Intrusion Detection System for IoT Heterogeneous Perceptual Network Based on Game Theory

Man Zhou, Lansheng Han(✉), Hongwei Lu, and Cai Fu

School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan, China
{zhou_man,hanlansheng,luhw,fucai}@hust.edu.cn

Abstract. With the acceleration of the Internet of things (IoT) construction, the security and energy consumption of IoT will become an import factor restricting the overall development of the IoT. In order to reduce the energy consumption of the IoT heterogeneous perceptual network in the attack-defense process, the placement strategy of the intrusion detection system (IDS) described in this paper is to place the IDS on the cluster head nodes selected by the clustering algorithm called ULEACH, which we have proposed in this paper. Furthermore, by applying modified particle swarm optimization, the optimal defense strategy is obtained. Finally, the experiment results show that proposed strategy not only effectively detects multiple network attacks, but also reduces energy consumption.

Keywords: IoT security · Particle swarm optimization · Energy consumption · Intrusion detection system · Game model

1 Introduction

1.1 Current Research and Motivation

As the Internet of things (IoT) develops rapidly, its security faces serious challenges [2]. One of the major problems the perceptual layer of IoT faces is energy consumption [3]. In fact, many experts are currently proposing a variety of methods to optimize energy efficiency for the IoT [10]. Ozger [12] has proposed a totally new networking architecture, namely, Energy Harvesting Cognitive Radio Networking for Internet of Things-enabled Smart Grid. Luo [9] has analyzed energy consumption model and data relay model in WSN-based IoT, and then proposed the concept of "equivalent node" to select relay node for optimal data transmission and energy conservation. Unfortunately, all those studies in the field of energy optimization have focused only on the operation of the IoT system, while ignoring the energy consumption of the intrusion detection itself [1].

Most of the intrusion detection algorithms proposed can be divided into two categories: misuse detection algorithms (signature-based) and anomaly detection

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 459–471, 2019.
https://doi.org/10.1007/978-3-030-21373-2_37

algorithms (behavior-based) [7]. Sedjelmaci has designed a new framework for intrusion detection in cluster-based wireless sensor networks (CWSN) [15]. In CWSN, all sensor nodes were clustered, and a cluster head (CH) was elected to manage the operation of its own cluster. However, those proposed hybrid technologies simultaneously activate intrusion detection on low energy IoT devices, and reduce the network performance.

To date, some proposed solutions have applied game theory to IoT security strategy in order to reduce energy consumption [8]. Senouci has proposed a game theoretic technique to activate anomaly detection technique only when a new attack's signature was expected to occur [14]. For the purpose of reducing energy consumption and ensuring high efficiency, Han has proposed an intrusion detection model based on game theory and an autoregressive model. Most of those papers do not consider the dynamic change of both parties' decision in the game process when solving the equilibrium solution of the model. As a result, we apply modified particle swarm optimization (PSO) to obtain model's mixed Nash equilibrium solution. As one of the most representative methods, PSO aims to generate computational intelligence by simulating collective behavior in nature. Therefore, it has the advantages of simple implementation, good performance and fast convergence speed.

1.2 IoT

IoT service systems are aimed at monitoring and controlling the behavior of the physical world using a vast interlinked network of devices such as sensors, gateways, switches, routers, computing resources, applications or services, and humans to link the digital world with the physical. Considering the technical architecture of the IoT, which could be divided into three layers: the perceptual layer, the network layer, and the application layer, as shown in Fig. 1.

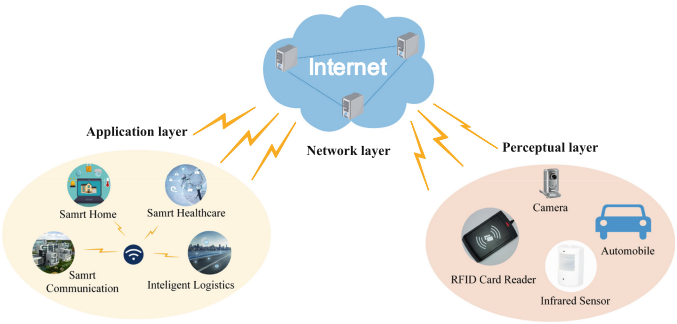


Fig. 1. The architecture of the IoT

The perceptual layer uses multiple sensors, sensor network, RFID, QR code and cameras, etc. to comprehensively sense physical world information. The layer

mainly deals with information recognized and collected by the sensing devices. The collected information is then securely transmitted to the upper layer through the network layer to achieve remote control or direct communication between objects. The nodes of the perceptual layer are heterogeneous and simple. They have limited computing and storage capabilities and carry less energy, and often in an unattended environment without effective monitoring, which makes them more vulnerable.

With the increase in the number of IoT applications, the problem of cross-coverage of multiple networks has become an increasingly prominent issue. The perceptual layer of the IoT is composed of multiple heterogeneous nodes, and the performance of the nodes and density differ among themselves. In addition, a large number of sensor nodes are deployed in different scenarios and are responsible for collecting various information. There is also a great difference in energy consumption between nodes. Therefore, it is necessary to balance energy consumption of nodes and take comprehensive consideration of the nodes' heterogeneity to improve the traditional technology, and thus improve the quality and effectiveness of communications.

In terms of a single network, the Internet, mobile communication, etc. have established some effective mechanisms, but the research on the perceptual layer of the IoT is still in the initial stage. There are more and more attacks on the perceptual layer, including physical attacks, forgery, resource exhaustion attacks, privacy leakage threats and so on. At the same time, the communication capability, storage capacity, energy consumption rate, and residual energy of the nodes in the perceptual layer are diverse. For the purpose of balancing detection efficiency and the energy consumption of the IDS in heterogeneous perceptual network, we place the IDS on the CHs selected by proposed clustering algorithm ULEACH. Then build dynamic intrusion detection model and apply modified particle swarm optimization to obtain optimal defense strategy.

2 Non-uniform Clustering Algorithm ULEACH

Clustering improves the network lifetime and stability period and efficiently helps in solving congestion and collusion that have high drainage effect of the energy. CH aggregates and access as a relay by having the data from the members and send it to the BS. If a node with small density is selected as a CH, the network energy will be quickly depleted and the network will become paralyzed. In order to select the optimal CH and improve the utilization of the node, this paper improves the original LEACH protocol [6], and proposes a new clustering algorithm ULEACH which is suitable for the heterogeneous perceptual layer of the IoT.

In order to fully analyze the heterogeneity of the perceptual layer network, we define the following concepts and provide calculation formulas:

Definition 1 ***Residual energy.*** *In the first round of the data transmission step, a node reports its own position information and the current residual energy*

E_{re} *to the Sink node, and the Sink node then calculates the average residual energy* $\overline{E_{re}}$ *of all nodes in the collection based on the received information. If* E_{re} *is lower than* $\overline{E_{re}}$*, it is ineligible to be a candidate CH. In the second round, in order to reduce the node's traffic, all nodes in the network send only their own current energy information to the Sink node and no longer send location information.*

Definition 2 ***Energy consumption rate.*** *The energy consumption rate represents the average energy consumption per round of the node and reflects the energy consumption during the operation. In fact, if a node is repeatedly selected as a CH, its average energy consumption is relatively high. Therefore, in the CH selection algorithm, the probability that a node with a higher energy consumption rate would be selected as a CH is smaller so as to maintain a balanced distribution of loads in the network. The energy consumption rate is evaluated as:*

$$E_R = \frac{E_{init} - E_{re}}{r - 1}, \tag{1}$$

where E_{init} *represents the initial energy of the node. Based on the information it receives, Sink node will calculate the average energy consumption* $\overline{E_R}$ *of all the nodes. If* $\overline{E_R}$ *is lower than* E_R*, it is ineligible to be a candidate CH.*

Definition 3 ***Overall performance.*** *The overall performance of the perceptual layer node includes both the communication and storage capabilities. The data transmission capabilities of different types are distinct, and the heterogeneous communication capability is mainly manifested in the data transmission rate. The specific formula is as follows:*

$$B_c = (a * V_c + b * R_c) \triangle t_1, \tag{2}$$

where B_c*,* V_c*,* R_c*, and* $\triangle t_1$ *respectively indicate communication capability, the transmission rate of heterogeneous data, the transmission rate of homogeneous data, and a period of time. Furthermore, a,b is the ratio of homogeneous and heterogeneous nodes.*

The data processing is another important part of the node, and different monitoring application scenarios require different data processing capabilities. CHs possess greater data storage capabilities and stronger data fusion capabilities: that is, CHs generally player a more important role in the perceptual layer network. Therefore, the heterogeneous storage power includes both the data storage speed and the storage capacity and is calculated as follows:

$$B_s = T_s + \triangle t_2 * (a * V_s + b * R_s), \tag{3}$$

where B_s*,* T_s*,* V_s*,* R_s*, and* $\triangle t_2$ *respectively represent the storage power, the total storage capacity, the storage speed of heterogeneous data, the storage speed of homogeneous data, and a period of time.*

Combining both the communication capabilities Eq. (2) and storage capabilities Eq. (3), the overall performance of the perceptual layer nodes is defined as Eq. (4), where B and ξ_1 express the overall performance and the influence of communication capabilities on the overall performance, respectively.

$$B = \xi_1 * B_c + (1 - \xi_1) * B_s \tag{4}$$

In summary, for the purpose of maintaining the performance of the network, the nodes selected as CHs must possess the following characteristics: the residual energy is greater than the average energy of all nodes; the energy consumption rate is lower than the average energy consumption rate of all nodes; and overall performance is higher. Therefore, $P_i(t)$ of the LEACH clustering protocol [6] is adjusted as $P_i(t_{iso})$.

$$P_i(t_{iso}) = \begin{cases} \frac{p_{iso}}{1 - p_{iso} \times (r \bmod (1/p_{iso}))}, & (C_i(t) \in R) \cap (E_{re} \geq \overline{E_R}) \cap (E_R < \overline{E_R}) \\ 0, & others \end{cases} \tag{5}$$

where $p_{iso} = k/N * (1 + (B - B_{min})/(B_{max} - B_{min}))$, and B_{max}, B_{min} represent the highest and lowest overall performance of all nodes, respectively.

By optimizing the calculation method of the node threshold, the ULEACH clustering algorithm will comprehensively take the residual energy, energy consumption rate, and overall performance of the nodes into account. That will balance the energy consumption between nodes, and extend the lifetime of the perceptual layer network. The main steps of the ULEACH clustering algorithm are as Algorithm 1.

3 Intrusion Detection System

In the following, we will establish a dynamic intrusion detection model based on game theory to simulate the attack-defense process, and apply the improved PSO algorithm to obtain model's mixed Nash equilibrium solution between the attacker and IDS, in which a game mechanism is added to the fitness function.

3.1 Dynamic Intrusion Detection Model Based on Game Theory

As described above, the CHs possess more residual energy, a smaller energy consumption rate, and higher overall performance. For this reason, an attacker would select CHs to attack rather than cluster member nodes. In the same way, the IDS also tends to deploy the defense system on the CHs. Therefore, we declare that the establishment of the attack-defense process is based on the CHs.

The IoT intrusion detection model mainly includes two players: the attacker (A) and IDS (I). For the moment, the strategy space is recorded as S_A and S_I, and the payoff function is expressed as U_A and U_I. Therefore, at time t the status of each combat unit is defined as $G_i(t) = \{(I, A), (S_{Ii}(t), S_{Ai}(t)), (U_{Ii}(t), U_{Ai}(t))\}$ [5]. There is no point when an attacker or defender does not take

Algorithm 1. ULEACH clustering algorithm

Input: parameters E_{re}, E_R and B
Output: lifetime

Initialize the heterogeneous network of the perceptual layer
Set the basic information of the nodes and run round r=0
while lifetime **do**
  if r=0 **then**
    Obtain the location information
    Calculate $\overline{E_{re}}$, $\overline{E_R}$, and the overall performance
    Each node generates a random number between 0 and 1, and if this number is less than a certain threshold $P_i(t_{iso})$ shown as **Eq. (5)**, the node becomes a CH.
    The CH broadcasts the message that it has become a CH to all nodes
    The node that has not become a CH decides which cluster to join based on the strength of the received broadcast signal, and responses to the CH
    Set the running round $r = r + 1$
    liftime=lifetime_reducing( )
  else
    The cluster member nodes send their own information (E_{re}, E_R, and B) to the CH
    The CH sends the integrated information to the Sink node
    Select the node with more residual energy, a smaller energy consumption rate, and higher overall performance as CH
    The node that has not become a CH chooses a suitable cluster to join, and responds to the CH
    Set the running round $r = r + 1$
    liftime=lifetime_reducing( )
  end if
end while
return lifetime

action. Therefore, we only consider the situation when both the attacker and the defender take action at the same time.

According to the advantages and disadvantages of the two detection techniques and their complementarities [4], the paper coordinate the two detection methods and adopt one at each detection process. In this case we need to develop a strategy where the IDS chooses the optimal method at the right moment.

The attacker can either select the common means (P_{A1}), or new methods (P_{A2}). At the same time, the IDS can either use the anomaly detection method (M_{I1}), or the misuse detection method (M_{I2}). The strategies of the IDS and attacker are expressed as I_i and A_j, respectively, and their total utility function is each defined as B_I and B_A. We define $B_{ij}(I)$ and $B_{ij}(A)$ as the benefit to the IDS and attacker, respectively, when strategies I_i and A_j are chosen.

False alarm rate and missed report rate are two key metrics to measure IDS performance. Assume that, using the anomaly detection method, the missed report rate and the false alarm rate for common attacks are φ_1 and 0; the missed report rate and the false alarm rate for new methods of attack are 0 and ω_1. Similarly assume that, using the misuse detection method, the missed report rate and the false alarm rate for common attacks are 0 and ω_2; the missed report rate and the false alarm rate for new methods of attack are φ_2 and 0.

When the attacker chooses the common methods, and the IDS adopts the anomaly detection method. In this scenario, the missed report rate and false alarm rate are φ_1 and 0. Suppose that $\gamma_1 = \varphi_1\alpha_i(t)\beta_i(t)$, $\gamma_2 = \omega_1\alpha_i(t)\beta_i(t)$, $\gamma_3 = \omega_2\alpha_i(t)\beta_i(t)$, and $\gamma_4 = \omega_2\alpha_i(t)\beta_i(t)$. Obtaining the value of B_{ij} shown as Table 1.

Table 1. Benefit parameter B_{ij} and value

Parameter	Value
$B_{11}(I)$	$[\frac{1-\varphi_1}{\varphi_1}U_4(t) - \frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t)]\gamma_1$
$B_{11}(A)$	$[\frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t) - \frac{(2\varphi_1-1)\alpha_i(t)-\varphi_1}{\varphi_1\alpha_i(t)}L_{Ai}(t)]\gamma_1$
$B_{12}(I)$	$[\frac{1-\omega_1}{\omega_1}U_4(t) - \frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t)]\gamma_2$
$B_{12}(A)$	$[\frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t) - \frac{(2\omega_1-1)\alpha_i(t)-\omega_1}{\omega_1\alpha_i(t)}L_{Ai}(t)]\gamma_2$
$B_{21}(I)$	$[\frac{1-\omega_2}{\omega_2}U_4(t) - \frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t)]\gamma_3$
$B_{21}(A)$	$[\frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t) - \frac{(2\omega_2-1)\alpha_i(t)-\omega_2}{\omega_2\alpha_i(t)}L_{Ai}(t)]\gamma_3$
$B_{22}(I)$	$[\frac{1-\varphi_2}{\varphi_2}U_4(t) - \frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t)]\gamma_4$
$B_{22}(A)$	$[\frac{1-\alpha_i(t)}{\alpha_i(t)}U_3(t) - \frac{(2\varphi_2-1)\alpha_i(t)-\varphi_2}{\varphi_2\alpha_i(t)}L_{Ai}(t)]\gamma_4$

$$X' = \begin{bmatrix} B_{11}(I) & B_{12}(I) \\ B_{21}(I) & B_{22}(I) \end{bmatrix}, Y' = \begin{bmatrix} B_{11}(A) & B_{12}(A) \\ B_{21}(A) & B_{22}(A) \end{bmatrix} \tag{6}$$

The rows and columns in bivariate utility matrix (6) represent separately the IDS's and attacker's strategies.

Assuming that the attacker adopts the common means and the new methods with probability q and $1-q$, respectively. Meanwhile the IDS uses the anomaly detection and the misuse detection methods with probability p and $1-p$, respectively. By using bivariate utility matrix (6), we can gain the total utility function B_I and B_A of the IDS and attacker.

$$\begin{aligned} B_I &= pqB_{11}(I) + p(1-q)B_{12}(I) + (1-p)qB_{21}(I) + (1-p)(1-q)B_{22}(I), \\ B_A &= pqB_{11}(A) + p(1-q)B_{12}(A) + (1-p)qB_{21}(A) + (1-p)(1-q)B_{22}(A). \end{aligned} \tag{7}$$

Table 2. Alternate parameters and value

Parameter	Value
ε_1	$(1-\varphi_1)\alpha_i(t)\beta_i(t)$
ε_2	$(1-\omega_1)\alpha_i(t)\beta_i(t)$
ε_3	$(1-\omega_2)\alpha_i(t)\beta_i(t)$
ε_4	$(1-\varphi_2)\alpha_i(t)\beta_i(t)$
τ_1	$\varphi_1(2\alpha_i(t)-1)\beta_i(t)-\alpha_i(t)\beta_i(t)$
τ_2	$\omega_1(2\alpha_i(t)-1)\beta_i(t)-\alpha_i(t)\beta_i(t)$
τ_3	$\omega_2(2\alpha_i(t)-1)\beta_i(t)-\alpha_i(t)\beta_i(t)$
τ_4	$\varphi_2(2\alpha_i(t)-1)\beta_i(t)-\alpha_i(t)\beta_i(t)$

$B_{ij}(I)$ and $B_{ij}(A)$ in the matrices (6) are brought into Eq. (7), suppose that the parameters shown as Table 2. Obtaining:

$$\begin{aligned} B_I =& (\varepsilon_4 + pq(\varepsilon_1+\varepsilon_3-\varepsilon_2-\varepsilon_4) + p(\varepsilon_2-\varepsilon_4) + q(\varepsilon_3-\varepsilon_4)) * (U_1(t)+U_2(t)-L_{Ii}(t)) \\ & - (\gamma_4 + pq(\gamma_1+\gamma_3-\gamma_2-\gamma_4) + p(\gamma_2-\gamma_4) + q(\gamma_3-\gamma_4)) * \frac{1-\alpha_i(t)}{\alpha_i(t)} U_3(t), \\ B_A =& (\gamma_4 + pq(\gamma_1+\gamma_2-\gamma_3-\gamma_4) + p(\gamma_2-\gamma_4) + q(\gamma_3-\gamma_4)) * \frac{1-\alpha_i(t)}{\alpha_i(t)} U_3(t) \\ & - (\tau_4 + pq(\tau_3+\tau_4-\tau_1-\tau_2). \end{aligned} \tag{8}$$

Next, we need to find the value of (p,q) that makes the IDS obtain the most benefit at the game time.

3.2 PSO for Mixed Equilibrium Nash Solution

In the PSO algorithm, each particle represents potential solution (p, q), and the group consists of M particles $X = \{X_1, X_2, \cdots, X_M\}$ representing potential solutions [16]. In the 2-dimensional target search space, the solution represented by the particle is $X_i = \{x_{i1}, x_{i2}\}$, where $X_{ij} \subseteq [0,1], j = 1, 2$. x_{i1} indicates the probability that a defender will perform an anomaly detection, and x_{i2} represents the probability that an attacker uses a common means.

All particles have no weight, no volume, and fly at a certain speed in the search space. In addition, each particle has a Fitness Function value determined by the optimization function, and both search optimal solution in a random way according to its own Fitness Function value. The position and velocity of the particle i at time t are expressed as: $S_i = (s_{i1}(t), s_{i2}(t), \cdots s_{iM}(t))$, $V_i = (v_{i1}(t), v_{i2}(t), \cdots v_{iM}(t))$.

In each search process, particle i constantly updates its velocity and position by tracking two extreme values. The first extreme value is the position of

the particle with the best Fitness Function value found in the particle experience, usually called the individual extreme value, expressed as PS, where $PS_i = \{ps_{i1}, ps_{i2}, \cdots, ps_{iM}\}$. And the other extreme value is the position of the particle with the best Fitness Function value in the current population. For the global extremum, denoted by GS, where $GS(t) = (gs_1(t), gs_2(t), \cdots, gs_M(t))$, $GS(t)$=$G_g(t)$, $g \in \{1, 2, \cdots, M\}$, and g is the subscript of a particle with the best global position. The changes of particle swarm position and velocity are shown as Eq. (9).

$$\begin{aligned} v_{ij}(t+1) &= \omega v_{ij}(t) + c_1 r_1(p_{ij}(t) - s_{ij}(t)) + c_2 r_2(p_{ij}(t) - s_{ij}(t)) \\ s_{ij}(t+1) &= p_{ij}(t) + s_{ij}(t) + v_{ij}(t+1)\ i = 1, 2, \cdots, N\ \ j = 1, 2 \end{aligned} \tag{9}$$

where ω is called the inertia weight, and its value determines the inheritance degree of the current velocity, which makes the algorithm capable of development and exploration. The range of the ω is set as $[\omega_{\min}, \omega_{\max}]$, then, the ω of the ith iteration is shown in Eq. (10). i_{max} is the maximum number of iteration.

$$\omega_i = \omega_{\max} - \frac{\omega_{\max} - \omega_{\min}}{i_{\max}} \times i \tag{10}$$

c_1, c_2 are learning factors or acceleration factors, and are set to 2. Learning factors enable particles to self-satisfy and learn from the best individuals in the group, thus approaching their historical best within the group. And $r_1, r_2 \sim U(0, 1)$.

In addition, each particle has a Fitness Value determined by the optimization function, and conducts a certain random search in the solution space according to its own adaptive value. For the IDS, fitness function is MSE shown as Eq. (11).

$$\begin{aligned} &MSE = B_I - B_A \\ &= [(\varepsilon_4 + pq(\varepsilon_1 + \varepsilon_3 - \varepsilon_2 - \varepsilon_4) + s_{i1}(\varepsilon_2 - \varepsilon_4) + s_{i2}(\varepsilon_3 - \varepsilon_4)) * (U_1(t) + U_2(t) - L_{Ii}(t)) \\ &\quad - (\gamma_4 + pq(\gamma_1 + \gamma_3 - \gamma_2 - \gamma_4) + s_{i1}(\gamma_2 - \gamma_4) + s_{i2}(\gamma_3 - \gamma_4)) * \frac{1 - \alpha_i(t)}{\alpha_i(t)} U_3(t)] \\ &\quad - [(\gamma_4 + pq(\gamma_1 + \gamma_2 - \gamma_3 - \gamma_4) + s_{i1}(\gamma_2 - \gamma_4) + s_{i2}(\gamma_3 - \gamma_4)) * \frac{1 - \alpha_i(t)}{\alpha_i(t)} U_3(t) \\ &\quad - (\tau_4 + pq(\tau_3 + \tau_4 - \tau_1 - \tau_2)]. \end{aligned} \tag{11}$$

The main steps to find the value of (p,q) that makes the most profit for the IDS at the game time are shown in Algorithm 2.

Finally, the solution s_g represented by the particle at the optimal position is gained through the Algorithm 2, and the value of (p, q) that makes the IDS obtain the most benefit.

3.3 Model for Dynamic Intrusion Detection Based on Game Theory

The proposed dynamic intrusion detection game model combines anomaly detection with misuse detection to defend against both common attacks and new methods of attacks, as shown in the Algorithm 3.

Algorithm 2. Find the values of p and q based on PSO

Input: Randomly generated initial particles
Output: Particle value of (p, q)

1: Let $t = 0$, and initialize the position and velocity of the particles in the algorithm space
2: **while** ($\left|MSE_{s_i(t+1)} - MSE_{ps_i(t)}\right| > 0.001$ or $t < 1000$) **do**
3: Let $t = t + 1$
4: Update the velocity of all particles
5: Update the position of all particles
6: Calculate the current Fitness Function value and compare it with the that of the previous iteration. If the current value is smaller than that of the previous iteration, update the current position of the particle according to the position of the particle. That is if $MSE_{s_i(t+1)} < MSE_{ps_i(t)}$, then $ps_i(t+1) = s_i(t+1)$.
7: Calculate the current global optimal position g_{t+1} of the population
8: Compare the current global optimal location with the previous iteration's global optimal location, if g_{t+1} is superior to g_t, then g_{t+1} is the global optimal position of the group
9: Update $\omega, s_{ij}(t+1)$ according to Eq. (10), Eq. (9).
10: **end while**
11: **return** Particle value of (p, q) for the IDS to maximum the profit.

4 Simulation Experiment and Analysis

Due to the limitations of a real experimental environment, such as high cost, and poor performance, we evaluate the proposed intrusion detection model in the DeterLab platform [11]. The topology of three clusters in the model are shown in Fig. 2. All of their initial energy was set to 10J, except for the Sink node located in the center, which had no energy restriction. We set the alterable number of the attack nodes per round to 5% to 15%, and the sum of the number of the attack nodes and the common member nodes was stable. The number of selected CH nodes in each round of the experiments were 5% to 10%. The duration of each round of the attack-defense process was 50 s, the interval was 1 min, and the number of CHs selected per round was not fixed. The experimental parameters are shown in Table 3.

In order to obtain more convincing results, we compared the game-based intrusion detection model for IoT perceptual layer (GTULDS-Proposed) with the current advanced algorithms. Rowayda has proposed a new hybrid heterogeneous energy-aware IoT protocol (HHEDS) for complex IoT network with multiple levels of heterogeneity located in different regions [13]. Sedjelmaci has proposed a game theory based technique to activate anomaly detection technique only when a new attack's signature is expected to occur(LHDS) [14]. Figure 3a shows the intrusion detection rate of each intrusion detection algorithm when the number of the attack nodes changes. The detection rate represents the ratio of the number of attackers correctly detected to the total number of attackers.

According to Fig. 3a, the increase in the number of the attack nodes reduces the detection rate and has roughly the same impact on the three algorithms.

Table 3. Simulative experimental parameters

Parameter	Value
Each round time/s	50
Node pause time/s	60
Node interface	IEEE 802.15.4
Network clustering protocol	ULEACH
Size of detection area/m	100^2
Number of sensor nodes	200
Number of attack nodes	From 5% to 15% of overall nodes
Initial energy of node/J	10

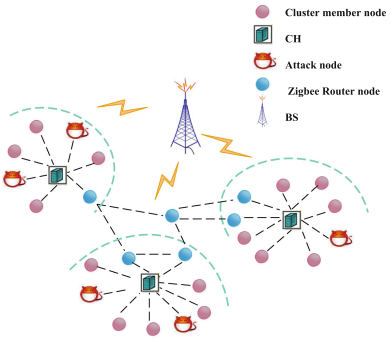
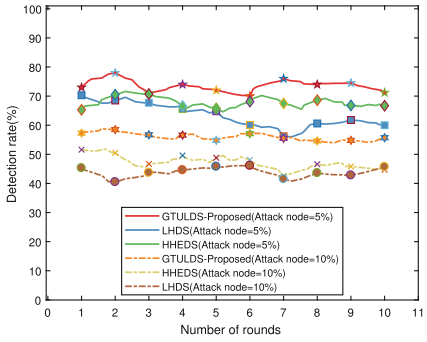
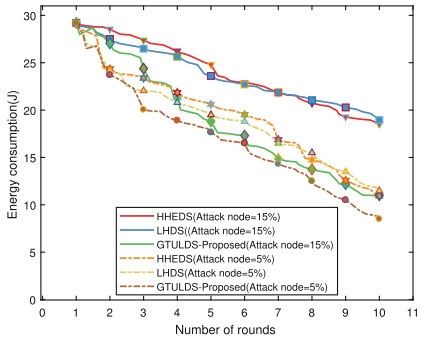


Fig. 2. The topology of three clusters in the model



(a) Comparison of intrusion detection rate.



(b) The energy consumption.

Fig. 3. The intrusion detection rate and energy consumption of the algorithm.

Algorithm 3. Dynamic intrusion detection model based on game model

Input: parameters $U_1(t)$, $U_2(t)$, $U_3(t)$, $L_{Ii}(t)$, $L_{Ai}(t)$, $E_i(t)$, E_{max}, E_{min}, $\beta_i(t)$, and $\alpha_i(t)$

Output: Optimal defense strategy

1: Initialize heterogeneous network of the perceptual layer
2: Set the basic information of the nodes
3: With the clustering algorithm ULEACH, the CHs for the IDS placement strategy are selected
4: Construct dynamic intrusion detection model based on game theory to minimize energy consumption
5: According to Algorithm 2, the probability p of performing the anomaly detection method and the probability q of adopting the common means are obtained
6: Based on the value of p and q, the mixed utility of the IDS B_I and the attacker B_A are calculated to solve the mixed Nash equilibrium solution, and the optimal defense strategy that could balance the detection efficiency and energy consumption of the system is obtained
7: Using the defense strategy, the predicted targeted CH node, and attack time, the Sink node adopts the corresponding detection method on the targeted node
8: **return** Optimal defense strategy

In addition, it is obvious that the intrusion detection model built with the game theory is more trustworthy. Consequently, the intrusion detection algorithm based on game theory provides a higher detection rate and ensures that the perceptual layer network of IoT can be safely used in a more complex network environment.

In the simulation, we made a record of the average energy consumption of all nodes in the perceptual layer. Figure 3b shows the energy consumption of the three intrusion detection algorithms when the number of malicious nodes changes. It can be seen from Fig. 3b that the increase in the number of the attack nodes has little effect on the energy consumption of the intrusion detection model proposed in this paper, but greatly increases the energy consumption of the LHDS and HHEDS algorithms. It is also obvious that our proposed intrusion detection model consumes far less energy than the LHDS and HHEDS algorithms.

5 Conclusion

This paper researches and proposes an intrusion detection model based on game theory to reduce the energy consumption of the IoT perceptual network in the attack-defense process. The proposed detection system improves on previous work in three main ways: (i) it proposes a clustering algorithm ULEACH that comprehensively considers the residual energy, energy consumption rate, and overall performance of nodes, to select the CHs for the IDS placement; (ii) it takes energy consumption of the attack-defense process into account, establishes the intrusion detection model based on the game theory; and (iii) by applying modified particle swarm optimization, the optimal defense strategy that could balance the detection efficiency and energy consumption of the system is obtained.

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

References

1. Castiglione, A., Palmieri, F., Fiore, U.: Modeling energy-efficient secure communications in multi-mode wireless mobile devices. Comput. Syst. Sci. **81**, 1464–1478 (2015)
2. Bhunia, S.: Internet of things security: are we paranoid enough. In: 2018 IEEE International Conference on Consumer Electronics (ICCE), p. 1. IEEE (2018)
3. Caviglione, L., Merlo, A.: The energy impact of security mechanisms in modern mobile devices. Netw. Secur. **2012**(2), 11–14 (2012)
4. Hajisalem, V., Babaie, S.: A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. Comput. Netw. **136**, 37–50 (2018)
5. Han, L., Zhou, M., Jia, W., Dalil, Z., Xu, X.: Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Inf. Sci. **476**, 491–504 (2018)
6. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on IEEE, vol. 2, p. 10 (2000)
7. Henningsen, S., Dietzel, S., Scheuermann, B.: Misbehavior detection in industrial wireless networks: challenges and directions. Mobile Netw. Appl. **23**(5), 1330–1336 (2018)
8. Hossein, J.: Designing an agent-based intrusion detection system for heterogeneous wireless sensor networks: robust, fault tolerant and dynamic reconfigurable. Int. J. Commun. Netw. Syst. Sci. **4**, 523–543 (2011)
9. Luo, J., Wu, D.: Optimal energy strategy for node selection and data relay in WSN-based IoT. Mobile Netw. Appl. **20**(2), 169–180 (2015)
10. Merlo, A., Migliardi, M., Caviglione, L.: A survey on energy-aware security mechanisms. Pervasive Mob. Comput. **24**, 77–90 (2015). special Issue on Secure Ubiquitous Computing
11. Michael Quick, T.R.D.: The deter project. https://www.isi.deterlab.net/index.php3
12. Ozger, M., Cetinkaya, O., Akan, O.B.: Energy harvesting cognitive radio networking for IoT-enabled smart grid. Mobile Netw. Appl. **23**(4), 956–966 (2018)
13. Sadek, R.A.: Hybrid energy aware clustered protocol for IoT heterogeneous network. Future Comput. Inform. J. **3**(2), 166–177 (2018)
14. Sedjelmaci, H., Senouci, S.M., Taleb, T.: An accurate security game for low-resource IoT devices. IEEE Trans. Veh. Technol. **66**(10), 9381–9393 (2017)
15. Sedjelmaci, H., Senouci, S.M., Feham, M.: New framework for a hierarchical intrusion detection mechanism in cluster-based wireless sensor networks. Secur. Commun. Netw. (2011)
16. Shi, Y., Eberhart, R.: A modified particle swarm optimizer. In: Proceedings of the IEEE Conference on Evolutionary Computation, pp. 69–73 (1998)