Intrusion Detection Model of Wireless Sensor Networks Based on Game Theory and an Autoregressive Model

Lansheng Han*[a], Man Zhou*[a], Wenjing Jia[b], Zakaria[c], Xingbo Xu[a]

[a]*School of Computer Science and Technology,*
Huazhong University of Science and Technology, Wuhan, China
[b]*Engineering and Information Technology School, University of Technology Sydney,Australia*
[c]*Huazhong University of Science and Technology, Wuhan, China*
Email: hanlansheng@hust.edu.cn, chexin1417@163.com, 13070819676@163.com

Abstract

A Wireless Sensor Network (WSN) security strategy is imperative to counteract security threats, and energy consumption directly affects the network life-time of a wireless sensor; thus an attempt to exploit a low-consumption Intrusion Detection System (IDS) to detect malicious attacks makes a lot of sense. Current Intrusion Detection Systems can detect just some specific attacks and the network life time is reduced due to their high energy consumption. For the purpose of energy limitation and high efficiency, this paper proposes an intrusion detection model based on game theory and an autoregressive model. The paper not only improves the autoregressive theory model to a non-cooperative complete information static game model, but makes a prediction about attack pattern based on the reliable model. The proposed approach improves on previous approaches in two main ways: it takes energy consumption of the intrusion detection process into account, and it obtains the optimal defense strategy, balancing detection efficiency and the system's energy consumption by analyzing the model's mixed Nash equilibrium solution. In the simulation experiment, the running time of the process is regarded as the main indicator of energy consumption of the system. The simulation results show that the IDS proposed not only effectively predicts the attack time and the next targeted cluster based on the game theory, but also reduces energy consumption.

Keywords: Wireless Sensor Network, Intrusion Detection System, Optimal Defense Strategy, Energy Consumption

1. Introduction

1.1. Current researches

Recent developments in network infrastructure have heightened the need for sensor networks; it is a development direction of intelligent sensor to integrate artificial intelligence with sensor

*Corresponding author

technology , because it improves intelligence of sensor (1; 2). A WSN is a multi-hop distributed network formed by intelligent, miniature, and cheap sensor nodes (3; 4). It consists of three main parts: sensor nodes, a base station (BS), and an observer (5). Sensor nodes are usually deployed randomly in the form of airdrops, and deliver the information to the base station.

As the Internet of Things and the use of sensors become more and more popular, security issues are becoming increasingly prominent (6; 7). In addition, the sensor operating system and its safety protection are very simple, so the sensor invasion is easy and convenient; but its threat is effective and direct, thus attracting more and more malicious intrusion. Different from computers and smart mobile devices, the detection of the sensor provides few external operation interfaces, and can be detected by paying little attention to the source, type, or signal flow of operation. Therefore, the attacks on sensor networks are increasingly artificially or intelligently controlled, and are no longer persistent attacks, because continuous attacks are easy to detect. The topic has received much attention from researchers in both network and security fields. Key management, authentication, security routing, and security services are at core of this technology (8). An IDS monitors user behavior or network traffic at different network levels and adopts an active detection technology to protect the network from various intrusions (9; 10). So far, a considerable number of approaches have been proprosed on this issue (11; 12).

Most of the intrusion detection algorithms proposed can be divided into two major categories: misuse detection algorithms (signature-based) and anomaly detection algorithms (behavior-based). The former can only detect specific attacks; the latter can detect more attacks but is not efficient (13). Hybrid intrusion detection mechanisms are the combination of both, but are difficult to achieve (14). From the perspective of wireless sensor networks data, Jianli Guo proposes a sensing data mining based intrusion detection algorithm and intrusion detection of abnormal sensory data from the network protocol, node type (15). Although this system solves the detection of a new hybrid heterogeneous network, detection efficiency is low. Zeyu Sun introduces a variety of wireless sensor networks key management scheme in-depth study and based on the design of a key pre-distribution scheme using a node identifier. However, his main concern is trust probability, not detection efficiency (16).Yun Wang analyzes the problem of intrusion detection in a Gaussian-distributed WSN by characterizing the detection probability with respect to the application requirements and the network parameters under both single-sensing detection and multiple-sensing detection scenarios(17). Who examines the effects of different network parameters on detection probability, but ignores the impact of the opening time of the node on the detection rate.

Once the sensor nodes are configured, the main function of the sensor is to obtain a single type of information. One of the characteristics of sensor networks is poor computing power, and energy consumption is a key indicator: reducing the energy consumption of the sensor is thus an urgent bottleneck problem (18; 19). In fact, there are many experts proposing a variety of methods to optimize energy efficiency for WSN (20; 21). Unfortunately, all those studies in the field of energy optimization have focused only on the operation of the sensor network, while ignoring the energy consumption of the intrusion detection itself (22). There is no doubt that one of the major problems WSNs face is energy (23). Battery power is the main energy source used by the sensor nodes, but a the battery's energy density is limited, impeding the normal operation of a sensor node. Hence, an energy-efficient sensor network would offer a significant benefit for carring out the work in such conditions, and our proposed schemes take energy consumption as the major consideration.

So far there are some proposed solutions that apply game theory to WSN security strategy in order to reduce energy consumption (24; 25). But most of them regard the game as a single process and assume that there is only one choice for the attacker (26). Instead, in the actual WSN environment there are always replay attacks, and the attack methods are more diversified (27; 28). For the purpose of balancing detection efficiency and the energy consumption of the system, our proposed scheme uses game theory to intelligently control the sensor network, adjust the configuration of the nodes in layout, and predict the next targeted cluster, and the attack time.

1.2. Our motivation and outline

With the development of communication technology, embedded technology, and the Internet of Things, the sensors are increasingly intelligent, miniaturized, and wireless networked. Meanwhile, the attacks on sensor networks are gradually becoming human or intelligent-controlled. In addition, a core problem of WSN is to effectively utilize the node energy and extend the lifetime of the network (29). In order to solve those problems, the design proposed in this paper has taken a comprehensive view of this issue by presenting an intelligent intrusion detection model based on game theory and an autoregressive model to minimize energy consumption. This model has been developed and improved to a non-cooperative complete information static game model. For this purpose, the network is divided into clusters using clustering routing protocols and a set of cluster head nodes (CHs) are systematically chosen. Hence only good quality nodes from the perspective of game theory are selected as CH to activate IDS. Ultimately a defense strategy is obtained, which can balance detection efficiency and the energy consumption of the system.

This paper is organized as follows. Section II is an overview of related game theory. Section III presents our model in detail. Section IV discusses the autoregressive (AR) model applied to mitigate the attack times. Finally, after the simulation test in section V, we summarize the paper in section VI.

2. Overview of related game theory

As a mathematical theory of confrontation research, game theory takes the predictive and actual behavior of the individual in the game into account (30). Individuals involved in the game process must choose the best plan based on their opponent's choices in order to achieve maximum interest. To explore how to take action under the corresponding reaction of other participants. We have identified several basic concepts of game theory: Participant, Information, Strategy space, Benefit, and Equilibrium.

Definition 1. *Participant is a decision-maker in the game, who takes reasonable actions to maximize benefits (or utility). Usually showed as* $i = 1, 2, \ldots, n$.

Definition 2. *Information refers to the information in the game process observed by the participants, which includes the number of participants, features and actions, etc.*

Definition 3. *Strategy space is an action taken by the participant in a specific time in reaction to the other participants' behavior.* S_i *is a particular strategy of participant* i*. The n-dimensional vector* $S = \{S_1, S_2, ..., S_n\}$ *is called a combined strategy.*

Definition 4. *Benefit is the deterministic or expected utility obtained under a specific combination of strategies. Utility usually shows the results (winning or losing), and must be expressed in terms of its size, where* U_i *is the benefit of participant* i*. If* $(S_1, S_2, ..., S_n)$ *is a combination of strategies, then the profit of every participant is* $U_i = U_i\ (S_1, S_2, ..., S_n)$*, where* $i = 1, 2, ..., n$.

Definition 5. *Equilibrium is the optimal strategy combination of all participants. It is expressed as* $S^* = (S_1^*, S_2^*, ..., S_n^*)$*, where* S_i^* *is the optimal strategy of participant* i*. It is a strategy for maximizing* U_i *in all possible strategies of participant* i.

Depending on whether there is a binding agreement among the participants, game theory can be divided into cooperative and non-cooperative. Cooperative game theory is not only more complex, but also far less considered than the non-cooperative game theory. For this reason, non-cooperative game theory has been widely adopted.

Various equilibrium concepts consist of different types and conditions of the game problem. Non-cooperative game equilibrium is also called Nash equilibrium. In the Nash equilibrium solution, any participant's decision is the optimal value relative to others. In this case, all participants maintain their chosen strategy and the equilibrium system. When the Nash equilibrium is reached, it does not mean that both sides of the game are in a state of immobility. In the sequential game, this equilibrium is reached in the continuous actions and reactions of the participants, called dynamic balance.

3. Intrusion detection model based on game theory

As compared to the computer smart networks, WSN has many resource constraints, such as memory, power, and processing power capabilities. Therefore it is vulnerable to special attacks, for instance sybil attack, hello flood attack, blackhole attack, and grayhole attacks(31). Younis have proposed a novel security attack known as snooze attack on cluster-based routing in WSN. Recently Qiong shi applied an the internal attack detection model as an epidemiological model(32). However most of these models ignore the game process between attackers and the

IDS. Actually attackers always attempt to damage the sensor network nodes in order to obtain the benefits; simultaneously the IDS will be activated to maintain the normal operation of the system. Obviously it is an opposed game process. On the one hand, attackers will pay a certain price in order to obtain certain profits. On the other hand, the IDS will consume energy to defend the system. As a result, we propose the game theory model to simulate the attack-defense process, and to identify the equilibrium solution between the attacker and IDS as a means of solving the problems of energy consumption and detection efficiency, as shown in **Fig. 1**.

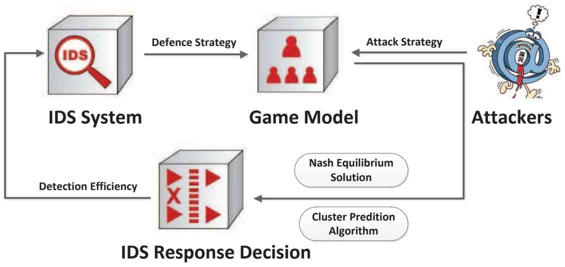


Fig. 1. Intrusion detection model based on game theory.

3.1. Model establishment

During the game process, there is no cooperation between the attacker and the IDS, so the non-cooperative game model is chosen. In addition, attackers and defenders may act again and again at random times. However, the latter actor knows nothing about the strategy of the former, and consequently it is a static game process. Furthermore, assuming that attackers and defenders have an accurate knowledge of each other's characteristics, strategy space and benefit function during the process; in other words, it conforms to complete information game theory. From what has been discussed above, we propose the non-cooperative complete information static game model.

The attack-defense model in WSN is composed of two participants: the attacker (A) and the defender (D). As explained above, information is fully perceptible for both participants. For the moment, the strategy space is recorded as S_A and S_D, and the benefit function is expressed as U_A and U_D. Moreover the equilibrium solution is deduced from these four parameters, and thus the game model is presented as $G = \{(D, A), (S_D, S_A), (U_D, U_A)\}$.

As a result of the energy limitation in WSN, the IDS can be activated for a limited number of nodes. Therefore, clustering routing protocols are applied to divide the network into clusters to balance the system's energy consumption and detection efficiency. Each cluster contains a number of member nodes and a CH that is periodically elected from the cluster nodes. The member nodes are in charge of collecting information and delivering it to CH, and CH is then responsible for transmitting the information and implementing the intrusion detection program. Finally, the base station (BS) controls the operation of the IDS in the CH.

Suppose that there are N nodes in the WSN, divided into k clusters as $C_1, C_2, ..., C_k$. C_i represents the number of nodes in each cluster, where $i = 1, 2, ..., k$. Only one cluster can be attacked during each attack, and BS can only select one CH to start the IDS. Then in each attack-defense process, the attacker has three strategies on cluster node C_i: attacking (A_1), waiting for time t and then attacking (A_2), or choosing a different cluster node C_j to attack (A_3), that is $S_A = \{A_1, A_2, A_3\}$. At the same time, there are three alterative strategies for the defender: protecting the cluster node $C_i(D_1)$, closing the IDS (D_2), or choosing a different cluster node $C_j(i \neq j)$ to protect (D_3), so $S_D = \{D_1, D_2, D_3\}$. After combining S_A and S_D we will obtain all of the combination strategies between the IDS and the attacker, as shown in the following matrix X.

$$X = \begin{bmatrix} (D_1, A_1) & (D_1, A_2) & (D_1, A_3) \\ (D_2, A_1) & (D_2, A_2) & (D_2, A_3) \\ (D_3, A_1) & (D_3, A_2) & (D_3, A_3) \end{bmatrix} \tag{1}$$

The rows and columns in the matrix (1) represent the options of the defender and attacker respectively, in order to determine the utility function, some signs need to be defined, as shown in **Table 1**.

Table 1
Sign and explanation

Sign	Explanation
U(t)	The utility of the normal operation at time t
Avg	The average value of each node
$C_i(t)$	The cost for protecting cluster C_i at time t
$V_i(t)$	The utility for successfully protecting cluster C_i at time t
$Q_i(t)$	The cost for attacking cluster node C_i at time t
$P_i(t)$	The utility for successfully attacking cluster C_i at time t
W(t)	The cost for waiting for next attack time
$S_A \& S_D$	The strategy space of the attacker and the defender.
$U_A \& U_D$	The benefit function of the attacker and the defender.
β	The average detection accuracy for new attacks by the anomaly method
α	The average detection accuracy for common attacks by the misuse method

$X_{11} = (D_1, A_1)$ indicates that both the attacker and the IDS choose the cluster node C_i. Suppose that in this case, the IDS can successfully detect the intrusion. As a result, the benefit and cost of the protection are $V_i(t)$ and $C_i(t)$; furthermore, the benefit $U(t)$ from normally operating the system should be considered. It is apparent that $U_D = U(t) + V_i(t) - C_i(t)$. Simultaneously the attacker must unsuccessfully attack, and the benefit and cost of the attack are respectively 0, $Q_i(t)$; that is, $U_A = -Q_i(t)$.

Ultimately, the benefit matrix Y, Z of the attacker and defender are shown as :

$$Y = \begin{bmatrix} -Q_i(t) & -W(t) & P_j(t) - Q_j(t) \\ P_i(t) - Q_i(t) & -W(t) & P_j(t) - Q_j(t) \\ P_i(t) - Q_i(t) & -W(t) & -Q_j(t) \end{bmatrix} \tag{2}$$

$$Z = \begin{bmatrix} U(t) + V_i(t) - C_i(t) & U(t) - C_i(t) & U(t) - C_i(t) - C_j * Avg \\ U(t) - C_i^{'} * Avg & U(t) & U(t) - C_j^{'} * Avg \\ U(t) - C_j(t) - C_i^{'} * Avg & U(t) - C_j(t) & U(t) + V_j(t) - C_j(t) \end{bmatrix} \tag{3}$$

Corresponding to matrix (1), the row and column in matrix (2) and (3) are the strategies chosen by IDS and the attacker, respectively.

In this case, the simplest way to find the Nash equilibrium solution is the scribing method for the bivariate utility matrix. The core idea is to find the optimal strategy for participant 1 in each column of the bivariate matrix and draw a line below the corresponding utility. Correspondingly, the optimal strategy for participant 2 is found in each row of the bivariate matrix, and underlined. Finally, if the two benefit values of a unit in the matrix are underlined, the corresponding strategy combination of the unit is a pure strategy Nash equilibrium solution of the game theory.

It is obvious that the revenue $P_i(t)$ obtained by successfully attacking cluster C_i is greater than the cost $Q_i(t)$; that is, $P_i(t) > Q_i(t)$. Otherwise, the attacker will be rational and give up attacking. The pure utility obtained by successfully attacking cluster C_i or C_j isn't much different in essence, which means that $P_i(t) - Q_i(t) \approx P_j(t) - Q_j(t)$. Thus, the maximum profits of the first, second, and third row are y_{13} and y_{21} (or y_{23}), and y_{31}.

The matrix Z is symmetric and revenue $V_i(t)$-obtained by successfully defending cluster C_i-is greater than the cost $C_i(t)$; therefore $V_i(t) > C_i(t)$. In the circumstances, the maximum profits of the first, second, and third column are Z_{11}, Z_{22}, and Z_{33}.

Since the subscript of the maximum profit in the two matrices (Y and Z) isn't exactly the same, we can draw the following conclusions:

Theorem 1. *There is no pure strategy Nash equilibrium in the game theory model.*

***Proof*.** The optimal solution for the attacker is assumed to attack the cluster node C_i. In this case, the defender will choose to guard cluster node C_i. Hence the attacker will reselect another attack strategy to obtain more benefits. As a result the system can't be stabilized, and there is no pure strategy Nash equilibrium in the game theory.

Theorem 2. *In order to obtain the maximum benefit, the attacker always chooses to attack.*

***Proof*.** Although there is no equilibrium solution, the maximum benefits of rows in the matrix Y are y_{13}, y_{21} (or y_{23}), and y_{31}. It is obvious that the column subscripts are 1 and 3; in other words, regardless of the strategy chosen by the defender, the attacker will always choose strategy A_1 or A_3 to maximize profit.

Different from the analysis of the convergence and stability of the system of equations by genetic algorithm(33). One of the advantages of the game theory is to find the equilibrium point in the dynamic process. When the system is in a steady state, both participants of the game choose the equilibrium strategy of utility called Nash equilibrium solution(34). The Nash equilibrium strategy describes the local static property of the equilibrium point, which is a local optimal concept rather than the global. Therefore, the Nash equilibrium is not guaranteed to be the fixed point with the highest detection rate or the least energy consumption, but means any participant's decision is the optimal value relative to others. In this case, all participants maintain their chosen strategy and the equilibrium system, which guarantees the convergence and the stability of solution.

3.2. Multiple attack detection model based on game theory

A misuse detection method may be an efficient way to detect most common attacks; however, that isn't applicable for new attacks, because their characteristics are unknown. As a result, we need to adopt an anomaly detection method. The characteristics of the data collected by the two methods are not the same. For a network suffering only one type of attack, collecting more data means more energy consumption, and gradually detecting each module can be costly and time consuming. Consequently, it is reasonable to coordinate the two detection methods and adopt one at each detection process. In this case we need to develop a strategy to make the IDS choose the optimal method at the right moment.

3.2.1. Model based on game theory

If the game model is recorded as G_1, the participants are still the attacker (A) and the defender (D). The attacker can select either the common means (A_1) or a new type of means (A_2). The defender can also either use the misuse detection method (D_1) or the anomaly detection method (D_2). Now the strategies of the defender and attacker are expressed as D_i and A_j, and each of their total benefit functions is defined as U_A and U_D. The terms $U_{ij}(D)$ and $U_{ij}(A)$ are the benefit of the defender and attacker respectively, when strategies (D_i) and (A_j) are chosen. Consequently the attack-defense game function can be described as: $G_1 = \{(D, A), (S_D, S_A), (U_D, U_A)\}$, where $S_D = \{D_1, D_2\}$, $S_A = \{A_1, A_2\}$. The strategy matrix for the game model is M, shown as following:

$$M = \begin{bmatrix} (D_1, A_1) & (D_1, A_2) \\ (D_2, A_1) & (D_2, A_2) \end{bmatrix} \tag{4}$$

Assume that the average detection accuracy for new attacks by the anomaly detection method is β and the average detection accuracy for common attacks by the misuse detection method is α . When $M_{11} = (D_1, A_1)$, the attacker chooses the common attack methods, and the defender adopts the misuse detection method. Then the detection accuracy is α, thus:

$$\begin{aligned} U_{11}(A) &= (1-\alpha)(P_i(t) - Q_i(t)) - \alpha Q_i(t) = (1-\alpha)P_i(t) - Q_i(t) \\ U_{11}(D) &= (1-\alpha)(U(t) - C_i(t) - C_i^{'} * Avg) + \alpha(U(t) - C_i(t)) \\ &= U(t) - C_i(t) - (1-\alpha)C_i^{'} * Avg. \end{aligned} \tag{5}$$

The benefit $P_i(t)$ obtained by attacking cluster i is equal to the cost $C_i' * Avg$; hence the defender's benefit can be simplified as:

$$U_{11}(D) = U(t) - C_i(t) - (1-\alpha)P_i(t). \tag{6}$$

Similarly, the other three sets of data can also be analyzed to obtain the bivariate utility matrix:

$$Y' = \begin{bmatrix} (1-\alpha)P_i(t) - Q_i(t) & P_i(t) - Q_i(t) \\ P_i(t) - Q_i(t) & (1-\beta)P_i(t) - Q_i(t) \end{bmatrix} \tag{7}$$

$$Z' = \begin{bmatrix} U(t) - C_i(t) - (1-\alpha)P_i(t) & U(t) - C_i(t) - P_i(t) \\ U(t) - C_i(t) - P_i(t) & U(t) - C_i(t) - (1-\beta)P_i(t) \end{bmatrix} \tag{8}$$

The matrices Y' and Z' represent separately the utility matrix of the attacker and the defender, in which rows and columns denote the attacker's and defender's strategies.

Suppose that the defender performs the misuse detection method and the anomaly detection method with probability p and $1-p$. Meanwhile the attacker adopts the common attack method and the new attack method with probability q and $1-q$. We try to obtain the value of (p, q) when the attacker and defender get the maximum benefit. According to the above bivariate utility matrix, we can gain the total benefit function U_D and U_A of the defender and attacker, where $(1-p)(1-q)$ is expressed as ε:

$$\begin{aligned} U_D &= p(1-q)U_{12}(D) + (1-p)qU_{21}(D) + pqU_{11}(D) + \varepsilon U_{22}(D) \\ U_A &= p(1-q)U_{12}(A) + (1-p)qU_{21}(A) + pqU_{11}(A) + \varepsilon U_{22}(A). \end{aligned} \tag{9}$$

$U_{ij}(D)$ and $U_{ij}(A)$ in the matrices Y' and Z' are brought into U_D and U_A:

$$\begin{aligned} U_D &= U(t) - C_i(t) - P_i(t)[1 - \alpha pq - \varepsilon\beta] \\ U_A &= [1 - \alpha pq - \varepsilon\beta]P_i(t) - Q_i(t). \end{aligned} \tag{10}$$

3.2.2. Analysis of Nash equilibrium solution

It is appropriate to look for the strategy that maximizes the U_D and U_A by the extreme method to make the utility function optimal.

In the defender's total utility function U_D, there are variables p, q, and the constants α, β, $U(t)$, $C_i(t)$, and $P_i(t)$. In order to maximize U_D, we calculate the partial derivative about p of U_D and q of U_A, then make them equal to 0:

$$\frac{\partial U_D}{\partial p} = [(\alpha + \beta)q - \beta]P_i(t) = 0. \tag{11}$$

$$\frac{\partial U_A}{\partial q} = [\beta - (\alpha + \beta)p]P_i(t) = 0. \tag{12}$$

Obtaining:

$$q = \frac{\beta}{\alpha + \beta}, p = \frac{\beta}{\alpha + \beta}. \tag{13}$$

Consequently, the strategy S_D and S_A are:

$$S_D = (p, 1-p) = (\frac{\beta}{\alpha+\beta}, \frac{\alpha}{\alpha+\beta}). \tag{14}$$

$$S_A = (q, 1-q) = (\frac{\beta}{\alpha+\beta}, \frac{\alpha}{\alpha+\beta}). \tag{15}$$

The defender's probabilities of adopting the misuse and the anomaly detection method in intrusion detection are $\frac{\beta}{\alpha+\beta}$ and $\frac{\alpha}{\alpha+\beta}$, respectively.

Accordingly, the attacker's probabilities of adopting the common and the new detection method are $\frac{\beta}{\alpha+\beta}$ and $\frac{\alpha}{\alpha+\beta}$, respectively.

In the equation (14) and (15), S_D and S_A are the Nash equilibrium solutions. When p and q are equal to the values, we obtain the maximum benefit of the attack and defender. Then, there is a simple analysis of the Nash equilibrium solution.

On the one hand, when α is a fixed value, the greater the β, and the greater the $p = q = \frac{\beta}{\alpha+\beta}$, which indicates that the detection accuracy of the anomaly detection method increases. Therefore, the attacker can be rational to reduce the probability of adopting a new attack method ($1 - q = \frac{\alpha}{\alpha+\beta}$). From the perspective of the defender, due to the attacker's new strategy, the probability of adopting the misuse detection method ($p = \frac{\beta}{\alpha+\beta}$) will increase.

On the other hand, when β is a fixed value, the greater the α, the smaller the $p = q = \frac{\beta}{\alpha+\beta}$. This indicates that the detection accuracy of the misuse detection method increases. So the attacker will avoid adopting a common attack (reducing q). It is the same for the defender, which reveals that our strategies are exactly in line.

The variables α and β are the detection rate of adopting the misuse and the anomaly detection method in the IDS, respectively. It is possible to use the misuse and the anomaly detection method based on the probability value ($\frac{\beta}{\alpha+\beta}$, $\frac{\alpha}{\alpha+\beta}$) to obtain the maximal benefit and reduce the energy consumption.

3.2.3. Model for multiple attack detection based on game theory

A network is divided into k clusters by the LEACH clustering algorithm(35). The basic idea is to reduce the energy consumption of the network and improve the lifetime of the network by randomly selecting the CH nodes and fairly distributing the energy load of the system. The proposed multiple attack detection game model combines game theory with the existing intrusion detection model to develop various intrusion detection strategies, as in the following algorithm:

1. Initializing the WSN, and setting the basic information of the node and the base station.
2. By the clustering protocol LEACH, the network is divided into k clusters. The base station sets the values of $U(t)$, Avg, $C_i(t)$, $V_i(t)$, $Q_i(t)$, $P_i(t)$, and $W(t)$ (see **Table 1**).
3. The base station will take these values into the corresponding formula above to construct first $U_{ij}(D)$ and $U_{ij}(A)$, then the utility matrices Y' and Z', where $1 \leq i, j \leq 2$.

4. The base station solves both utility matrices to determine whether or not there is a pure strategy Nash equilibrium solution. If it exists, jump to step 7; otherwise continue to step 5.
5. Inputting detection rate of each module (p and q).
6. Applying p and q, the mixed profits of the attacker U_D and the defender U_A are calculated to solve the mixed Nash equilibrium solution.
7. Depending on the solution, the base station starts the corresponding detection module for the intrusion detection.

4. Cluster prediction algorithm based on an autoregressive model

As mentioned above, activating our detection model on the cluster will consume energy and reduce the lifetime of the node. Consequently, it is necessary to both make the IDS energy efficient and maintain a high detection accuracy. This work has focused on accurately predict the attack time and target nodes. As a result, the IDS will start only on the target nodes at the time of the attack, thus saving energy and extending network lifetime.

4.1. Prediction of attack time

The time of an attack on the WSN is usually random. Consequently, in order to predict the attack time, the IDS needs to be started on all CHs for a short time in the beginning in order to obtain a certain amount of intrusion information and predict the next attack time.

Suppose that the n invasion is detected at this time: the time point is then denoted as T_1, T_2,..., $T_n(i, T_i)$. Therefore the least square method can be applied to fit the curve to approximately predict the attack time T_{i+1}.

In addition, the linear or the curve fitting is available to predict the attack time. Certainly we can choose the appropriate function in accordance with the fitting effect, then predict the next attack time T_{i+1}. In order to make our prediction more accurate, we set a confidence probability θ. Furthermore with the help of the mathematical properties of the confidence interval, we can calculate a threshold δ. Thus the confidence interval $(T_{i+1} - \delta, T_{i+1} + \delta)$ can cover the next attack time T_{i+1} with the confidence probability θ.

4.2. Prediction of the next targeted cluster

The attacker's target is a random choice; as a result we can build a prediction model based on the time series and make use of the existing finite data to predict the future value. There are several basic time series models to choose from: the autoregressive (AR) model, the moving average (MA) model, and the autoregressive moving average (ARMA) model (36).

As the linear regression model, the AR model uses the linear combination of random variables at a certain moment in the previous period to describe the random variables at a later time (37). In time series analysis, the MA model is a common approach for modeling univariate time series, which specifies that the output variable depends linearly on the current and various past values of a stochastic (imperfectly predictable) term (38). Finally, the ARMA model provides a parsimonious description of a (weakly) stationary stochastic process in terms of two polynomials, one for the AR and the second for the MA.

As mentioned earlier, in the beginning the IDS is started on all CHs for a period of time T to obtain the cluster attacked. According to these data, the AR model is employed to predict the next targeted cluster:

$$\overline{Z}_t = \phi_1 \overline{Z}_{t-1} + \phi_2 \overline{Z}_{t-2} + ... + \phi_p \overline{Z}_{t-p} + a_t, \tag{16}$$

where ϕ_1, ϕ_2,...,ϕ_p is called the autoregressive coefficient, and a_t is the white noise sequence whose mean and variance are zero and σ_a. Additionally, p represents the order of the model, which indicates that the value at the t moment depends only on the values of the previous p moments. Therefore the model (16) can also be called the AR (p) model. Obviously, the AR (1) model is:

$$\overline{Z}_t = \phi_1 \overline{Z}_{t-1} + a_t. \tag{17}$$

In order to establish the AR model, we need to make sure of the order and estimate the parameters. There are many kinds of standards to determine the order in an AR model. First of all, it can depend on the partial correlative coefficient and the autocorrelation coefficient. Second, the methods of mathematical statistics are useful for examining the residual or whether the confidence intervals of the parameters contain zero. Finally, the information criterion method is also available to determine the order by defining the characteristic function related to model order.

Currently, the most popular method in the AR model is the AIC criterion method, which is a kind of information criterion method. The criterion function of AIC is:

$$AIC = 2lg(Maximun\ likelihood\ of\ simulation)\ +\ 2(Paramters\ of\ the\ model). \tag{18}$$

The AIC criterion function of AR (p) model is:

$$AIC(p) = Nlg\sigma_a^2 + 2(p+1). \tag{19}$$

In formula (19) the smallest p is the order of the model; p can be determined by the AIC criterion method.

Moment estimation and least squares estimation are the most common methods for estimating the parameters of the AR model. A brief introduction to these techniques follows.

A) Moment estimation of parameters in the AR model.

In the AR model, an important characteristic of the observation sequence $x(t)$ is the trailing property of the autocorrelation function, that is:

$$R_k = \sum_{j=1}^{p} \phi_{pj} R_{k-j}, k > 0. \tag{20}$$

Where $k = 1, 2, ..., p$, equations are written as matrix:

$$\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_p \end{bmatrix} = \begin{bmatrix} R_0 & R_1 & R_2 & \dots & R_{p-1} \\ R_1 & R_0 & R_1 & \dots & R_{p-2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ R_{p-1} & R_{p-2} & R_{p-3} & \dots & R_0 \end{bmatrix} \begin{bmatrix} \phi_{p1} \\ \phi_{p2} \\ \vdots \\ \phi_{pp} \end{bmatrix} \tag{21}$$

The equation (21) is the famous Yule-Walker(Y-W) equation. If R_k in equation (21) is replaced by a moment estimator

$$\bar{R}_k = \bar{R}_{-k} = \frac{1}{N} \sum_{i=1}^{N-k} x_i x_{i+k}, \tag{22}$$

the Y-W estimate of $(\phi_{p1}, \phi_{p2}, ..., \phi_{pp})$ can be obtained by the positive definition of $\{\bar{R}_k\}$:

$$\begin{bmatrix} \bar{\phi}_{p1} \\ \bar{\phi}_{p2} \\ \vdots \\ \bar{\phi}_{pp} \end{bmatrix} = \begin{bmatrix} \bar{R}_0 & \bar{R}_1 & \bar{R}_2 & \dots & \bar{R}_{p-1} \\ \bar{R}_1 & \bar{R}_0 & \bar{R}_1 & \dots & \bar{R}_{p-2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \bar{R}_{p-1} & \bar{R}_{p-2} & \bar{R}_{p-3} & \dots & \bar{R}_0 \end{bmatrix}^{-1} \begin{bmatrix} \bar{R}_1 \\ \bar{R}_2 \\ \vdots \\ \bar{R}_p \end{bmatrix} \tag{23}$$

The moment estimation of the variance $\sigma_a^2(p)$ about residual sequence $\{a_t\}$ in the AR (p) model is:

$$\sigma_a^2(p) = E(\bar{a}_t^2) = \bar{R}_0 - \sum_{j=1}^{p} \bar{\phi}_{pj} \bar{R}_j. \tag{24}$$

The parameters of the model (24) can be solved by taking the known data from the sequence into the formula.

B) Least squares estimation.

With the help of the least squares method, the least squares estimation is applied to estimate the parameters of the the AR (p) model. Thus we can obtain the residual function shown as:

$$L(\phi) = \sum_{t=p+1}^{N} a_t^2 = \sum_{t=p+1}^{N} (\bar{Z}_t - \phi_1 \bar{Z}_{t-1} - \phi_2 \bar{Z}_{t-2} - ... - \phi_p \bar{Z}_{t-p})^2. \tag{25}$$

According to the principle of least squares, we explore the partial derivative of the formula (25) and make it equal to zero:

$$\bar{\phi} = \begin{bmatrix} \bar{\phi}_1 \\ \bar{\phi}_2 \\ \vdots \\ \bar{\phi}_p \end{bmatrix} = \begin{bmatrix} \bar{r}_{11} & \bar{r}_{12} & \dots & \bar{r}_{1p} \\ \bar{r}_{21} & \bar{r}_{22} & \dots & \bar{r}_{2p} \\ \vdots & \vdots & \dots & \vdots \\ \bar{r}_{p1} & \bar{r}_{p2} & \dots & \bar{r}_{pp} \end{bmatrix}^{-1} \begin{bmatrix} \bar{r}_{01} \\ \bar{r}_{02} \\ \vdots \\ \bar{r}_{0p} \end{bmatrix} \tag{26}$$

$$\bar{\sigma}_a^2 = \frac{1}{N-p} \sum_{t=p+1}^{N} (\bar{a}_t)^2. \tag{27}$$

After the order and parameters in the AR (p) model are estimated, we can completely establish our prediction model and provide guidance for IDS. The numbers of CH are positive integers, but the results predicted by the AR (p) model are usually fractional, so the result is rounded down.

4.3. The cluster prediction algorithm of the autoregressive model

The cluster prediction algorithm of the autoregressive model is a combination of the time of the attack and the prediction of the attacked cluster. The least squares method is useful for making a rough estimation of the attack time, and the credibility of the prediction time is increased by introducing the confidence probability. In addition, the AR model is applied to predict the target cluster. The algorithm contains the following main steps:

1. The WSN is initialized, and the basic information of the node and the base station is set.
2. With the clustering protocol LEACH, the network is divided into k clusters; θ is the confidence probability of the attack time.
3. In the beginning, the IDS in all CHs are activated within a period T to obtain attack records (i, T_i, K_i).
4. The least squares method is used to deploy the polynomial fit for (i, T_i), and the confidence probability α is set, to approximately calculate threshold δ in order to determine the next attack interval $(T_{i+1} - \delta, T_{i+1} + \delta)$.
5. Using the AIC criterion or the partial autocorrelation function and the autocorrelation function of the time series (i, K_i), the order p of the sequence is determined.
6. The Yule-Walker formula is used to develop moment estimation of parameters in the AR (p) model, and the parameters are obtained.
7. Based on the results of Step 5 and 6, the AR (p) model is determined to predict the next attacked cluster.

Combining the prediction results of Step 4 and 7, the IDS is activated in the corresponding cluster to protect the system. The above steps are implemented with pseudo-code, shown in **Table 2**.

5. Simulation experiment and analysis

In reality, the current sensor network is still in an initial stage of construction, and a large-scale physical test is difficult to perform. The strategy of IDS proposed in this paper not only focuses on the configuration of the nodes in layout and the prediction of the next targeted

Table 2
Pseudo code of autoregression cluster prediction algorithm.

```
$Init\_NetWork()$
$AR\_Forecast(T, a)$
$\{$
    $while(t < T)$
        $switch\_on\_all()$
        $Record\_Information(i, T_i, K_i)$
        $Increase(t)$
    $b = Least\_Squares(i, T_i, a)$
    $p = Partial\_auto\_func(i, K_i)\&\&Autocorr\_func(i, K_i)$
        $\|AIC\_func(i, K_i)$
    $Yule\_Walker(i, k_i)\|Max\_like\_Estimate(i, K_i)$
    $predict\_n = AR\_Calculate()$
    $Intrusion\_Detection\_Start(a, b, predict\_n)$
$\}$
```

cluster to activate IDS, but also simplifies the data analysis processing. There are many types of sensors. In order to highlight the general type of the paper, we chose Xiaomi phone as the sensor platform. The phone contains: distance sensor, fingerprint sensor, position sensor, image sensor, barometric sensor, and inertial sensor; which can set three-dimensional coordinates and provide specific location information. In addition, these data could be directly obtained from the built-in sensor of Xiaomi phone through the sensor interface function SensorUDP in MATLAB. That was operable, easy to track and adjust.

5.1. Simulation experiment

To simulate the simplicity and contingency of actual WSN intrusion, the intrusion was regarded as a simple data transformation function. In addition, it was designed as a single process to reflect the traces of intrusion (such as: data is converted to a specific number); and it was the same that the detection was designed as another separate process. The purpose of this design is mainly to realize the acquisition and differentiation of the running time of the process; that is a direct indicator of energy consumption. Intrusion and detection functions were installed on each phone, but the functions of trigger and running times were adjustable according to the actual experimental condition. The operation of the experimental program alone can't reflect the game idea, but it could not always simulate the program with manual interference, so the random function was introduced in the simulation program.

In the simulation of intrusion and detection location, we set up 4 groups, each group was regarded as a cluster, there were 5 Xiaomi phones; simulation detections were divided into CH detections and ordinary phone detections.

In the simulation of intrusion and detection time, the experimental operation time could be adjusted manually according to the game theory. For example, running once every 5 minutes and running for 30 seconds.

The above two simulations weren't measured simultaneously. When measuring the intrusion and detection time, the simulation experiment was performed in the same mobile phone, and the running time was used as a direct quantitative indicator of energy consumption. When measuring the intrusion and detection location, 5 mobile phones of each group were randomly running according to the game theory in the simulation experiment.

There were 100 sensor nodes randomly deployed in a selected area of 100 $*$ 100 square meters. All of their initial energy was set to 0.5 J, except for the BS located in the center, which had no energy restriction. Although the actual energy consumption of the sensors isn't easy to detect, we assumed that the energy consumption was the same due to the same property. With LEACH clustering algorithm, CHs were randomly selected with a probability of 0.1, so there were 10 cluster head nodes in the whole network. The simulation parameters are shown in **Table 3**.

Table 3
Simulative experimental parameters

Parameter	Value
Size of detection area/m	100^2
Number of sensor nodes	100
Location of base station/m	(50,50)
Network Clustering Protocol	LEACH
Probability of the node elected as CH	0.1
Whether can the node move	no
Initial energy of node/J	0.5
The unit energy consumption of data transmission $E_{elec}(nJ/bit)$	50
Consumption parameter of free-space channel model $E_{fs}pJ(bit \times m^2)$	10
Consumption parameter of multipath fading channel model $E_{mp}pJ(bit \times m^2)$	0.013

Fig. 2 shows the network structure of the MATLAB simulation. Suppose that only one cluster can be attacked in a time unit. To simulate the attack, a malicious node was appended to the network, and randomly sent data packets. The cluster receiving these data was considered under attack. We divided the packets into two types, depending on their length: the shorter packets represent the common attacks; the longer packets represent the new attacks.

According to game theory, the attacker acts in each time gap to obtain the maximum benefit. In actuality, the network was randomly attacked, and the time for each simulation experiment was set to 10 minutes divided into 50 intervals. At the beginning of the simulation, the IDS in all cluster heads was started to record the attack data during this time. Then, we applied the AR model to predict the next target node, as shown in **Fig. 3**.

In **Fig. 3** the previous 20 attacks were history records that were analyzed and processed with the AR model to predict the next target cluster. Similarly, we can extract the time sequence

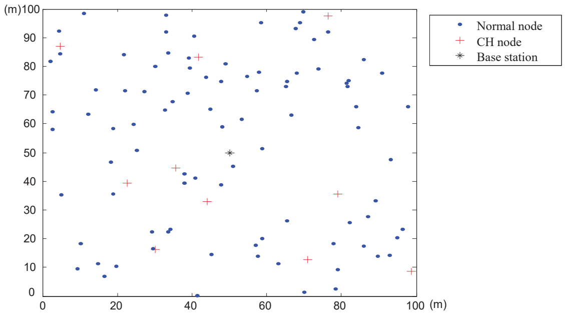


Fig. 2. Randomly distributed nodes in a cluster network by the MATLAB simulation. The CH nodes selected by the LEACH clustering protocol are denoted by a red plus sign; the common nodes are represented by blue solid dots; the base station is indicated by a black asterisk, which is located at the center of the whole network. It can send control information to the CHs.

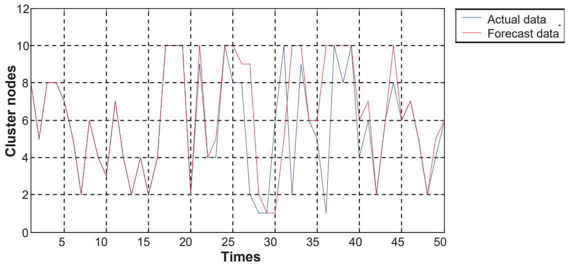


Fig. 3. Cluster prediction algorithm based on AR model. The abscissa is the number of attacks; the ordinate is the cluster number.

of the attack time points. The fitting curve is shown as **Fig. 4**.

In **Fig. 4**, we can learn that the quadratic curve fitting is utilized from the degree value in the figure. There is a confidence curve on both sides of the fitting curve. The parameter passed in the polytool function is 0.05, so the confidence interval of the curve is 95%. This means that 95% of the data falls between the two lines. In additon, the size of the interval is 4.9331, so that the time interval $a\pm$ 4.9331 will contain the real attack time point with a 95% confidence rate, where a is the prediction value.

It is assumed that the detection rate of the misuse detection module and the abnormal intrusion detection module are both 0.9. According to the improved game model, the IDS should be started with the probability of (0.5, 0.5), then the simulation should be run.

In order to obtain more convincing results, intrusion detection algorithms used for traffic prediction and CH surveillance are introduced to carry on the contrast experiment under the same conditions. The basic idea of the traffic prediction algorithm is to protect cluster nodes with the largest flow. The basic idea of CH surveillance is to start the IDS on all the cluster head nodes.

According to **Fig. 5**, the attack-defense model built with the game theory is more stable, because the detection rate is about 75%, compared to the detection rate of the model built

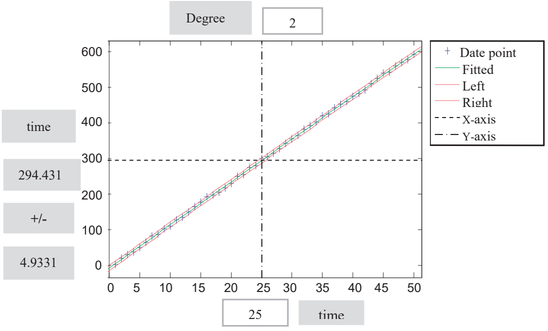


Fig. 4. Time curve fitting to extract the time sequence of the attack time points. The blue plus sign is the time point for the network attacker to attack; the green curve is the fitting curve.

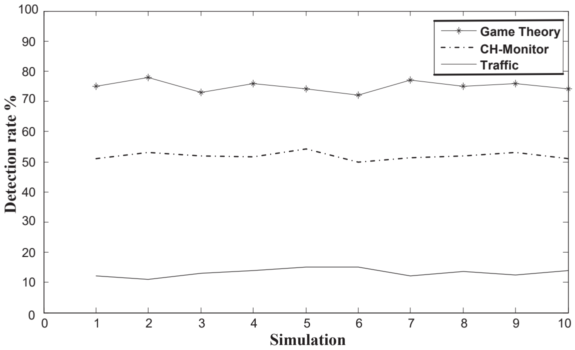


Fig. 5. Comparison of intrusion detection rate of each intrusion detection algorithm. Shows the intrusion detection rate of each intrusion detection algorithm under the ideal conditions

with the CH detection algorithm, which is about only 50%. The main reason for this difference is that starting IDS on all cluster nodes consumes more energy, which affects overall detection efficiency; there is no way to specify the start order of the detection modules, so they can only be randomly operated at equal probability. According to the general consensus (14), the detection accuracy of the intrusion detection algorithm based on traffic is about 15%, because there is no necessary connection between the traffic volume in the cluster and the attacker's choice.

Consequently, the intrusion detection algorithm based on game theory provides a high detection rate and ensures that the WSN network can be safely used in a more complex network environment.

5.2. Assessment for energy

Some energy consumption models monitor several performance counters related to the CPU in order to estimate power consumption (18). Zhang et al. validate that energy usage of an application is directly related to the amount of CPU time it uses (19). Our paper focuses on critical power and regards running time as the main indicator of energy consumption of the system. In order to reduce energy consumption errors due to not directly considering loads handled by I/O devices and multi-core processing, each family of machines was equipped with a similar hardware configuration in our experiment.

The energy consumption was based on the running time of the process. For example, in the simulation of intrusion and detection time, the experiment run every five minutes; then the energy consumption ratio was: $30s/5 * 60s = 1/10$.

After accumulating times of each group, the total energy consumption ratio was obtained:

$$\sum_{i=1}^{20} \frac{30(s)}{x_i * 60(s)}; \tag{28}$$

where x_i respected the running time interval of each cell phone.

Suppose that there are N nodes in a WSN, the total time deployed in the monitoring area is T, and the energy consumption for each node in per unit time is μ. When the IDS is started on all nodes, the energy consumption is:

$$p_1 = \mu NT. \tag{29}$$

At this point, the clustering protocol LEACH is adopted to divide the network into K clusters, the IDS is started in real time in the CH, and the energy consumption is:

$$p_2 = \mu KT. \tag{30}$$

The time T is equally divided into n time slots $T_1, T_2, ..., T_n$. Because certain historical data is necessary to predict the next attack, the IDS is fully operated for a period in the beginning. Afterwards, the error threshold δ of the attack time can be calculated under the confidence probability $\alpha\%$. The energy consumption of the system is:

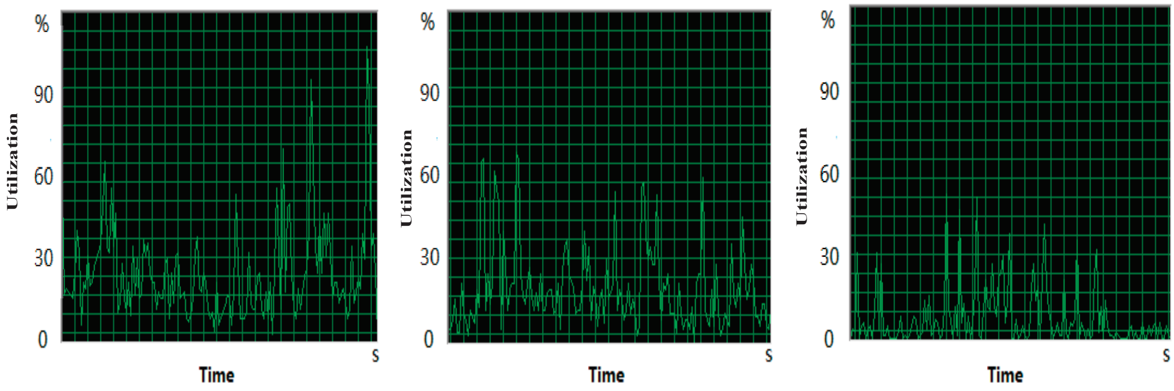
$$p_3 = \mu(KT^{'} + 2\delta n(1 - \frac{T^{'}}{T})). \tag{31}$$

In this simulation experiment, there were $N = 100$ nodes in the WSN, and the monitoring time was $T = 10min$. Furthermore, the probability of selecting cluster nodes to be CH was set to 0.1 by the LEACH clustering algorithm, so the number of CH was $K = 100 * 0.1 = 10$. Moreover, we divided the monitor time into $n = 50$ gaps, then took the data from the first 20 intrusions as historical data to calculate the error threshold 4.9331, containing real intrusion time points with 95% confidence ratio. Specifically, the consumption energy μ of per node in per unit time was almost identical in all three cases. Finally, taking the values into the formula above, $p_2/p_1 = 0.1, p_3/p_2 = 0.4491$.

It is worth mentioning that the energy consumption ratio is not fixed, because the configuration of the nodes in layout, the prediction of the next targeted cluster to activate IDS, the experimental operation time, and the running time interval will change according to the status of the simulation. This also reflects the dynamic balance when the game model reaches Nash equilibrium.

As a result, the cluster-based intrusion detection algorithm consumed about 90% less energy than the node-based algorithm under the same conditions. Nevertheless, the intrusion detection algorithm based on game theory and the autoregressive model proposed in this paper performed even better than the existing cluster-based detection algorithm, whose energy consumption was only about 55% less than the node-based approach.

In the simulation experiment, the running time of the process is regarded as the main indicator of energy consumption of the system. **Fig. 6** contrasts energy consumption of the system under the same conditions. Therefore, in the case of the same initial energy, the lower the running time is, the lower the energy consumption is. It is worth noting that the additional energy consumption due to the cluster partition protocol and the IDS's failure is negligible.



(a) Start on all nodes. (b)CH detection. (c)Game theory model.

Fig. 6. Utilization of CPU.

From **Fig. 6**, under the same experimental environment, the running time (used as a proxy for the energy consumption of the WSN adopting an intrusion detection model based on game theory and an autoregressive model) is significantly lower than that based on a CH detection algorithm and a scenario where the IDS is started on all nodes.

6. Conclusions

For the purpose of reducing energy consumption, this paper proposed an intrusion detection model for a wireless sensor network based on game theory and an autoregressive model, in which the attack-defense process between the IDS and the attacker is viewed as a non-cooperative game model. Furthermore, the autoregressive theory game model (AR) was established and applied to improve on a non-cooperative information static game model that was being applied to predict attack times. In addition, by analyzing the model's mixed Nash equilibrium solution, the optimal defense strategy that could balance the detection efficiency and energy consumption of the system was obtained. In the simulation experiment, the running time of the process is regarded as the main indicator of energy consumption of the system. The simulation results show that the game model can not only effectively predict the attack time and the next targeted cluster based on the game theory, but also reduce energy consumption.

Game theory also provides new feasible ideas and technologies to address essential problems in WSN security, a significant and promising direction for future research.

7. Acknowledgments

This paper is supported by National Natural Science Fund NSF: 61272033 & 61572222.

References

[1] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov (2015) Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications, IEEE Access, 3, 1503-1511.

[2] Arcangelo Castiglione, Paolo DArco, Alfredo De Santis, Rosario Russo (2017) Secure group communication schemes for dynamic heterogeneous distributed computing, Future Generation Computer Systems, 74, 313-324.

[3] Perrig, A., Stankovic, J. and Wagner, D. (2009) Security in wireless sensor networks, Computer Communications and Networks, Springer, London. 47(6), 53-57.

[4] Pei, Q., Shen, Y.L. and Ma, J. (2007) A survey of wireless sensor network security technology, Journal of communication science, 28.

[5] Ping, Y., Hao, X.J. and Yue, W. (2008) Distributed intrusion detection for mobile ad hoc networks, Journal of Systems Engineering and Electronics, 19, 851C859.

[6] Daniele, M., Salmin, S. and Elisa B. (2012) A System for Response and Prevention of Security Incidents in Wireless Sensor Networks, SenSys' 14 Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, 148-162.

[7] Zhu, S.C., Setia, S.J. and Jajodia, S. (2006) LEAP:Efficient security mechanisms for large-scale distributed sensor networks, Acm Transactions on Sensor Networks, 2, 500-528.

[8] Liao, H.J. and Lin C.H. (2013) Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, 36, 16-24.

[9] Krontiris, L., Dimitriou, T. and Freiling, F.C. (2007) Towards intrusion detection in wireless sensor networks, Proceedings of the 13th European Wireless Conference, Paris, France, April

[10] Geetha, V. and Chandrasekaran, K. (2014) A Distributed Trust Based Secure Communication Framework for Wireless Sensor, Network.Wireless Sensor Network, 6, 173-183.

[11] Anhtuan, L., Jonathan, L. and Aboubaker, L. (2012) 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach, International Journal of Communication Systems, 25, 1189-1212.

[12] Cramer M L (2001) New methods of intrusion detection using control-loop measurement.

[13] Kavitha, T. and Sridharan, D. (2002) Security vulnerabilities in wireless sensor networks: A survey, Journal of information Assurance and Security, 38, 393-422.

[14] Yan, K.Q., Wang, S.C. and Liu, C.W. (2009) A hybrid intrusion detection system of wireless sensor networks, Proceeding of the International Multi Conference of Engineers and Computer Scientists, 1, 18-20.

[15] Hu X, Bai R (2011) Research on intrusion detection model of wireless sensor network, International Conference on Computer Science and Service System. 3471-3474.

[16] Sun Z, Li L, Li X (2016) Research on intrusion detection technology based on nodes optimization deployment in wireless sensor networks, International Journal of Security & Its Applications, 10(8), 159-172.

[17] Wang Y, Fu W, Agrawal D P (2013) Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks, IEEE Press, 24,342 - 355.

[18] Marcelloni F, Vecchio M (2010) Enabling energy-efficient and lossy-aware data compression in wireless sensor networks by multi-objective evolutionary optimization, Information Sciences, 180, 1924-1941.

[19] X. zhang, L. Jian-Jun, X. Qin (2013) A high-level energy consumption model for heterogeneous data centers, Simulation Modelling Practice and Theory, 39, 41-55.

[20] H. Lu, J. Li and M. Guizani (2014) Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 25, 750-761.

[21] Xu L, Chen G, and Cao J (2015) Optimizing Energy Efficiency for Minimum Latency Broadcast in Low-Duty-Cycle Sensor Networks, ACM Transactions on Sensor Networks, 11(4), 57.

[22] Arcangelo Castiglione, Francesco Palmieri, Ugo Fiore (2015) Modeling energy-efficient secure communications in multi-mode wireless mobile devices, Computer and System Sciences, 81, 1464-1478.

[23] A. Castiglione, A. D. Santis, A. Castiglione, F. Palmieri and U. Fiore (2013) An Energy-Aware Framework for Reliable and Secure End-to-End Ubiquitous Data Communications, 2013 5th International Conference on Intelligent Networking and Collaborative Systems, 157-165.

[24] Chi-Ming Wong, Chih-Fong Chang, Bih-Hwang Lee (2013) A Simple Time Shift Scheme for Beacon Broadcasting Based on Cluster-Tree IEEE 802.15.4 Low-Rate WPANs, Wireless Personal Communications, 72(4), 2837-2848.

[25] Hossein, J. (2011) Designing an Agent-Based Intrusion Detection System for Heterogeneous Wireless Sensor Networks: Robust, Fault Tolerant and Dynamic Reconfigurable, Int. J. Communications, Network and System Sciences, 4, 523-543.

[26] A. A K S, Ovsthus K, Kristensen L M (2014) An Industrial Perspective on Wireless Sensor Networks A Survey of Requirements, Protocols, and Challenges, IEEE Communications Surveys & Tutorials, 16(3), 1391-1412.

[27] Akyildiz, I.F., Su, W. and Sankarasubramaniam, Y. (2002) Wireless sensor networks: a survey, Computer networks, 38, 393-422.

[28] Al-Karaki, J.N. and Kamal, A.E. (2004) Routing techniques in WSN: a survey, IEEE Journal of Wireless communications, 11, 6-28.

[29] Z.Haiying, L.Danyan, G.Yan, De-Cheng (2011) Modeling of Node Energy Consumption for Wireless Sensor Networks, Wireless Sensor Network, 3(1), 18-23.

[30] Sha K, Gehlot J, Greve R (2013) Multipath Routing Techniques in Wireless Sensor Networks: A Survey, Wireless Personal Communications, 70(2), 807-829.

[31] Muhammad Saleem, Israr Ullah, and Muddassar Farooq (2012) An energy-efficient and scalable routing protocol for wireless sensor networks, Information Sciences, 200, 38-56.

[32] Qiong Shi, Li Qin, Lipeng Song, Rongping Zhang, and Yanfeng Jia (2017) A Dynamic Programming Model for Internal Attack Detection in Wireless Sensor Networks, Discrete Dynamics in Nature and Society, 3, 9.

[33] Arqub O A, Abo-Hammour Z (2014) Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm, Information Sciences, 279, 396-415.

[34] Hart S (2008) Nash Equilibrium and Dynamics, Simple Adaptive Strategies:From Regret-Matching to Uncoupled Dynamics, 289-293.

[35] RI Tandel (2016) Leach Protocol in Wireless Sensor Network: A Survey, International Journal of Computer Science and Information Technologies, 7(4), 1894-1896.

[36] Mehdi Khashei, Farimah Mokhatab Rafiei, Mehdi Bijari (2013) Hybrid Fuzzy Auto-Regressive Integrated Moving Average (FARIMAH) Model for Forecasting the Foreign Exchange Markets, International Journal of Computational Intelligence Systems, 6(5), 954-968.

[37] Singh Pushpendra, Joshi Shiv Dutt (2017) Appendix A from The Fourier decomposition method for nonlinear and non-stationary time series analysis, The Royal Society,

[38] TAKATA Soichiro, KINOSHITA Shohei, Kumura Takahiro (2016) Asymmetric nonlinear system identification using auto regressive time series analysis, The Proceedings of the Dynamics & Design Conference, 142.