aspects. In section 3, the multi-stage intrusion detection game is formulated and then the security-weight threshold is calculated. In Section 4, the Nash equilibrium is derived under different conditions. In Section 5, the optimal strategy for multi-stage intrusion detection is designed based on the network parameters in WSNs. Experiment and comparison are given in Section 6 and conclusions are reached in Section 7.

2. Related Work

IDS has been an active research field in recent years. Most research efforts address the problem of how to accurately detect the illegal behaviors: e.g., increase relational database, shorten detection period, decrease false alarm rate, etc [16]. As a proactive defense technology, IDS in WSNs makes it possible to prevent internal and external attacks simultaneously.

Recently, several theoretical approaches to the intrusion detection in WSNs have been proposed to improve the performance of IDS. Kolias et al. proposed a distributed IDS based on the abnormal behavior detection and key parameter selection of cluster heads, in which single-point independent detection mechanism is realized to improve the detection rate, but the system overhead is increased [16]. Later Yu et al. developed the previous work on traffic prediction to detect malicious nodes using a behavior-tree-based algorithm [17]. In [18], the ARMA model is constructed to predict the data flow in each region of the network, and the traffic threshold is configured to detect the illegal behaviors. Based upon detecting the traffic threshold, Patel et al. introduced a cooperative IDS in which attacks can be decided by the neighbor node when the local detection engine cannot be determined. Kalnoor et al. constructed an IDS model based on proxy cooperation. Monitoring agents, decision agents and agent equivalents achieve the isolation of malicious nodes [19]. However, the model does not take into consideration the resource characteristics of WSNs in hierarchical tree structure. Considering the weakness of proxy-cooperation-based IDS model, Manandhar et al. proposed a hierarchical hybrid detection architecture, which takes advantage of different functional nodes and the degree of threat to the implementation of Kalman filter [20]. Forootaninia et al. introduced a cooperative watchdog detection method, which deploys neighbor node of the sender and the receiver as a watchdog to monitor the relationship between the measurement parameters and the threshold. In their model, a rotation mechanism is designed to improve response speed of the detection, but the algorithm is based on the predictable security threat type. Hence, this algorithm cannot apply to the unpredictable network environment [21]. Wang et al. proposed a competitive clustering algorithm to train and modify supervisory rules, which is aimed to make the WSNs tolerant to labels lost and improve the system's self-learning function. Nevertheless, the limited supervisory rules relatively weaken the system’s robustness for attack defense [22].

Currently, many researchers pay attention to the game theoretical model of IDS in WSNs. The external node and IDS are regarded as participants in the game. In [23], the main emphasis is placed on the noncooperative nonzero-sum game with chi-square detection method. A Bayesian hybrid solution is computed based on the maximum likelihood equation for the defender to strike a balance between security costs and monitoring gains. To a certain extent, the scheme is not suitable for node replication attack because of the exceptional pattern in this situation. Jokar et al. modeled the interaction between sensor node and external node as a continuous differential game (CDG) where the external node is either "normal" or "malicious" [24]. In reality, time is continuous, that is to say, the IDS has to update its strategy over time, rather than chooses its behaviors at discrete time, which is not suitable to the WSNs environment. In order to reduce the computational cost of the algorithm, Moosavi et al. [25] put forward an anomalous behavior detection mechanism (ABDM) based on the Markov-chain game and set the predefined thresholds for comparison. However, the threshold is difficult to calculate accurately, which indicates that it needs to be further improved.

Despite the substantial work on the IDS in WSNs, none of them addresses the problem in resource-constrained environment and multi-stage game [26]. The realization of each scheme in WSNs needs to adapt to the characteristics of limited resources, which include node power, communication bandwidth, computing speed and storage capacity. Otherwise, the nodes embedded security strategy will be quickly exhausted, which seriously threaten the network topology and system security. The IDM should efficiently run in the nodes with limited resource to ensure the security of the communication, which demands the optimal resource utilization. Motivated by this observation, our work contributes to the existing research results by providing a multi-stage game theoretical framework of the IDS problem in resource-constrained environment consisting of sensor nodes with different security weights. By calculating the solution of Bayesian equilibrium, we further derive the optimal defense strategy for clustered WSNs in each stage.

3. Dynamic Intrusion Detection Game Model

Consistently with the existing researches, it is assumed that N sensor nodes in WSNs have been clustered and each cluster holds only one cluster head. According to the classical defense model, the IDS consists of cluster head and sensor nodes in each cluster [23, 24]. Cluster head and sensor nodes cooperate with each other to implement the detection and defense mechanism. It is started with the situation where there are the attacker and defender. The interaction between them is modeled as a noncooperative nonzero-sum game. Assuming that the external nodes and IDS are rational, it is defined that the strategy is completely governed by the utility functions. The IDS and external nodes have limited resources. Sensor nodes in the cluster possess different security weights respectively, ie. $W_1 \geq W_2 \geq \ldots \geq W_N$.

The notations in the multi-stage intrusion detection game (MIDG) are shown in **Table 1**.

Table 1. Definition of the notations

Notation	Definition
p_i	The probability that the external nodes attacks sensor node i
P_A	The set of strategies for external node
P	Resource constraints for external node
u_S	The utility function of external node
W_i	Security weight of the sensor node i in the cluster

p_i^*	Equilibrium solution to attack sensor node *i*
a	Detection rate
θ_S	The type of external nodes
$C_a W_i$	Resource consumption to attack sensor node *i*
$C_f W_i$	Resource consumption generated by false alarm
β	Wireless channel reliability
q_i	The probability that cluster head allocate resources to sensor node *i*
Q_D	The set of strategies for IDS
Q	Resource constraints of IDS
u_R	Utility function of IDS
Γ	The set of sensor nodes which may be attacked
q_i^*	Equilibrium solution to detect sensor node *i*
b	False alarm rate
θ_R	The type of IDS
$C_d W_i$	Resource consumption in that node *i* defense attack
Θ	The type space of participants
$P^{(t)}(\theta_S = 1)$	The posterior probability that IDS considers the external node as malicious node in the t^{th} stage
$a_S(t)$	The action of *S* in the t^{th} stage
$\hat{a}_S(t)$	The action of *S* in the t^{th} stage which is detected by *R*
$P^{(t)}(\theta_S = 1 \mid \hat{a}_S(t))$	The priori inference probability that *S* is a malicious node in the $(t+1)^{th}$ stage
$P(\hat{a}_S(t+1) \mid \theta_S = 1)$	The probability that *R* detects the action $\hat{a}_S(t+1)$ when *S* is a malicious node in the $(t+1)^{th}$ stage

3.1 Game Model

Assume that cluster heads and sink node linked to base station are the trusted nodes in WSNs. The types of external node outside the communication range of cluster head may be “legal” or “malicious”. Malicious node can attack all the sensor nodes in the cluster. Cluster head takes advantage of the defense strategy to allocate network resource to each sensor node with certain probability. Then, sensor node combines the security mechanism with network resource to defense malicious behaviors. Thus, the IDS consists of cluster head, sensor nodes and corresponding sets of the security strategy.

Fig. 1 depicts the network model, which includes cluster head, sensor nodes, external node and base station. The external node is the data sender and intruder. The IDS is the data receiver and detector. The relationship between the participants is consistent with the characteristics of signal game. Since the type of external node is uncertain to the defender, it is necessary for the IDS to update the estimated possibility that external node is malicious in the dynamic game. Therefore, the continuous time is divided into independent stages. A signal game between external node and IDS is executed in each stage. The overall interaction between the attacker and defender is illustrated with a multi-stage intrusion detection game (MIDG). When multiple external nodes attack the same cluster simultaneously, these nodes are regarded as one malicious node in this paper. Considering the attack revenue in the network is not superimposed, one or more malicious nodes have the same utility to the sensor node.

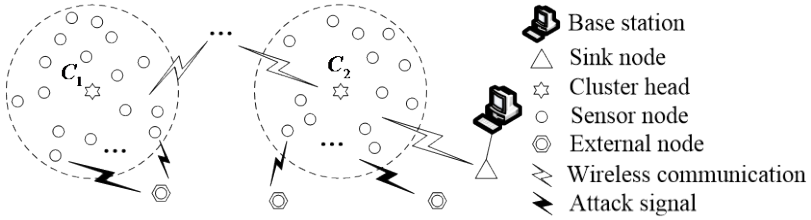


Fig. 1. Network model

It is started with the assumption that the set of sensor nodes in the cluster is $\Gamma = \{1, 2, \ldots, N\}$. The network is modeled as a seven-tuple $\mathbb{Z}(N, \Theta, A, P_E, P_A, Q_D, U)$, where N is the set of two participants in MIDG which we refer to as external node/sender *S* and intrusion detection system/receiver *R* throughout the paper, $\Theta = \Theta_S \times \Theta_R$ is the set of type space in which Θ_S and Θ_R denote the type space of external nodes and intrusion detection system respectively, $A = A_S \times A_R$ is the set of actions.

$A_S = \{\{a_S(\theta_S = 0) \mid Cooperate\}, \{a_S(\theta_S = 1) \mid Attack, Cooperate\}\}$ is the set of actions *S* can take, similarly, $A_R = \{a_R \mid Defend, Idle\}$ is the set of actions *R* can take. If the sender *S* is a legal node, it cooperates with the receiver *R*. Otherwise, the sender *S* can choose to attack or cooperate with receiver *R* as a malicious node. Furthermore, the receiver *R* executes the strategy to defend or idle, which is aimed to get the optimal payoff. $\Theta_S = \{\theta_S = 0, \theta_S = 1\}$ is the type space of external nodes *S* which represents legal node if $\theta_S = 0$ and malicious node if $\theta_S = 1$ respectively. $\Theta_R = \{\theta_R = 1\}$ denotes the IDS is a receiver. $P_E : \Theta_S \mapsto [0,1]$ represents the prior probability that the external nodes *S* is a malicious node. In Bayesian statistical inference, a prior probability of an uncertain quantity p (for example, suppose p is the proportion of voters who will vote for the politician named Tim in a future election) is the probability distribution that would express one's uncertainty about p before the "data" (for example, an opinion poll) is taken into account. $P = (p, 1-p)$, where *p* represents the initial probability that receiver *R* believe sender *S* is a malicious node in the first stage. The purpose of *S* is to achieve the maximum damage to the sensor nodes without being detected by IDS. To this end, external nodes choose the strategy $P_A = (p_1, p_2, \cdots, p_N)$, which is the attack probability to each sensor node within the cluster. Similarly, $Q_D = (q_1, q_2, \cdots, q_N)$ is the strategy of the defender to each sensor node. That is to say, the defender monitors the sensor node *i* with the probability q_i. $\sum_{i \in \Gamma} p_i \le P$ represents resource constraint of the external nodes. We have $P \le 1$ that represents there is one external node outside the cluster and $P > 1$ that represents there are multiple external nodes. $\sum_{i \in \Gamma} q_i \le Q \le 1$ reveals that IDS has only one cluster head in the cluster. $U = (u_S, u_R)$, where u_S is the utility function of the sender *S*, u_R is the utility function of the receiver *R*.

In practice, security weights of sensor nodes are evaluated depending on appropriate standard. The set of security weights for sensor nodes is denoted by $W = \{W_1, W_2, \ldots, W_N\}$, which represents the importance of the secret information possessed by sensor nodes or the position of the nodes in the topology. If the attack on sensor node *i* is successful, the attacker will get payoff W_i.

Table 2 illustrates the payoff matrix of the sender's/receiver's interaction on sensor node *i* in different situations. In **Table 2**, *a* denotes the detection rate of the receiver *R*. *b* denotes the false alarm rate under the influence of electromagnetic environment, and $0 \le a, b \le 1$. The resource consumption of the attack and defense is taken into account. Consequently, it is assumed that the loss to attack and defend sensor node *i* is denoted as $C_a W_i$ and $C_d W_i$ respectively. Then, we have the constraint $C_a < 1$. Otherwise, the rational *S* will never choose to attack *R*. Similarly, $C_d < 1$. β represents the wireless channel reliability which can influence the judgment of the action taken by *S*. $C_f W_i$ denotes the loss of receiver *R*, which is generated by false alarm. If *S* is a legal node, zero is the payoff of *S* in MIDG (in other words, *S* has to choose the action "Cooperate" and this action has no negative effects on the network). Assume that *S* is a legal node and it chooses the action "Cooperate", then the payoff of *R* can be denoted by $-bC_f W_i - C_d W_i$ if *R* takes the action "Defend". Thus, $\{0, -bC_f W_i - C_d W_i\}$ is the payoff set in this situation. Similarly, if *S* and *R* take different actions, the payoff matrixes are constructed in **Table 2(a)** and **Table 2(b)**.

Table 2. Payoff matrix of intrusion detection game

(a) The sender *S* is a legal node

	Defend	Idle
Cooperate	$\{0, -bC_f W_i - C_d W_i\}$	{0,0}

(b) The sender *S* is a malicious node

	Defend	Idle
Attack	$\{(1-\beta)W_i + \beta(1-2a)W_i - C_a W_i,$ $-(1-\beta)W_i - \beta(1-2a)W_i - C_d W_i\}$	$\{W_i - C_a W_i,$ $-W_i\}$
Cooperate	$\{0, -bC_f W_i - C_d W_i\}$	{0,0}

According to the Bayesian rule [25], the posterior probability that *S* is of a malicious node in the $(t+1)^{th}$ stage can be updated from the parameters of the game in the t^{th} stage, which can be expressed as:

$$P^{(t+1)}(\theta_S = 1 \mid \hat{a}_S(t+1)) = \frac{P(\hat{a}_S(t+1) \mid \theta_S = 1) \cdot P^{(t)}(\theta_S = 1 \mid \hat{a}_S(t))}{\sum_{\theta_S \in \Theta_S} P(\hat{a}_S(t+1) \mid \overline{\theta_S}) \cdot P^{(t)}(\overline{\theta_S} \mid \hat{a}_S(t))}, \tag{1}$$

where the difference between $\hat{a}_S(t)$ and $a_S(t)$ is determined by the detection rate *a* and false positive rate *b*. If the action $a_S(t)$ is "Cooperate", then the probability that $\hat{a}_S(t)$ is "Attack" can be calculated by percentage *b*.

Traditionally, the malicious node chooses the action depending on a mixed strategy. It is assumed that malicious node performs the strategy $\delta_S = (\rho, 1-\rho)$, where ρ denotes the probability to attack the receiver *R*, and similarly, $1-\rho$ denotes the probability to cooperate with the receiver *R*. Thus, we have $\rho = \sum_{i \in \Gamma} p_i$.

The probability formulas in equation (1) can be expressed as:

$$P(\hat{a}_S(t+1) = Attack \mid \theta_S = 1) = a\rho\beta + (1-\rho) \cdot b\beta, \tag{2}$$

$$P(\hat{a}_S(t+1) = Attack \mid \theta_S = 0) = b\beta, \tag{3}$$

$$P(\hat{a}_S(t+1) = Cooperate \mid \theta_S = 1) = 1 - \beta + (1-a) \cdot \rho\beta + (1-b) \cdot (1-\rho)\beta, \tag{4}$$

$$P(\hat{a}_S(t+1) = Cooperate \mid \theta_S = 0) = 1 - b\beta. \tag{5}$$

With the upcoming iterations of parameter $P^{(t)}$, the dynamic game model G exists a perfect Bayesian equilibrium if and only if it satisfies the Bayesian conditions. Thus, it should be proved that the Bayesian conditions is satisfied in MIDG.

The definition of the Bayesian conditions is as follows [25].

Definition 2: Bayesian conditions include:

1. The posterior probability is strictly calculated by the prior probability and Bayesian rules;
2. The posteriori probabilities of the participants are linearly independent with each other and all types of the participants have the unified prior probability;
3. The participants do not transmit any information that they don't know;
4. The joint probability distribution of the posterior probability is consistent with type space Θ.

Theorem 1 If the MIDG is defined as seven-tuple G in Definition 1, then the Bayesian condition is satisfied in MIDG.

Proof. Obviously, the posterior probability is obtained by the combination of the prior probability and Bayesian rule according to formula (1). Thus, the MIDG satisfies conditions 1 in Definition 2. Since the receiver *R* only has the ability to defense malicious nodes, Bayesian condition 2 is clearly satisfied. The information transmitted by the sender *S* is determined by the action performed. When the sender *S* executes the same action, the posterior probabilities that the sender *S* is malicious node must be equal. Therefore, Bayesian condition 3 is satisfied. Considering there are only two participants in each stage of MIDG, the other nodes and systems will not affect the update of the posteriori probability that sender *S* is a malicious node. Thus, Bayesian condition 4 is satisfied. Proof finished.

The purpose of MIDG is to formulate the equilibrium solution p_i^* and q_i^*, which can optimize the utility function of IDS.

Depending on the payoff matrixes of the sender *S* and receiver *R*, the utility functions u_S and u_R are given as follows:

$$\begin{aligned} u_S(P_A,Q_D) &= P^{(t)} \cdot \sum_{i\in\Gamma} \{ p_i q_i [(1-\beta)W_i + \beta(1-2a)W_i - C_a W_i] + p_i(1-q_i)(W_i - C_a W_i) \} \\ &= P^{(t)} \cdot \sum_{i\in\Gamma} p_i W_i (1 - 2a\beta q_i - C_a) \end{aligned} , \quad (6)$$

$$\begin{aligned} u_R(P_A,Q_D) &= P^{(t)} \sum_{i\in\Gamma} \{ p_i q_i (-(1-\beta)W_i - \beta(1-2a)W_i - C_d W_i) - p_i(1-q_i)W_i \\ &\quad - (1-p_i)q_i(bC_f W_i + C_d W_i)\} - (1-P^{(t)}) \sum_{i\in\Gamma} q_i (bC_f W_i + C_d W_i) \\ &= \sum_{i\in\Gamma} q_i W_i [p_i \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] - P^{(t)} \cdot \sum_{i\in\Gamma} p_i W_i \end{aligned} . \quad (7)$$

Knowing that the resource is constraint and sensor nodes have different security weights respectively, sender *S* will choose to attack the sensor nodes whose security weight is larger relatively to get more payoffs. Thus, there exists a security-weight threshold of the sensor nodes. In order to maximize the utility function of *S*, sender *S* will only attack the sensor nodes whose security weights are above the threshold. Since the sender *S* and receiver *R* are rational, the key problem is how to calculate the security-weight threshold to get the set of vulnerable nodes.

3.2 Node Security Weight Analysis

The security weights of the sensor nodes can be given as $W_1 \geq W_2 \geq \ldots \geq W_N$. *N* is the number of the sensor nodes in the cluster. In order to investigate the attack characteristics of the sender to

sensor nodes, the sensor nodes are divided into different sets according to the security weights. The definition is as follows:

Definition 3 The set Γ_S of sensor nodes that are most vulnerable to attack and Γ_Q that are more vulnerable to attack are defined below:

$$\begin{cases} W_i > \dfrac{|\Gamma_S|\cdot(1-C_a)-2a\beta Q}{(\sum\limits_{j\in\Gamma_S}\dfrac{1}{W_j})(1-C_a)}, & \forall i\in\Gamma_S \\ W_i = \dfrac{|\Gamma_S|\cdot(1-C_a)-2a\beta Q}{(\sum\limits_{j\in\Gamma_S}\dfrac{1}{W_j})(1-C_a)}, & \forall i\in\Gamma_Q \\ W_i < \dfrac{|\Gamma_S|\cdot(1-C_a)-2a\beta Q}{(\sum\limits_{j\in\Gamma_S}\dfrac{1}{W_j})(1-C_a)}, & \forall i\in\Gamma-\Gamma_S-\Gamma_Q \end{cases}, \tag{8}$$

where $|\Gamma_S|$ is the cardinality of the set Γ_S and is denoted by N_A, $\Gamma-\Gamma_S-\Gamma_Q$ denotes the set of sensor nodes that are neither in set Γ_S nor in set Γ_Q.

The value of utility function of *S* is optimal depending on Definition 3. The explanation of the conclusion above and sets division of sensor nodes in Definition 3 will be presented in the proof of Theorem 2 below.

Lemma 1 If the sensor nodes hold unequal security weights, then the set Γ_S and Γ_Q are unique. Γ_S is composed of sensor nodes with the highest security weight, satisfying the conclusions below:

1) If $W_N > (N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$, then $N_A = N$, $\Gamma_S = \Gamma$, $\Gamma_Q = \varnothing$.

2) If $W_N \le (N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$, then N_A is calculated by the following formulas:

$$\begin{cases} W_{N_A} > \dfrac{N_A\cdot(1-C_a)-2a\beta Q}{\left(\sum\limits_{j=1}^{N_A}\dfrac{1}{W_j}\right)\cdot(1-C_a)} \\ W_{N_A+1} \le \dfrac{N_A\cdot(1-C_a)-2a\beta Q}{\left(\sum\limits_{j=1}^{N_A}\dfrac{1}{W_j}\right)\cdot(1-C_a)} \end{cases}. \tag{9}$$

Proof. In conclusion 1), if $W_N > (N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$ and $\forall i < N$, then $W_i \ge W_N$. Thus, $W_i > \dfrac{N\cdot(1-C_a)-2a\beta Q}{(\sum\limits_{j\in\Gamma_S}\dfrac{1}{W_j})(1-C_a)}$ is clearly established. It can be derived that $N_A = N$, $\Gamma_S = \Gamma$, $\Gamma_Q = \varnothing$. In summary, the conclusion 1) is proved definitely.

In conclusion 2), to prove that N_A exists and satisfies formula (9), it should be ensured that the existence and uniqueness of N_A are certified.

1. Proof the existence. Considering $W_N \le (N(1-C_a)-2a\beta Q)/(1-C_a)\sum_{j=1}^{N}\frac{1}{W_j}$, we have $N_A < N$. If $\forall i < N_A$, then $W_i \ge W_{N_A} > \frac{N_A\cdot(1-C_a)-2a\beta Q}{\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)\cdot(1-C_a)}$. Combined with formula (9), it follows that $W_{N_A+1}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)\cdot(1-C_a) \le N_A\cdot(1-C_a)-2a\beta Q$. Then, $W_{N_A+1}\left(\sum_{j=1}^{N_A+1}\frac{1}{W_j}\right)\cdot(1-C_a) = \left[1+W_{N_A+1}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)\right]\cdot(1-C_a) \le (N_A+1)\cdot(1-C_a)-2a\beta Q$. Thus, the inequality is derived that $W_{N_A+1} \le \frac{(N_A+1)\cdot(1-C_a)-2a\beta Q}{\left(\sum_{j=1}^{N_A+1}\frac{1}{W_j}\right)\cdot(1-C_a)}$. Hence, it is proved that the set of sensor nodes whose number is N_A with the highest security weight satisfies the conditional constraints in formula (8).

2. Proof of the uniqueness. Assume a situation where set Γ_S is composed of *m* sensor nodes and $m < N_A$. From formula (9), we have $W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right) > N_A - \frac{2a\beta Q}{1-C_a}$, then it is inferred that $W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)-(N_A-m) > m-\frac{2a\beta Q}{1-C_a}$. Noticing $m < N_A$ and $W_i \ge W_{N_A}$ if $i < N_A$, it follows that $W_{m+1} \ge W_{N_A}$. Hence, we have $W_{m+1}\left(\sum_{j=1}^{m}\frac{1}{W_j}\right) \ge W_{N_A}\left(\sum_{j=1}^{m}\frac{1}{W_j}\right) = W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right) - W_{N_A}\left(\sum_{m+1}^{N_A}\frac{1}{W_j}\right) \ge W_{N_A}\left(\sum_{j=1}^{N_A}\frac{1}{W_j}\right)-(N_A-n) > m-\frac{2a\beta Q}{1-C_a}$. That is $W_{m+1} > (m\cdot(1-C_a)-2a\beta Q)/(1-C_a)(\sum_{j=1}^{m}1/W_j)$. Obviously, it conflicts with the above conclusion. The assumption $m < N_A$ is invalid according to the analysis. Similarly, it can be certified that $m > N_A$ is impossible. The uniqueness of N_A is proved.

Theorem 2 In the cluster of WSNs, if sender *S* is rational, then it will never attack sensor nodes that belong to the set $\Gamma-\Gamma_S-\Gamma_Q$.

Proof. If $W_N > (N(1-C_a)-2a\beta Q)/(1-C_a)(\sum_{j=1}^{N}1/W_j)$ and $\Gamma-\Gamma_S-\Gamma_Q=\varnothing$, the Theorem 2 is obviously true.

If $W_N \le (N(1-C_a)-2a\beta Q)/(1-C_a)(\sum_{j=1}^{N}1/W_j)$ and $\Gamma-\Gamma_S-\Gamma_Q\ne\varnothing$, a vector $Q_D^1=(q_1^1,q_2^1,\cdots,q_N^1)$ is constructed. The detailed definition is as follows:

$$q_i^1 = \begin{cases} \{1 - C_a - [N_A \cdot (1 - C_a) - 2a\beta Q] / W_i \cdot \sum_{j=1}^{N_A} 1/W_j\} / 2a\beta, & i \in \Gamma_S \\ 0, & i \in \Gamma - \Gamma_S \end{cases} \tag{10}$$

Assume that a rational sender will attack at least one sensor node in the set $\Gamma - \Gamma_S - \Gamma_Q$. The attack strategy is $P_A = (p_1, p_2, \cdots, p_N)$ such that $\sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i > 0$. Then the strategy $P_A^1 = (p_1^1, p_2^1, \cdots, p_N^1)$ is constructed such that $\sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i^1 = 0$. The distribution of p_i^1 is as follows:

$$p_i^1 = \begin{cases} p_i, & i \in \Gamma_S, i \neq n \\ p_n + \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_j, & i = n \\ p_i, & i \in \Gamma_Q \\ 0, & i \in \Gamma - \Gamma_S - \Gamma_Q \end{cases} \tag{11}$$

Our objective is to prove the result $u_S(P_A, Q_D) < u_S(P_A^1, Q_D)$. The utility functions of the attack strategy P_A and P_A^1 should be primarily calculated, respectively. Then, the rational sender *S* will select the strategy with larger value of utility function u_S. Depending on formula (6), (10), (11) and $q_n^1 \geq q_n$, it can be obtained that:

$$\begin{aligned} u_S(P_A, Q_D) - u_S(P_A^1, Q_D) &= P^{(t)} \cdot \sum_{i \in \Gamma} p_i W_i (1 - 2a\beta q_i - C_a) - P^{(t)} \cdot \sum_{i \in \Gamma} p_i^1 W_i (1 - 2a\beta q_i - C_a) \\ &= P^{(t)} \cdot \sum_{i \in \Gamma} p_i W_i (1 - 2a\beta q_i - C_a) - P^{(t)} \cdot \Big(\sum_{i \in \Gamma_S + \Gamma_Q, i \neq n} p_i W_i (1 - 2a\beta q_i - C_a) \\ &\quad + (p_n + \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_j) \cdot W_n (1 - 2a\beta q_n - C_a) \Big) \\ &= P^{(t)} \cdot \left(\sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i W_i (1 - 2a\beta q_i - C_a) - \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i W_n (1 - 2a\beta q_n - C_a) \right) \\ &\leq P^{(t)} \cdot \left(\sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i W_i (1 - 2a\beta q_i - C_a) - \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i W_n (1 - 2a\beta q_n^1 - C_a) \right) \cdot \\ &= P^{(t)} \cdot \left(\sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i W_i (1 - 2a\beta q_i - C_a) - \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i \frac{N_A \cdot (1 - C_a) - 2a\beta Q}{\sum_{j=1}^{N_A} 1/W_j} \right) \\ &\leq P^{(t)} \cdot \sum_{i \in \Gamma - \Gamma_S - \Gamma_Q} p_i \left(W_i (1 - C_a) - (N_A \cdot (1 - C_a) - 2a\beta Q) / \sum_{j=1}^{N_A} 1/W_j \right) \\ &< 0 \end{aligned}$$

A rational sender tends to choose the most profitable behaviors, and the strategy P_A^1 gives the sender more payoff than P_A. That is to say, sender *S* will choose strategy P_A^1 compared with P_A.

Theorem 2 illustrates that only the sensor nodes in Γ_S and Γ_Q is attractive to sender *S* and receiver *R*. Sender *S* has no intention to attack the sensor nodes in $\Gamma - \Gamma_S - \Gamma_Q$, even if these nodes are not defended by receiver *R*. Similarly, the rational receiver *R* will never allocate the limited resource to set $\Gamma - \Gamma_S - \Gamma_Q$ to defend the attacks.

4. Solution of the Model

In this section, the Bayesian equilibrium of MIDG is derived according to the characteristics of security weights in section 3. Considering the range of the parameters and the utility functions of the participants, the solution of equilibrium is classified in several cases below.

Theorem 3 (P_A^*, Q_D^*) is the solution of equilibrium in MIDG if it holds that

1) If $N_D \geq N_A$ and $N_A(1-C_a) \geq 2a\beta Q$, then

$$p_i^* = \begin{cases} \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \dfrac{1}{W_j}} - \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)} \cdot \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \dfrac{1}{W_j}} - 1 \right), & i \in \Gamma_S \\ \in [0, \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \dfrac{1}{W_j}} - \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)} \cdot \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \dfrac{1}{W_j}} - 1 \right)], & i \in \Gamma_Q \\ 0, & i \in \Gamma - \Gamma_S - \Gamma_Q \end{cases},$$

$$q_i^* = \begin{cases} \dfrac{1}{2a\beta} \left(1 - C_a - \dfrac{N_A(1-C_a) - 2a\beta Q}{W_i \sum_{j=1}^{N_A} \dfrac{1}{W_j}} \right), & i \in \Gamma_S \\ 0, & i \in \Gamma - \Gamma_S \end{cases},$$

where P_A denotes the sum of the attack probabilities allocated in the set Γ_S, $\sum_{i \in \Gamma} p_i^* = P$, $\sum_{i \in \Gamma} q_i^* = Q$, and $P_A > (N_A - W_{N_A} \sum_{j=1}^{N_A} (1/W_j))((bC_f + C_d)/(P^{(t)}(2a\beta + bC_f)))$.

2) If $N_D < N_A$, then

$$p_i^* \begin{cases} = \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)}, & W_i > W_{N_D+1} \\ \in [0, \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)}], & W_i = W_{N_D+1} \\ = 0, & W_i < W_{N_D+1} \end{cases}, \quad q_i^* = \begin{cases} \dfrac{1 + C_a}{2a\beta} \left(1 - \dfrac{W_{N_D+1}}{W_i} \right), & W_i > W_{N_D+1} \\ 0, & W_i < W_{N_D+1} \end{cases},$$

where $\sum_{i \in \Gamma} p_i^* = P$, and $\sum_{i \in \Gamma} q_i^* < Q$.

3) If $N_D \geq N_A$ and $N(1-C_a) < 2a\beta Q$, then

$$\begin{cases} p_i^* = (bC_f + C_d)/P^{(t)}(2a\beta + bC_f) \\ q_i^* = (1 - C_a)/2a\beta \end{cases} i \in \Gamma,$$

where $\sum_{i \in \Gamma} p_i^* < P$, and $\sum_{i \in \Gamma} q_i^* < Q$.

Proof. Assume that (P_A^*, Q_D^*) is Bayesian equilibrium of MIDG. Noticing that sender S chooses the strategy that guarantees the maximum revenue of the utility function, the attack probability to sensor node i tends to zero in case of $P^{(t)} \cdot \sum_{i \in \Gamma} W_i(1 - 2a\beta q_i - C_a) < 0$. If $0 \leq P^{(t)} \cdot \sum_{i \in \Gamma} W_i(1 - 2a\beta q_i - C_a) < P^{(t)} \cdot \sum_{j \in \Gamma} W_j(1 - 2a\beta q_j - C_a)$, sender S has plenty of incentive to

decrease p_i^* and increase p_j^*. Hence, p_i^* tends to zero. Depending on the utility function $u_S(P_A, Q_D)$, the inequality can be obtained as follows:

$$\begin{cases} 0 \le P^{(t)} \cdot \sum_{i\in\Gamma} W_i(1-2a\beta q_i - C_a) = P^{(t)} \cdot \sum_{j\in\Gamma} W_j(1-2a\beta q_j - C_a) \\ P^{(t)} \cdot \sum_{k\in\Gamma} W_k(1-2a\beta q_k - C_a) \le P^{(t)} \cdot \sum_{i\in\Gamma} W_i(1-2a\beta q_i - C_a) \end{cases} . \quad (12)$$
$$\forall i, j, k \in \Gamma, p_i^*, p_j^* > 0, p_k^* = 0$$

Similarly, noticing that the utility function $u_R(P_A, Q_D)$ has been calculated in formula (7), the inequality is formulated below.

$$\begin{cases} 0 \le W_i[p_i \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] = W_j[p_j \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] \\ W_k[p_k \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] \le W_i[p_i \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] \end{cases} \quad (13)$$
$$\forall i, j, k \in \Gamma, q_i^*, q_j^* > 0, q_k^* = 0$$

Considering the resource constraints of the participants, the equilibrium solution of MIDG is computed in three cases.

(1) When the resources of the participants are exhausted in MIDG, combined with formula (12) and (13), the equilibrium solution is calculated as follows:

$$p_i^* = \begin{cases} \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)} \cdot \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1\right), & i \in \Gamma_S \\ \in [0, \dfrac{P_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)} \cdot \left(\dfrac{N_A}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}} - 1\right)], & i \in \Gamma_Q \\ 0, & i \in \Gamma - \Gamma_S - \Gamma_Q \end{cases},$$

$$q_i^* = \begin{cases} \dfrac{1}{2a\beta}\left(1 - C_a - \dfrac{N_A(1-C_a) - 2a\beta Q}{W_i \sum_{j=1}^{N_A} \frac{1}{W_j}}\right), & i \in \Gamma_S \\ 0, & i \in \Gamma - \Gamma_S \end{cases}.$$

The necessary conditions for the existence of Bayesian equilibrium in this situation are as follows:

$$\begin{cases} W_i[p_i \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] \ge 0, P_A \le P \\ (1 - 2a\beta q_i^* - C_a)W_i \ge 0, & i \in \Gamma_S \end{cases}.$$

It can be simplified as $\begin{cases} N_D \ge N_A \\ N_A(1-C_a) \ge 2a\beta Q \end{cases}$, where $N_D = \lfloor (2a\beta + bC_f)P / (bC_f + C_d) \rfloor$, P_A denotes the sum of the attack probabilities allocated in the set Γ_S, and $P_A > (N_A - W_{N_A} \sum_{j=1}^{N_A} (1/W_j))((bC_f + C_d) / (P^{(t)}(2a\beta + bC_f)))$. $\lfloor m \rfloor$ denotes the maximum positive integer not more than *m*.

(2) The resource of sender *S* is exhausted while receiver *R* doesn't use up its detection resource. That is $\sum_{i\in\Gamma} p_i^* = P$ and $\sum_{i\in\Gamma} q_i^* < Q$. It can be inferred that $W_i[p_i \cdot P^{(t)}(2a\beta + bC_f) -$

$(bC_f + C_d)] = 0,\ \forall i, j \in \Gamma, q_i^* > 0$. Otherwise, R will take advantage of the remaining resource to increase q_i^* to maximize the utility function $u_R(P_A, Q_D)$ strictly. Depending on the formula (12) and (13), the equilibrium solution is calculated that:

$$p_i^* \begin{cases} = \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)}, & W_i > W_{N_D+1} \\ \in [0, \dfrac{bC_f + C_d}{P^{(t)} \cdot (2a\beta + bC_f)}], & W_i = W_{N_D+1} \\ = 0, & W_i < W_{N_D+1} \end{cases}, \quad q_i^* = \begin{cases} \dfrac{1 + C_a}{2a\beta}(1 - \dfrac{W_{N_D+1}}{W_i}), & W_i > W_{N_D+1} \\ 0, & W_i < W_{N_D+1} \end{cases}.$$

The necessary condition for the existence of Bayesian equilibrium in this situation is $\sum_{W_i > W_{N_D+1}} q_i^* < Q$. Then, it can be simplified as $N_D < \sum_{W_i > W_{N_D+1}} \dfrac{W_{N_D+1}}{W_i} + \dfrac{2aQ}{1 - C_a}$. Combined with the formula (9) in Lemma 1, it is inferred that $N_D < N_A$.

(3) In this case, neither the sender S nor the receiver R is exhausted. It can be denoted as $\sum_{i \in \Gamma} p_i^* < P$ and $\sum_{i \in \Gamma} q_i^* < Q$, respectively. Then, it is inferred that $W_i[p_i \cdot P^{(t)}(2a\beta + bC_f) - (bC_f + C_d)] = 0, i \in \Gamma$ and $(1 - 2a\beta q_i^* - C_a)W_i = 0, i \in \Gamma$. Otherwise, S and R will increase P_A^* and Q_D^*. Depending on the formula (6) and (7), the equilibrium solution is computed as follows:

$$\begin{cases} p_i^* = (bC_f + C_d) / P^{(t)}(2a\beta + bC_f) \\ q_i^* = (1 - C_a) / 2a\beta \end{cases} i \in \Gamma.$$

The necessary conditions for the existence of Bayesian equilibrium in this case are $N_D \geq N$ and $N(1 - C_a) \leq 2a\beta Q$. Combined with Lemma 1, it can be simplified as $N_A = N$.

Thus, Theorem 3 has been certified. The Bayesian equilibrium of MIDG is evaluated in multiple cases.

In case 1 of Theorem 3, all of the participants exhaust the resources, respectively. In other words, the resource P / Q is the positive factor to $u_S(P_A, Q_D) / u_R(P_A, Q_D)$. In case 2, sender S exhausts the resource while receiver R doesn't use up the resource. It indicates that the parameter a and $C_d W_i$ lead to too much defense cost. If the defense payoff is less than cost, R will not take any actions to defense the attack. In case 3, both sender S and receiver R do not use up the resources. That is to say, the Bayesian equilibrium is acquired before the exhaustion of resources.

Corollary 1 In Theorem 3, for $\forall P_A' \neq P_A^*,\ \forall Q_D' \neq Q_D^*$, if $\hat{P}_A = \arg\max_{\hat{P}_A \in P_A} u_S(P_A, Q_D')$ and $\hat{Q}_D = \arg\max_{\hat{Q}_D \in Q_D} u_S(P_A', Q_D)$, then $u_S(P_A^*, Q_D^*) > u_S(\hat{P}_A, Q_D')$ and $u_S(P_A^*, Q_D^*) > u_S(P_A', \hat{Q}_D)$.

Proof. The proof of Corollary 1 is similar to the Theorem 2.

5. Optimal Scheme of Intrusion Detection

Based on the solution of Bayesian equilibrium (P_A^*, Q_D^*) and the parameters of MIDG, the optimal scheme of IDS in WSNs is designed in this section. The intrusion detection

mechanism consists of security management center, intrusion detection system *R*, and external nodes *S*. **Fig. 2** depicts the interaction among the modules.

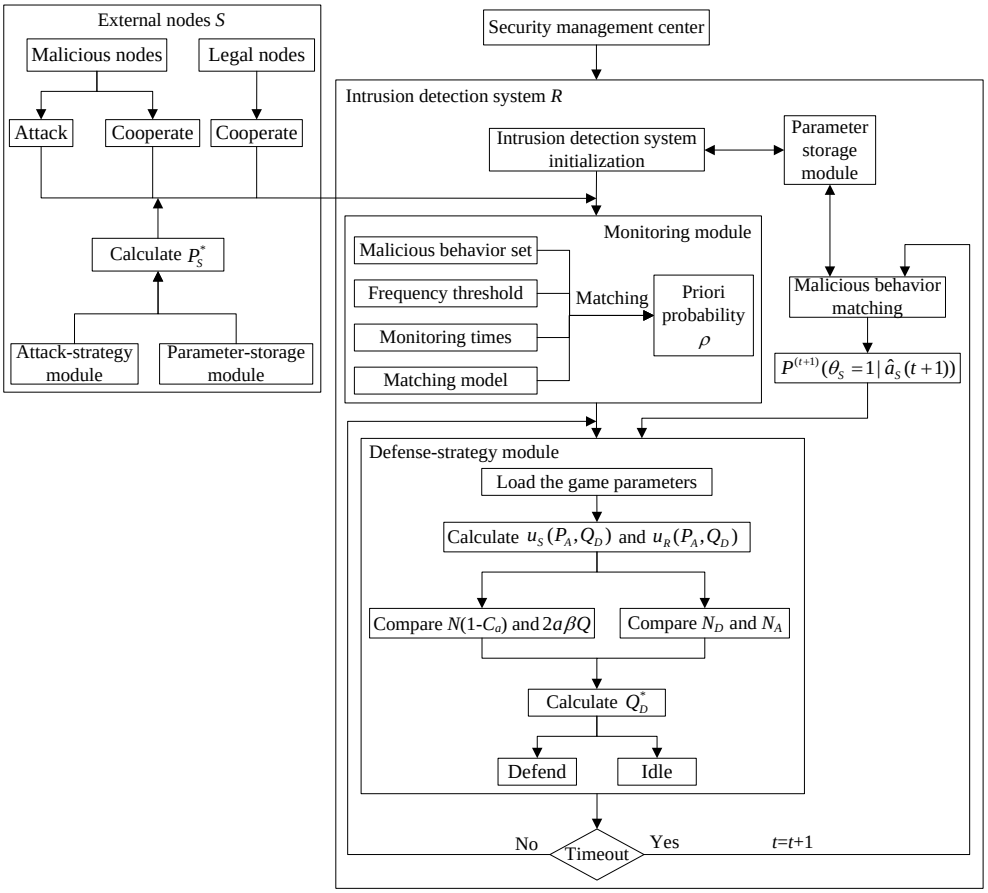


Fig. 2. IDM based on the perfect Bayesian equilibrium

Security management center in WSNs is primarily responsible for the update of knowledge database from the coordinator to cluster heads, which enables cluster head to cooperate with sensor nodes to detect and defense malicious nodes.

It can be argued that the intrusion detection system *R* is the central portion to defend the attacks. When *R* is turned on, the IDS in cluster head starts to initialize the parameters *a*, b, C_a, C_d, C_f, δ_S, $P^{(t)}(\theta_S=1|\hat{a}_S(t))$, *etc*. Since external nodes *S* may be malicious or legal, *S* can choose to take action "Attack" or "Cooperate". In IDS, the priori probability ρ is evaluated by monitoring module in the first stage. Cluster head cooperates with sensor nodes and then continuously monitor the behaviors from the external nodes. The database in monitoring module includes malicious behavior set, frequency threshold, monitoring times and matching model, which is essential to formulate the priori probability. In addition, it is taken into consideration that the sequence alignment algorithms in matching model will be accurate and high-efficiency, such as danger theory and robust theory. A timer is set in defense-strategy module to update the stage accurately. Once there is a timeout, the posterior probability in the t^{th} stage is calculated for MIDG, which can be denoted as $P^{(t+1)}(\theta_S=1|\hat{a}_S(t+1))$. Due to the dynamic nature of IDS in WSNs, the optimal defense strategies are updated periodically by

defense-strategy module depending on the Bayesian rules and corresponding posterior probability $P^{(t+1)}(\theta_S = 1 | \hat{a}_S(t+1))$. The relevant parameters are stored and invoked promptly in parameter storage module. Then the comparison of $N(1-C_a)$, $2a\beta Q$, N_D and N_A can determine which case the Bayesian equilibrium belongs to in Theorem 3. According to the parameters $P^{(t+1)}(\theta_S = 1 | \hat{a}_S(t+1))$, $u_S(P_A, Q_D)$, and $u_R(P_A, Q_D)$, R calculates the solution of Bayesian equilibrium Q_D^*. Then the security strategy is configured in the cluster.

Similarly, to formulate the optimal attack strategy of external nodes *S*, the strategy-game module and parameter-storage module is invoked in each stage. Then the equilibrium solution P_S^* is reached.

Since the constraints in MIDG are $\sum_{i \in \Gamma} p_i \le P$ and $\sum_{i \in \Gamma} q_i \le Q \le 1$, the IDM based on the Bayesian game can be applied to the clustered WSNs. More particularly, there is only one IDS in each cluster.

The optimal defense strategy in MIDG consists of seven steps as described below:

Step 1. Initialize the parameters adopted by MIDG, such as *a*, b, C_a, C_d, C_f, δ_S. Collect the behaviors of external nodes *S* and send them to the monitoring module.

Step 2. For each cluster, depending on malicious behavior set, frequency threshold, monitoring times and matching model, evaluate the initial priori probability ρ in the first stage.

Step 3. Load the game parameters. Then, calculate the utility functions $u_S(P_A, Q_D)$ and $u_R(P_A, Q_D)$ according to formula (6) and (7).

Step 4. Compute the posterior probability $P^{(t)}(\theta_S = 1 | \hat{a}_S(t+1))$ in the (t-1)$^{\text{th}}$ stage

Step 5. Compare the size of $N(1-C_a)$ and $2a\beta Q$. Then compare the size of N_D and N_A. Based on the results of comparison, the solution of Bayesian equilibrium can be determined and formulated.

Step 6. Depending on theorem 3, compute and execute the optimal defense strategy $Q_D^* = \{q_1^*, q_2^*, \cdots, q_N^*\}$ in the t$^{\text{th}}$ stage.

Step 7. If there is a timeout, compute the posterior probability $P^{(t+1)}(\theta_S = 1 | \hat{a}_S(t+1))$ in the t$^{\text{th}}$ stage and then turn to step 3. If not, continue to execute the current defense strategy.

The optimal attack strategy in MIDG is similar to the steps above. What needs to be emphasized is that the solution of Bayesian equilibrium calculated in step 6 is $P_A^* = \{p_1^*, p_2^*, \cdots, p_N^*\}$ in the t$^{\text{th}}$ stage.

6. Experimental Performance Evaluation

To measure the performance of MIDG in clustered WSNs, MATLAB 2010a is adopted to perform the configuration of communication protocol and the parameters to validate our analytical results. From the perspective of the overall WSNs, the ZigBee specification is taken into consideration to set the initial parameters in the cluster. In order to simulate the communication environment in this paper, the resource consumption coefficient of sender *S* and receiver *R* are defined as $C_a = C_d = 0.1$. The coefficient of false alarm is set to $C_f = 0.01$. The total number of sensor nodes in each cluster is $N = 12$. There are 40 clusters in the network and there is no cooperative relationship between cluster heads during the overall simulation. The security weights of the sensor nodes are configured as

$W_i = (12-i)*0.8\ (i=1,2,\cdots,12)$, which represents the importance of sensor nodes in the cluster. The resources that *S* and *R* hold are set to 1. The remaining parameters are defined as $a=0.9$, $b=0.06$, $\beta=0.95$, respectively.

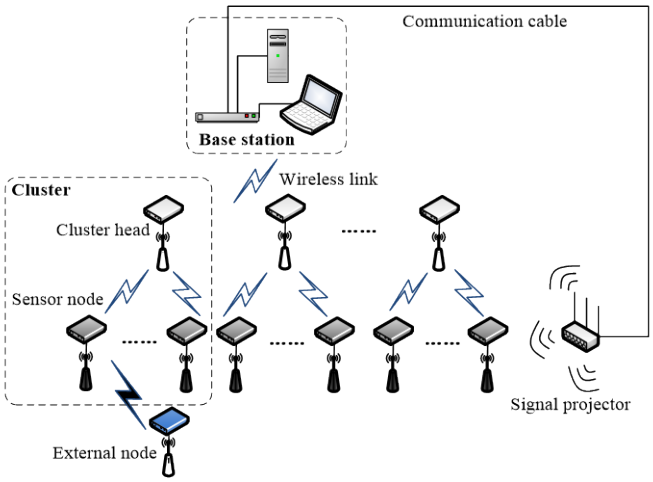


Fig. 3. Structure of the clustered WSNs

To evaluate the conclusions analyzed in this paper, a typical scenario is set that receiver *R* executes random security strategies. The results of utility function u_R in 100 random strategies are shown in **Table 3,** respectively**. Table 4** presents the solution of Bayesian equilibrium in the 20th stage in this paper.

In **Table 3,** $(u_R)_{\max}$ denotes the maximum value of utility function in random strategies. $(u_R)_{\min}$ denotes the minimum value of utility function in random strategies. $\overline{u_R}$ represents the average value of utility function in random strategies.

Depending on the numerical results in **Table 3** and **Table 4**, it can be verified that the Bayesian equilibrium in this paper tends to choose the more "profitable" defense strategy than others. In addition, **Table 4** reveals that there is no attack or defense strategy to sensor node *i* ($8 \le i \le 12$). The reason for this situation is that these nodes belongs to the set $\Gamma - \Gamma_S - \Gamma_Q$, which can be calculated and proved in Theorem 2.

Table 3. The results of utility function in random strategies

symbol	value
$(u_R)_{\max}$	-0.571
$\overline{u_R}$	-0.627
$(u_R)_{\min}$	-0.720

Table 4. The Bayesian equilibrium in the 20th stage

$p_1^* = 0.126, q_1^* = 0.312$
$p_2^* = 0.129, q_2^* = 0.206$
$p_3^* = 0.137, q_3^* = 0.201$
$p_4^* = 0.113, q_4^* = 0.129$

$p_5^* = 0.119, q_5^* = 0.056$
$p_6^* = 0.231, q_6^* = 0.051$
$p_7^* = 0.145, q_7^* = 0.045$
$p_8^* = 0, q_8^* = 0$
$p_9^* = 0, q_9^* = 0$
$p_{10}^* = 0, q_{10}^* = 0$
$p_{11}^* = 0, q_{11}^* = 0$
$p_{12}^* = 0, q_{12}^* = 0$
$u_S^* = 0.566, u_R^* = -0.567$

6.1 Performance Test

The parameters in CDG [24], ABDM [25] and MIDG can influence the behaviors of sender *S* who may attain a positive reward as it launches an attack if receiver *R* does not defend. In addition, a negative reward will render to the sender due to the defense from the receiver or the consumption it takes. Thus, the values of reward have an influence on the optimal strategy of the sender and receiver to make the decision whether to take action or not.

In order to evaluate the effectiveness of our scheme, the MIDG algorithm is compared with one proposed by Jokar et al. [24] and Moosavi et al. [25] according to the training system and Markov chain.

Considering the process of CDG, the support vector machine (SVM) and hybrid intrusion detection module (HIDM) are configured. In this experiment, the next generation intrusion detection system (NGIDS) from Australian defence force academy dataset (ADFA-D) is adopted as a sample to verify the performance of the SVM-based IDM. The relationships between nodes in the ADFA-D have 36 features and they are divided into five classification groups: normal and four malicious behaviors (DDos, U2r, R21, Probe). Our analysis and comparisons are performed by using the samples as sets of regulation. The parameter that denotes the state of malicious behaviors are defined as (-1). Then, the normal behaviors are classified as (+1). The training samples adopted in three algorithms comprises of 60 normal and 60 malicious cases.

Based on the assumptions above, the MIDG in WSNs is simulated and compared with those in [24] and [25]. Let the parameters in the experimental environment be static. By repeating the experiments and computing average values respectively, it is possible to analyze the performance of the schemes. The simulation results are illustrated in **Table 5**.

Table 5. The comparison of performance evaluation in different algorithms

Number of Features	Game Stage	Literature [24]		Literature [25]		This paper	
		Accuracy (%)	Detection rate (%)	Accuracy (%)	Detection rate (%)	Accuracy (%)	Detection rate (%)
12	6	94.13	91.21	87.80	83.66	97.02	93.26
	12	95.54	92.37	88.10	85.21	97.31	94.33
	18	95.83	92.51	88.79	86.47	97.39	95.28
24	6	95.87	92.79	89.92	87.68	98.12	96.07
	12	95.91	93.02	89.97	87.71	98.79	97.43
	18	96.02	93.46	90.06	88.19	99.01	97.96

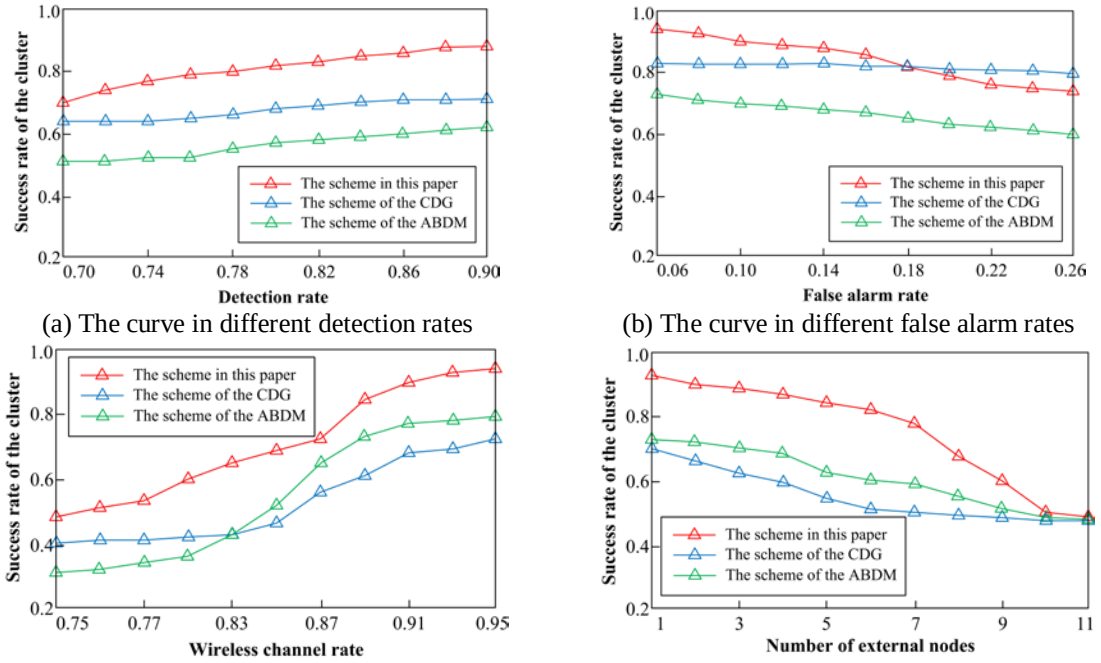
36	6	96.17	93.78	90.85	88.64	98.15	96.09
	12	96.25	93.82	91.42	89.96	98.81	97.76
	18	97.08	93.90	91.45	90.23	99.04	97.99

As is shown in **Table 5**, the scheme of MIDG with 36 features outperforms the CDG and ABDM in all of the game stages, in terms of accuracy and detection rate. This is due to the accurate posterior probability updated and modified by the Bayesian rules constantly. No matter how many features we adopt, the accuracy and detection rate tend to be stable in the 18th stage compared with the results in the 12th stage. The reason for this situation is that MIDG adopts the optimal strategy based on multi-stage game model and the cluster head in MIDG cooperates with multiple sensor nodes to detect and defense the malicious nodes, which improves the accuracy and detection rate to the maximum. As the allocation strategy of non-cooperative game in CDG and ABDM is formulated without considering whether the external node is a malicious node, the accuracy and detection rate of these algorithms is relative stable in each stage. The results in **Table 5** indicate that the scheme of MIDG in this paper has strengths in intrusion detection of WSNs.

6.2 Analysis of Parameters

It is defined that success rate of the cluster represents the ratio of clusters that detect and defense the malicious nodes successfully. γ denotes the number of external nodes in the cluster. According to the IDM in WSNs, the influence factors to success rate of the cluster are mainly depending on the detection rate, false alarm rate, wireless channel reliability (WCR) and the number of external nodes. By adjusting a, b, β and γ in the simulation respectively, it is feasible to intestigate the impact of each parameter on the performance of IDS in WSNs. According to the deployment of experimental environment in **Fig. 3**, the success rates of clusters are computed in different values of the influence factors. By making repeated experiments and calculating average values of the factors respectively, it is reasonable to verify the robustness of MIDG. In CDG, the availability A_{S_i} in the steady state of each sensor node and the discrete state space of WSNs are constant. The radial basis function (RBF) in ABDM is defined as $F_{RBF} = \exp(-\|x_1 - x_2\| / 2)$. Each IDM system constructs the SVM locally and then calculates a set of support vector. Then, the experimental results are shown in **Fig. 4 (a)** , **Fig. 4 (b)**, **Fig. 4(c)** and **Fig. 4 (d),** respectively.

Fig. 4 (a) indicates that the success rate of clusters in IDM increases with the detection rate. Furthermore, the performance in MIDG is always better than those in CDG and ABDM. **Fig. 4 (b)** shows that the number of clusters that detect and defense the malicious nodes successfully diminishes with the increase of false alarm rate. If b>0.18, then the performance in CDG is slightly better than that in MIDG. The relationship between wireless channel reliability and success rate of clusters in IDM is shown in **Fig. 4 (c)**. When the wireless channel keeps high reliability, the success rate of clusters in MIDG has the best performance results compared with other strategies. In **Fig. 4 (d)**, the performance in MIDG is much better than other schemes if the number of external nodes is less than eight. Otherwise, the performance of the schemes in MIDG declines rapidly.



(a) The curve in different detection rates (b) The curve in different false alarm rates

(c) The curve in different WCR (d) The curve in different external nodes

Fig. 4. The success rate of clusters in intrusion detection

7. Conclusion

In this paper, a dynamic multi-stage intrusion detection game is proposed to analyze the wrestling between the cluster and external nodes in WSNs. Depending on hierarchical tree structure, the intrusion detection model is established with limited resource and Bayesian rules. The utility functions of sender S and receiver R are formulated according to the payoff matrixes of sensor node and external nodes. In order to timely update posteriori probability of the sender, the continuous time is divided into multiple stages. Assuming that the sender is rational and security weights of sensor nodes are unequal, the set of sensor nodes vulnerable to attack is properly evaluated. The solution to MIDG with the purpose of optimal payoff to both sides is calculated. Combined with the characteristics and topology of WSNs, the optimal scheme to maximize the security of IDS is proposed. It performs better than the existing schemes in WSNs from the result of experiment on the number of clusters successfully detecting and defending malicious nodes.

The previous researches are committed merely to technical strategies to ensure system security and detection rate. These strategies or algorithms can be implemented in network systems with sufficient computing resources and storage resources. Unfortunately, the extreme application scenarios in WSNs make it impossible to perform the critical security functions. How to implement the techniques of IDS in cluster-based WSNs is an urgent issue to be solved. We expect that the optimal scheme proposed in this paper will be valuable for the application of security mechanism in WSNs.

References

[1] Y. Xue, X. M. Chang, S. M. Zhong and Y. Zhuang,"An efficient energy hole alleviating algorithm for wireless sensor networks," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 3, pp. 347-355, Aug. 2014. Article (CrossRef Link)

[2] J. Ren, Y. X. Zhang, K. Zhang and X. M. Shen,"Lifetime and energy-hole evolution analysis in data-gathering wireless sensor networks," *IEEE Transactions on industrial informatics*, vol. 12, no. 2, pp. 788-800, Jan. 2015. Article (CrossRef Link)

[3] S. Misra and P. D. Thomasinous, "A simple least-time and energy-efficient routing protocol with one-level data aggregation for wireless sensor networks," *The Journal of Systems and Software*, vol. 83, no. 5, pp. 852-860, May. 2010. Article (CrossRef Link)

[4] J. H. Ho, H. C. Shih, B. Y. Liao and S. C. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks," *Information Sciences*, vol. 192, no. 6, pp. 204-212, Jun. 2012. Article (CrossRef Link)

[5] A. Proano, L. Lazos and M. Krunz, "Traffic decorrelation techniques for countering a global eavesdropper in WSNs," *IEEE Transactions on Mobile Computing*, vol. 38, no. 7, pp. 1-14, Jan. 2016. Article (CrossRef Link)

[6] J. Wu, K. Ota and M. Dong, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, no. 4, pp. 416-424, Jan. 2016. Article (CrossRef Link)

[7] L. Cheng, C. D. Wu and Y. Z. Zhang, "Indoor robot localization based on wireless sensor networks," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1099-1104, Aug. 2011. Article (CrossRef Link)

[8] O. M. Vazquez, Y. Shmaliy and M. O. Ibarra, "Distributed unbiased FIR filtering with average consensus on measurements for WSNs," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 1-8, Jan. 2017. Article (CrossRef Link)

[9] M. K. Watfa, H. Al-Hassanieh and S. Salmen, "A novel solution to the energy hole problem in sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 949-958, Mar. 2013. Article (CrossRef Link)

[10] 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, Jan. 2014. Article (CrossRef Link)

[11] K. Lin, T. Xu and J. Song, "Node scheduling for all-directional intrusion detection in SDR-based 3D WSNs," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7332-7341, Jan. 2016. Article (CrossRef Link)

[12] Z. M. Cheng, "A differential game between intrusion detection system and attackers for wireless sensor networks," *Wireless Personal Communications*, vol. 90, no. 3, pp. 1211-1219, Jun. 2016. Article (CrossRef Link)

[13] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless Ad Hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 318-332, Feb. 2013. Article (CrossRef Link)

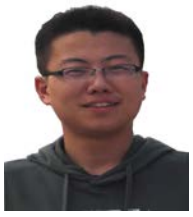
[14] L. Guo, J. Wu, Z. Xia and J. Li, "Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks," *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2577-2586, Mar. 2015. Article (CrossRef Link)

[15] S. Han, M. Xie and H. H. Chen, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1052-1062, Nov. 2014. Article (CrossRef Link)

[16] C. Kolias, V. Kolias and G. Kambourakis, "TermID: A distributed swarm intelligence-based approach for wireless intrusion detection," *International Journal of Information Security*, no. 6, pp. 1-16, Jun. 2016. Article (CrossRef Link)

[17] Q. Yu, J. Lyu and L. Jiang, "Traffic anomaly detection algorithm for wireless sensor networks based on improved exploitation of the GM (1, 1) model," *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, pp. 218-227, Jul. 2016. Article (CrossRef Link)

[18] A. Patel, H. Alhussian and J. M. Pedersen, "A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems," *Computers & Security*, vol. 64, no. 1, pp. 92-109, Jan. 2017. Article (CrossRef Link)
[19] G. Kalnoor, J. Agarkhed and S. R. Patil, "Agent-based QoS routing for intrusion detection of sinkhole attack in clustered wireless sensor networks," in *Proc. of 6th Int. Conf. on Computational Intelligence and Informatics*, pp. 571-583, May 28-30, 2017. Article (CrossRef Link)
[20] K. Manandhar, X. Cao and F. Hu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370-379, Apr. 2014. Article (CrossRef Link)
[21] A. Forootaninia and M. B. Ghaznavi, "An improved watchdog technique based on power-aware hierarchical design for Ids in wireless sensor networks," *International Journal of Network Security*, vol. 4, no. 4, pp. 161-178, Jul. 2012. Article (CrossRef Link)
[22] Y. Wang, D. Wang and F. Chen, "Efficient event detection using self-learning threshold for wireless sensor networks," *Wireless Networks*, vol. 21, no. 6, pp. 1783-1799, Jun. 2015. Article (CrossRef Link)
[23] Z. H. Xiao, Z. G. Chen and X. H. Deng, "Anomaly detection based on a multi-class CUSUM Algorithm for WSN," *Journal of Computers*, vol. 5, no. 2, pp. 306-313, Feb. 2010. Article (CrossRef Link)
[24] P. Jokarand and V. Leung, "Intrusion detection and prevention for ZigBee-based home area networks in smart grids," *IEEE Transaction on Smart Grid*, vol. 15, no. 3, pp. 1-12, Apr. 2016. Article (CrossRef Link)
[25] 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, Sep. 2014. Article (CrossRef Link)
[26] W. Haider, J. Hu, Y. Xie, X. Yu and Q. Wu, "Detecting anomalous behavior in cloud servers by nested arc hidden SEMI-Markov model with state summarization," *IEEE Transactions on Big Data*, vol. PP, no. 99, pp. 1-1, August. 2017. Article (CrossRef Link)



Weiwei Zhou was born in Henan, P. R. China, in December 1990. He received his B.S. degree and M.S. degree in the Zhengzhou Information Science and Technology Institute in 2012 and 2015, respectively. He is currently pursuing his Ph.D. degree in the Department of Computer Science and Information Engineering at Zhengzhou Information Science and Technology Institute. His research interest is wireless sensor networks and information security.

Bin Yu received his B.S. degree in Dept. of Electronic Engineering from the University of Shanghai Jiaotong in 1986, the M.S. degree in Dept. of Automatic Engineering from South China University of Technology in 1991 and the Ph.D. degree in 1999. From 1997 to 1999, he worked as a research assistant at Hong Kong University of Science and Technology. From 2002.12 to 2003.12, he worked as vice professor at University of Waterloo, ON, Canada. Currently, he is a professor of the Department of Computer Science and Information Engineering at Zhengzhou Information Science and Technology Institute, P. R. China. His research interests include the design and analysis of algorithms, visual cryptography and network security.