A Danger Theory Inspired Protection Approach for Hierarchical Wireless Sensor Networks

Xin Xiao[1*], Ruirui Zhang[2]
[1]School of Computer Science, Southwest Minzu University
Chengdu, China
[xiaoxin618@gmail.com]
[2]School of Business, Sichuan Agricultural University
Yaan, China
[zhangruiruisw@gmail.com]
*Corresponding author: Xin Xiao

Received June 15, 2018; revised October 20, 2018; accepted November 18, 2018; published May 31, 2019

Abstract

With the application of wireless sensor networks in the fields of ecological observation, defense military, architecture and urban management etc., the security problem is becoming more and more serious. Characteristics and constraint conditions of wireless sensor networks such as computing power, storage space and battery have brought huge challenges to protection research. Inspired by the danger theory in biological immune system, this paper proposes an intrusion detection model for wireless sensor networks. The model abstracts expressions of antigens and antibodies in wireless sensor networks, defines meanings and functions of danger signals and danger areas, and expounds the process of intrusion detection based on the danger theory. The model realizes the distributed deployment, and there is no need to arrange an instance at each sensor node. In addition, sensor nodes trigger danger signals according to their own environmental information, and do not need to communicate with other nodes, which saves resources. When danger is perceived, the model acquires the global knowledge through node cooperation, and can perform more accurate real-time intrusion detection. In this paper, the performance of the model is analyzed including complexity and efficiency, and experimental results show that the model has good detection performance and reduces energy consumption.

Keywords: wireless sensor network, artificial immune, intrusion detection, danger theory, genetic algorithms, security

---

http://doi.org/10.3837/tiis.2019.05.027 **ISSN : 1976-7277**

1. Introduction

As the development of sensor technology, wireless communication technology, distributed information processing technology and embedded technology, the wireless sensor network (WSN) - a network which is composed of a large number of tiny sensor nodes with micro processing ability, arises at the historic moment. It fuses the logical information world with the objective physical world, and has changed the way people interact with nature. WSNs have gained widespread attention from academia, industry and government, and become one of the most competitive application technologies in many fields such as national military defense, environment monitoring and forecasting, health care, smart home, building structure monitoring, complex machinery monitoring, urban traffic, space exploration, large workshop and warehouse management, large industrial park safety monitoring [1-5].

To ensure the safety of WSNs is one of the bases that wireless sensor networks can be widely applied. Some defense measures such as encryption, authentication, secure routing, can prevent the invasion to some extent, but cannot completely hold back all kinds of attacks. The main challenges of WSN intrusion detection are as follows.

(1) Attack form is varied. Means and characteristics of attacks in wireless sensor networks have a bigger difference with those in traditional computer networks. For example, most of attacks in the link layer and the network layer are peculiar to wireless sensor networks. Traditional computer network resources such as network, files, system logs, processes cannot be used in wireless sensor networks, and we need to consider the feature information which can be applied to the wireless sensor network intrusion detection.

(2) The attacks of new type in wireless sensor networks are endless. How to improve the ability of intrusion detection system to detect unknown attacks is a problem that needs to be solved.

(3) Wireless sensor network resources which include storage space, computing power, bandwidth and energy are limited. Limited storage means that a large number of system logs cannot be stored on sensor nodes. Intrusion detection system based on knowledge requires storing large amounts of defined intrusion patterns and detects intrusion through pattern matching. This method needs to store invasion behavior characteristics, and feature library will increase with the increase of invasion type. Limited computing power means that an intrusion detection algorithm with large amount of computing is not suitable for running on nodes. The current wireless sensor networks adopt low-speed and low-power-consumption communication technologies. the characteristics of limited energy request intrusion detection systems not to bring too much communication overhead. This is less considered in the traditional computer network.

The following is a brief introduction to the existing wireless sensor network intrusion detection technologies. Onat and Miri proposed an intrusion detection system for resource depletion attacks [8]. Roman et al. designed a framework for the application of intrusion detection system (IDS) in wireless sensor networks [9]. Martynov et al. proposed an intrusion detection model for wireless sensor network based on agents [10], and Al-Yaseen et al. put forward a real-time multi-agent based adaptive intrusion detection system [16]. Drozda studied an intrusion detection technology based on artificial immune system - the SNS model [11], to solve problems of discarding, packets delay forwarding and wormhole attacks. Schaust et al. applied principles of the degenerate behavior of T-cell receptors from artificial immune systems to wireless sensor networks, and proposed the misuse detection model [12].

Kim et al. proposed an interest cache poisoning attack for directed diffusion (DD) routing protocol in wireless sensor networks, and presented a detection method for this attack by dendritic cell algorithm (DCA) [13]. Wazid et al. put forward a hybrid anomaly detection scheme using K-means clustering to detect blackhole attack and misdirection attack in wireless sensor networks [14]. Ma et al. proposed a spectral clustering and deep neural network based intrusion detection algorithm, and verified the algorithm in the datasets of KDDCUP99 and NSL-KDD [15]. Gunasekaran et al. proposed a genetic algorithm based intrusion detection model to solve the denial-of-sleep attack in wireless sensor networks [20]. Shi et al. put forward a dynamic programming model for internal attack detection in wireless sensor networks through continuous time Markov chain and the epidemic model to optimize the detection rate [27]. Zeeshan et al. proposed an anomaly detection system (ADS) framework to detect Sybil attack which causes data flow anomaly in WSNs [28].

Through analysis of the existing wireless sensor network intrusion detection schemes, research on intrusion detection technology in WSNs is not very mature, and the above detection systems are mostly transplanted from traditional network intrusion detection technologies. There are three problems. Firstly, nodes are in promiscuous mode, which prevents them into sleep and force them into the idle or receiving state, which extremely consumes energy. Secondly, the intrusion detection model is deployed on a single sensor node, which greatly consumes resources. Thirdly, the intrusion detection model is aimed at specific attacks, and the universality needs to be improved.

Inspired by the danger theory in the biological immune system, this paper proposes an intrusion detection model based on the danger theory for wireless sensor networks, named DT-IDM. The main contributions of this model are as follows. (1) The model abstracts expressions of antigens and antibodies in wireless sensor networks, defines meanings and functions of danger signals and danger areas, and expounds the process of intrusion detection based on the danger theory. (2) The model realizes the distributed deployment, and there is no need to arrange an instance at each sensor node. In addition, sensor nodes trigger danger signals according to their own environmental information, and do not need to communicate with other node, which saves resources. When danger is perceived, the model acquires the global knowledge through node cooperation, and can perform more accurate real-time intrusion detection. The performance of the model is analyzed including scalability, robustness and complexity, and experimental results show that the model has good detection performance and reduces energy consumption.

The remainder of this paper is organized as follows. The related work which is also the background of this paper is described in Section 2. The theories of the model including description of the architecture, definitions of the model, implementation mechanisms of danger signal and danger area, and implementation mechanism of decision and response are described in Section 3. The performance is analyzed in Section 4. The effectiveness of DT-IDM is verified in Section 5. Finally, the conclusions and future works are given in the last section.

2. Related Work

2.1 Typical Attacks of WSNs

The following is a brief introduction to typical attacks of wireless sensor networks at the protocol level.

(1) Physical layer attack

Physical layer attacks mainly include jamming attacks and physical capture attacks. In the jamming attack, the attacker keeps transmitting blocking signals in the working band of wireless sensor networks, so that sensor devices in the communication radius of the attacker node cannot work properly. Sensor nodes which are deployed in harsh environments are easily captured by attackers, and attackers can obtain sensitive information in multiple ways for the captured sensor nodes.

(2) Link layer attack

The work of the data link layer focus on data frame monitoring, data flow multiplexing, media access and error control, which guarantees point-to-point or point-to-multipoint connection reliability. Typical attacks on the link layer include resource depletion attacks, collision attacks, unfair attacks, etc.

Resource depletion attacks require the attacker to be part of the network, and are primarily for wireless sensor nodes with limited energy. The attacker can modify the conflict avoidance mechanism to consume other nodes' energy. The collision attacker listens to the channel for information transmission. When there is information to transmit, the attacker launches interference signals which will collide with the legitimate information. Unfair attack is a weak form of denial of service (DOS) attack.

(3) Network layer attack

The network layer is responsible for routing the data provided by the transport layer. Typical attacks on the network layer mainly include neighbor discovery protocol attack, sybil attack, selective forwarding attack, wormhole attack, sinkhole attack, etc.

The neighbor discovery protocol attackers enable target nodes to believe that they provide network functions, so that the nodes could not obtain the correct network topology perception, and could also be overloaded. The famous hello flood attack belongs the neighbor discovery protocol attack. Sybil attack refers to that the attacker declares multiple identities and fakes multiple legal nodes, to destroy the voting mechanism, or to reduce the performance of the fault-tolerant mechanism such as multi-path routing, topology maintenance. The selective forwarding attack refers to that the attacker as the route node to forward data chooses to discard or forward packets selectively. The wormhole attackers transmit messages which are received from an area of the network through high-speed tunnel to other areas, in order to disrupt the routing or attract forwarding messages. The target of sinkhole attackers is to attract data streams in a region through broadcasting high quality routing information.

(4) Application layer attack

The application layer is responsible for implementing functions which are required for particular applications, such as integrating the data from the collection. Application layer attack is related to specific applications, such as location attack, malicious code, etc.

2.2 Intrusion Detection Characteristics of WSNs

Before the intrusion detection algorithm is implemented, it is necessary to analyze the node’s local log, communication data packet and network behavior, and extract the characteristics for intrusion detection. The detection features are the basis of wireless sensor network intrusion detection, and the detection algorithm can identify attacks by finding the abnormal characteristics. The characteristics of wireless sensor networks are briefly described below.

Physical layer features include: energy reduction rate, cache occupancy rate, and RSS. The characteristics of link layer include: packet collision rate, packet avoidance interval, packet avoidance times, RTS message frequency, data frame transmission success rate, data frame receiving rate, and data frame transmission rate. Features of network layer include: routing request message frequency, the success rate, packet retransmission rate, routing overhead change, packet receiving rate, packet type distribution, packet arrival rate, packet delay, packet forwarding rate, throughput capacity, and package integrity. The application layer characteristics mainly include: perception data change and perception data arrival rate.

2.3 Danger Theory

The danger theory proposed by biological immunologist Matzinger [17] believes that there are two death manners for cells in biological immune system which are apoptosis and necrosis. Apoptosis is a natural process, and is the result of environmental regulation in the body. Necrosis is irregular death associated with stress cells or other means. This approach of death will lead to specific biochemical reactions of the body, is different from natural rules, and will produce distinct degrees of danger signals which form the basis of the immune response. Thus, the biological system produces danger signals, then conducts the immune response according to changes in the environment. Danger signals build a danger zone around them, where immune cells will be activated to take part in immune responses. Compared with the traditional CLONALG theory, danger theory introduces environmental factors of the body, describes some important characteristics of the biological immune system, and explains some immune phenomena which the traditional theory cannot explain, such as autoimmune diseases.

Compared with the traditional Self-Nonself (SNS) model, the main difference between the two is that they have different explanations for activation conditions of antigen presenting cells. The SNS model suggests that antigen presenting cells are activated by the identification of external pathogens, and the danger theory believes that the root cause of the immune response is the danger signal issued by the damage or accidental death of organisms. Although there is still controversial about the danger theory in the traditional biological immune field, it gets rid of some limitations of the SNS model. The exogenous pathogens do not play a decisive role in triggering immune responses, but only perceiving damages of body cells will do the job. So, the danger theory is more suitable for the intrusion detection field than the SNS model [18,19].

Table 1 lists the concepts mapping of danger theory and the intrusion detection system in wireless sensor networks.

Table 1. Mapping of danger theory and the intrusion detection system

Danger theory	The intrusion detection system
Gene segments	The normal traffic information of nodes
Antigens	Consist of genes, the key information extracted from traffic packets
Antibodies	the same structure with antigens, and are generated by sink node
Apoptosis	Nodes can't work due to normal reasons such as energy depletion
Necrosis	Nodes can't work due to invasion or network anomalies
Lymphocytes	Sensor nodes and sink nodes
APC	Nodes cooperate to acquire global invasion or abnormal

	information
Danger signals	Node’s local environmental status affected by invasion or network anomalies
Danger areas	Set of nodes which are greatly affected by invasion or network anomalies

3. Model Description

3.1 Architecture of Intrusion Detection System

A typical wireless sensor network consists of sink nodes and sensor nodes [1-5]. Sensor nodes can be distributed in the monitored area by means of artificial placement or maybe spread by aircraft, and so on. And they can form a network through self-organization routing protocols such as clustering-based protocols, data-centered protocols. Each sensor node can collect data independently, and the collected data is sent to the sink node through single hop or multi hop relay. Sink node has numerous resources, and deals with data sent by sensor nodes. In the hierarchical wireless sensor networks, clustering-based routing protocol is adopted, and sensor nodes are divided into cluster heads and cluster members [24-26].

If each sensor node runs a complete testing instance at the same time, it will cost a lot of resources for the node. It is not proper. Therefore, the intrusion detection system proposed in this paper adopts the distributed structure. The system is divided into three levels, the application layer, the immune layer and the wireless sensor network layer. The detection model is scattered on the immune layer, including the danger perception module, antigen presentation module, decision module and intrusion response module. The danger perceiving module and the antigen presenting module are deployed on the sensor nodes, including cluster heads and cluster members. Decision module and intrusion response module are deployed on the sink node. As shown in **Fig. 1**.

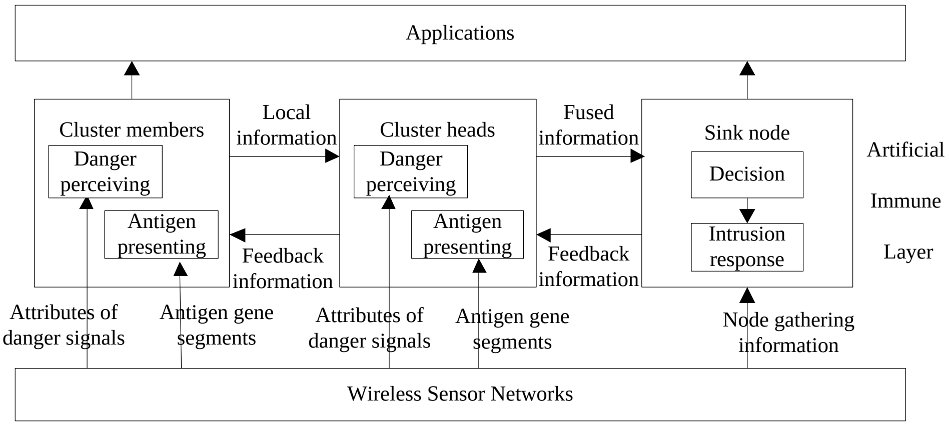


Fig. 1. The architecture of proposed intrusion detection system

The detection process of the model is described as follows, and **Table 2** shows the process. Firstly, cluster heads and cluster members detect changes of their own properties, extract the key data, and obtain the signal information of the current environment to perceive the risk.

When danger is perceived, cluster member transmits the danger signal to cluster head, cluster head integrates multiple danger signals and finally passes to the sink node. Then, sink node computes the degree of risk and the range of the risk domain, and demands presenting antigens. Sensor nodes within the danger area work together to collect the network traffic information for forming antigens. After that, the sink node generates antibodies to carry out immune responses, and decides whether an intrusion occurs. If an intrusion occurs, the response is taken, and the feedback information are sent to the network.

Table 2. The detection process of the model

```
Begin
  Sink node generates mature detector set $T$, and parameters are set: matching threshold $\theta$, danger threshold $\varepsilon$ and the max age of detectors $age_{max}$;
  Initialize each sensor node vector $V_i$;
  While the program has not reached the termination condition do
    While the value of sensor node danger signal $|DS_i(t)|$ does not reach $\varepsilon$ for cluster heads and cluster members do
      Cluster heads and cluster members periodically sample the environmental information $DS_{ij}(t)$, and add it to the node vector $V_i$;
    End;
    The danger signal is routed to sink node;
    Sink node computes the range of the danger area $D(Nd_i)$, and asks for presenting antigens;
    Sensor nodes within the risk domain cooperate to collect network information to form antigen $ag$;
    Mature detectors carry out immune responses;
    If intrusion is determined then
      the system notifies sensor nodes;
    End if;
  End;
End;
```

Fig. 2 shows the process.

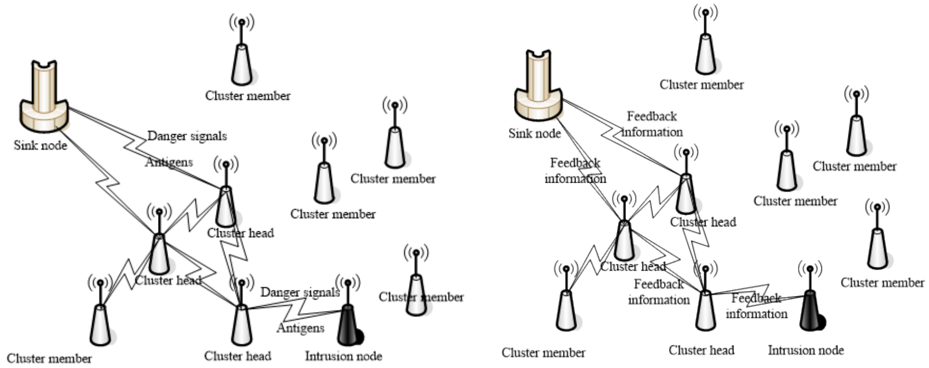


Fig. 2. Intrusion detection process

3.2 Model Definition

In wireless sensor networks, all the information in the end can be reduced to a binary string. In fact, intrusion detection is classification of the binary string according to certain rules and priori knowledge. Define the problem state space $\Omega = \cup_{i=1}^{\infty} \{0,1\}^i$. Based on the biological immunity, wireless sensor networks are defined as organisms, and sensor nodes are defined as immune tissues. Define the antigen set $AG \subset \Omega$.

Definition 1. An antigen is the structured characteristic vector in the solution space of the artificial immune system domain [21]. In this model, the antigen *ag* consists of multiple genes, and is represented by a binary string. Genes are extracted from key fields of packets broadcasted by neighbor nodes, and include attributes of the MAC layer and the network layer. Specifically, the gene contains the node address, the next-hop destination address, the packet source address, the packet destination address, the packet size, the MAC frame type, etc. Packets from the same node will be abstracted as the same kind of antigens. Define the antigen $ag=\{(g_1, g_2,\ldots, g_m)|g_i \in \{0,1\}^{l_i}, i=1,2,\ldots,m, l_i$ is the length of $g_i\}$. The set of all antigens in the space is expressed as $AG = \cup_{i=1}^{\infty} \{Ag_i\}$.

It is assumed that normal strings that can be recognized by the model are defined as self set *S*, all the unknown strings are defined as *N*, abnormal strings that produce danger signals are defined as *D*, and strings that are judged as invasions are defined as *I*.

Then, $S \cap N = \emptyset, S \cup N = AG$. Danger theory does not distinguish between self and non-self, only recognizes intrusion set $I = D \cap N$ which triggers immune responses, and does not respond to harmless set $D \cap S$.

Definition 2. Antibodies have the same structure with antigens, and are protein molecules which are secreted by antigen-stimulated B lymphocytes. They can be combined with specific antigens, and are used to detect and match antigens. In the model, antibodies are generated by sink node, and can perform immune responses after immune tolerance. Define antibody $ab = \{(g_1, g_2,\ldots, g_m)|g_i \in \{0,1\}^{l_i}, i=1,2,\ldots,m, l_i$ is the length of $g_i\}$. The set of antibodies is expressed as $AB = \cup_{i=1}^{\infty} \{Ab_i\}$.

Definition 3. The affinity between an antibody and an antigen is expressed as *Affinity(ag, ab)*, and represents the binding strength of the antibody and antigen. In this paper, an improved r-continuous bit matching method is adopted.

$$Affinity(ag, ab) = \begin{cases} 1, & \sum_{i=1}^{m} f(ab.g_i, ag)/m \geq \theta \\ & 0, \quad others \end{cases} \tag{1}$$

Where θ is the matching threshold, and $f(x, y)$ is the r-continuous bit matching method for antibody's gene segment g_i and antigen *ag*.

$$f(x,y) = \begin{cases} 1, & \exists i,j, j-i \geq |x|, 0 < i \leq j \leq m \cdot (l+1), x_i = y_j, x_{i+1} = y_{j+1}, \ldots, x_{|x|} = y_{j+|x|-1} \\ & 0, \quad others \end{cases} \tag{2}$$

The purpose of intrusion detection is to distinguish patterns: for an input schema x, $x \in AG$, the system detects and determines this schema belongs to self or non-self. The detection system can be expressed as $IDS = (F, M)$. F is the classification function, and M is a collection of detector information patterns extracted from Ω. The system may have two errors in the detection process: false negative, sorting non-self to be self, $\varphi_- = \{x \in N \cap F(x, M) = anomalous\}$; false positive, sorting self to be non-self, $\varphi_+ = \{x \in S \cap F(x, M) = normal\}$.

3.3 Danger Signals

Danger theory emphasizes that danger signals which are produced by environmental changes are used to guide different levels of immune responses, and zones around danger signals are regarded as danger areas. Because the danger signal is related to the environment, changes of sensor nodes' attributes reflect the environmental status in wireless sensor networks. Nodes do not need to communicate with surrounding nodes, only use local knowledge for statistics. This reduces the amount of data and network traffic, and will not generate additional communication overhead. Nodes only collect information in their own work time, and do not need additional wake-up operation, which will not bring too much energy consumption.

When nodes are under attack or network is abnormal, characteristics of the physical layer and link layer change more obviously. The energy decline rate of sensor node $DS_{i1}(t)$, the packet avoidance frequency $DS_{i2}(t)$, the average packet avoidance duration $DS_{i3}(t)$, the receiving frequency of frames $DS_{i4}(t)$ and the transmission frequency of frames $DS_{i5}(t)$, these characteristics' values vary greatly. And nodes can get these attributes' values in the local. Therefore, we select statistical values of these attributes to reflect the danger signal *DS*.

The energy decline rate of sensor node $DS_{i1}(t)$ is express as follows. When the DOS attack occurs, the value of this property changes greatly.

$$DS_{i1}(t) = \sum_{t}^{t+\Delta t} P \,/ \Delta t \tag{3}$$

Where, $\sum_{t}^{t+\Delta t} P$ is the normalized value of energy changes in the time interval Δt.

The packet avoidance frequency $DS_{i2}(t)$ is expressed as follows. In wireless sensor networks, the protocols used in the link layer are mostly based on competing MAC protocols. This property is more sensitive when packet jamming attack occurs.

$$DS_{i2}(t) = \sum_{t}^{t+\Delta t} Nd \,/ \Delta t \tag{4}$$

Where, $\sum_{t}^{t+\Delta t} Nd$ is the normalized value of the escape times of frames in the time interval Δt.

The average packet avoidance duration $DS_{i3}(t)$ is expressed as follows. This property changes greatly when the blocking attack occurs.

$$DS_{i3}(t) = \sum_{t}^{t+\Delta t} Td \,/ \Delta t \tag{5}$$

Where, $\sum_{t}^{t+\Delta t} T\mathrm{d}$ is the normalized value of fallback duration of frames in the time interval Δt.

The receiving frequency of frames $DS_{i4}(t)$ is expressed as follows. The abnormal change of the receiving frequency of frames implies the danger. For example, when the node is the attack target, the number of the received data frames increases and the value of the receiving frequency increases.

$$DS_{i4}(t) = \sum_{t}^{t+\Delta t} Nr \,/ \Delta t \tag{6}$$

Where, $\sum_{t}^{t+\Delta t} Nr$ is the normalized value of the number of received data frames in the time interval Δt.

The transmission frequency of frames $DS_{i5}(t)$ is expressed as follows. Abnormal change of the transmission frequency of frames also implies the risk. For example, when large-scale worm attacks or blocking attacks occur, nodes usually need to forward these malicious packets, which results in the number of transmission frames increasing and the transmission frequency increasing. While sinkhole attacks occur, routing nodes which are originally normal will no longer transmit data, which leads to the number of transmission frames plummeting and the transmission frequency dropping.

$$DS_{i5}(t) = \sum_{t}^{t+\Delta t} N\mathrm{s} \,/ \Delta t \tag{7}$$

Where, $\sum_{t}^{t+\Delta t} Ns$ is the normalized value of the number of transmission frames in the time interval Δt.

Suppose that $S_{ij}(t) = \left|DS_{ij}(t) - DS_{ij}(t-1)\right|$ is the changed amount of the property DS_{ij} in the time t.

Definition 4. danger signal $DS_i(t)$ is expressed as follows.

$$DS_i(t)=<Nd_i,\ t,\{\ S_{ij}(t)\,|\ j=1,2,\ldots,5\}> \tag{8}$$

Where, Nd_i is the sensor node i. $|DS_i(t)|$ is the value of danger signal in the time t, and is expressed as follows.

$$|DS_i(t)| = \left(\sum_{j=1}^{5} w_j \cdot (DS_i(t).S_{ij}(t))\right) / \sum_{j=1}^{5} w_j \tag{9}$$

w_j is the weights of danger signal attributes. Because $0 \le DS_i(t).S_{ij}(t) \le 1$, $0 \le |DS_i(t)| \le 1$. When the value of $|DS_i(t)|$ is greater than the danger threshold ε, the sensor node will route danger signals to the sink node.

3.4 Danger Areas

According to the danger theory, if an antigen Ag_i is in necrosis, the surrounding area around Ag_i will become the danger area $D(Ag_i)$. For the intrusion detection, when a node is attacked or the network is abnormal, we take the area near the node Nd_i as the danger area $D(Nd_i)$. The range of the risk region defines the extent of the immune response, and immune cells in this range will be activated and involved in the immune response.

Definition 5. Danger area $D(Nd_i)$ is defined as follows.

$$D(Nd_i)=\{Nd_j|DIS(Nd_i, Nd_j)<Rdanger_i \cap (Nd_j \text{ is cluster head } \cup j = i)\} \tag{10}$$

Where, $DIS(Nd_i, Nd_j)$ is the distance between node i and node j, and is expressed as (11). $Rdanger_i$ is the radius of the danger zone of node i, and is expressed as (12). Then, $D(Nd_i)$ represents the set of the node i and the head nodes of clusters whose distances from node i are smaller than the radius of the danger zone.

$$DIS(Nd_i, Nd_j)=\begin{cases} 0 \quad \text{if } i = j \\ 1/(N_{leapmax}+1) \quad if\ i \neq j \cap i\ and\ j\ are\ in\ the\ same\ cluster \\ N_{leap}/(N_{leapmax}+1) \quad if\ i\ and\ j\ are\ in\ different\ cluster \end{cases} \tag{11}$$

$N_{leapmax}$ is the maximum number of hops between clusters in wireless sensor networks. If $i=j$, N_{leap} is 0; if the node i and node j are different and in the same cluster, N_{leap} is 1; if the node i and node j are not in the same cluster, N_{leap} is the number of hops between the cluster where the node i is and the cluster where the node j is plus 1. Therefore, $0 \le DIS(Nd_i, Nd_j) \le 1$.

$$Rdanger_i = \sum_{j=0}^{N_{ds}} \frac{1}{DIS(Nd_i,Nd_j)+1} \cdot |DS_j(t)|/w_{ds} \tag{12}$$

N_{ds} is the number of danger signals received by the sink node in the time t. w_{ds} is the danger radius coefficient, and is used to adjust the size of the risk radius.

Obviously, the radius of the danger area is related to the strength of danger signal and the surrounding environment of the node. When the node's danger signal is stronger, it indicates that the node's environment is damaged or the probability of being damaged is larger, and the range of danger area is larger. The danger signals emitted by surrounding nodes will also affect the range of the risk area of the node. The more the number of nodes which send out danger signals is, the greater the changes of the surrounding environment are, and the bigger the range of risk area of the node is. The smaller the distance between the node and other nodes that send out danger signals is, the greater the impact on the risk area of the node is.

3.5 Decisions and Responses

When the sink node receives the antigen information, the immune response will be carried out. The process of immune response uses the traditional self-non-self identification, and the system calculates the affinity between antigens and antibodies to determine whether an invasion has occurred. The antibody corresponds to the mature detector in the intrusion detection algorithm, and the antigen corresponds to the network information that needs to be detected.

Definition 6. Detector set is expressed as $B = \{< ab, age > \mid ab \in AB \cap age \leq age_{max}\}$. Where, ab is the antibody of detector, age is the age of detector, and age_{max} is the max age.

Detectors are divided into immature ones and mature ones. We use **Fig. 3** to represent the model's immune mechanism. The model first produces a new immature detector through genetic coding. The immature detector evolves into a mature detector through the negation selection. If it matches the self in the tolerance period, it will die. The mature detector has a fixed length of life cycle. If it is activated by the danger signal during the life cycle, the clone selection operation is carried out. Otherwise it would be killed.

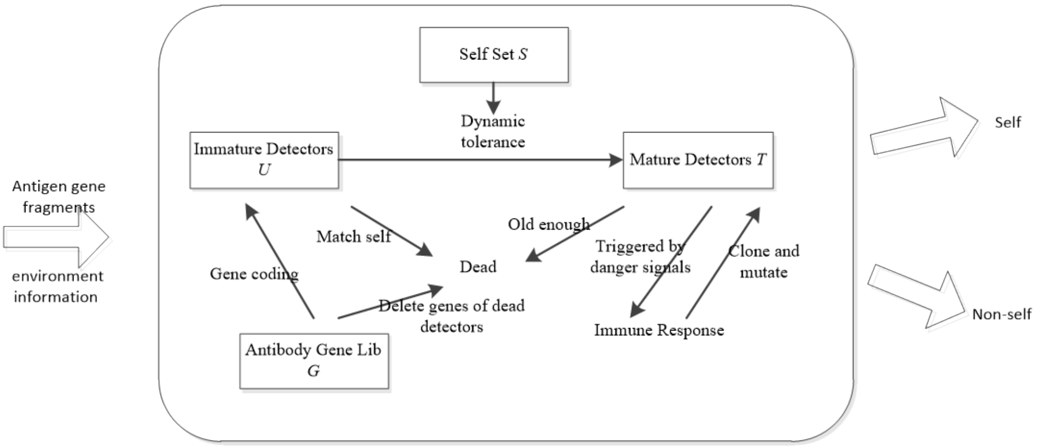


Fig. 3. The model's immune mechanism

Set of Immature detectors are expressed as $U = \{x | x \in B \cap x.age < \gamma\}$. Where γ simulates the tolerance period. The following is the evolution model of the immature detector set.

$$U(t) = \begin{cases} \emptyset, & t = 0 \\ f_{age}(U(t-1) - U_{untolerance}(t) \cup U_{matured}(t)) \cup U_{new}(t), & t > 0 \end{cases} \tag{13}$$

$$U_{untolerance}(t) = \{x|x \in f_{age}(U(t-1)) \cap \exists y \in S(t-1)(affinity(x.ab, y) = 1)\} \quad (14)$$

$$U_{matured}(t) = \{x|x \in f_{age}(U(t-1) - U_{untolerance}(t)) \cap x.age > \gamma\} \quad (15)$$

Where, $U(t), U(t-1) \subset U$ represent the immature detector sets in the time t and t-1 respectively. $f_{age}(X)(X \subset B)$ is the adding 1 operation to the age of each detector in X. $U_{untolerance}(t)$ is the set of immature detectors which do not pass the self-tolerance. $U_{matured}(t)$ is the set of immature detectors which pass the self-tolerance. $U_{new}(t)$ the set of immature detectors which are newly generated in the time t. $S(t)$ is the self set in the time t. Set of mature detectors are expressed as $T = \{x|x \in B \cap \gamma \leq x.age < age_{max} \cap \forall ag \in S(Affinity(ag, x.ab) > \theta)\}$. The following is the evolution model of the mature detector set.

$$T(t) = \left\{ \begin{matrix} \emptyset, \quad t = 0 \\ (f_{age}(T(t-1)) - (T_{dead}(t) \cup T_{cloned}(t))) \cup U_{matured}(t) \cup T_{permutation}(t), \quad t > 0 \end{matrix} \right\} \quad (16)$$

$$T_{dead}(t) = \{x|x \in f_{age}(T(t-1)) \cap x.age = age_{max} \cap \nexists y \in N(t-1)(x \in D(y))\} \quad (17)$$

$$T_{cloned}(t) = \{x|x \in (f_{age}\big(T(t-1)\big) - T_{dead}(t)) \cap \exists y \in N(t-1)(x \in D(y))\} \quad (18)$$

$$T_{permutation}(t) = f_{clone\_mutation}(T_{cloned}(t) \cup M_{cloned}(t)) \quad (19)$$

Where, $T(t), T(t-1) \subset T$ represent the mature detector sets in the time t and t-1 respectively. $T_{dead}(t)$ is the set of mature detectors which are not activated when the life cycle ends. $T_{cloned}(t)$ is the set of mature detectors which are activated by danger signals. $U_{matured}(t)$ the set of mature detectors which are newly matured. $T_{permutation}(t)$ is the set of mature detectors which are newly generated by clone and mutation operations. $f_{clone\_mutation}(X)(X \subset T)$ is the clone selection function, and performs clone and mutation operations on each detector in X.

In the process of antibody tolerance, if $Affinity(ag, x.ab) = 1$, the immature detector can describe self which triggers immune self-reaction, and must be removed; after the generation process, remaining detectors only describe elements in the non-self collection. In the process of intrusion detection, if $Affinity(ag, x.ab) = 1$, the antigen *ag* can be described by the detector *x*, which means *ag* belongs to the non-self space, and intrusion occurs. In the event of an invasion, response measures, including speed limit, isolation, and human intervention etc., are taken.

4. Performance Analysis

4.1 Complexity Analysis

This section analyzes the resource consumptions of the model from three aspects, the computational complexity, storage and communication traffic.

In this model, the computational complexity of sensor nodes obtaining danger signals from current environment is $O(|L|)$, the complexity of the sink node calculating values of danger signals and the radiuses of danger zones is $O(|L|)$, the complexity of sensor nodes performing antigen presenting is $O(|L|)$, and the complexity of the sink node conducting immune response is $O(|L|^2)$. So the computational complexity of this algorithm is $O(3|L| + |L|^2)$, and $|L|$ is the number of nodes in the system.

For sensor nodes, only the values of danger signal attributes need to be stored, and the storage complexity is $O(|DS|)$. For the sink node, it is required to maintain and store the antibody set, and the storage complexity is $O(|B|)$.

In the process of intrusion detection, communications between sensor nodes do not take special data transmission channel, and run only in the node working time. The communication data contains the three tuple of sensor nodes' danger signals $<Nd_i, t, \{S_{ij}(t)| j=1,2,\ldots,5\}>$ and the three tuple of antigen presenting information $<Nd_i, t, \{(g_1, g_2,\ldots, g_m)\}>$.

4.2 Detection Efficiency Analysis

The number of all antigens in the problem space is N_{Ag}, the number of selves is N_{Self}, the number of training selves is N_s, and the number of detectors is N_d. The matching probability between any given detector and any antigen is P', which is related to the specific matching rule [6,7]. $P(A)$ is defined as the probability of event A occurring.

Theorem 1. For any detector which passes the self-tolerance, the probability of matching an undescribed self is $P_d = (1-P')^{N_s} \cdot (1-(1-P')^{N_{Self}-N_s})$. For any given non-self, the probability of correct identification is $P_{tp} = 1-(1-P')^{N_d \cdot (1-P_d)}$, the probability of wrong identification is $P_{fn} = (1-P')^{N_d \cdot (1-P_d)}$. For any given self, the probability of correct identification is $P_{tn} = (1-P')^{N_d \cdot P_d}$, the probability of wrong identification is $P_{fp} = 1-(1-P')^{N_d \cdot P_d}$.

Prove. It is known from the proposition that a given detector passes the self-tolerance, which indicates that the detector does not match any self in the self training set. Set event A is "the given detector does not match any self in the self set," and event B is "the given detector matches at least one undescribed self". $P_d=P(A)P(B)$. In the event A, the times of detectors matching with selves satisfy the binomial distribution, $X \sim b(N_s, P')$. Then, $P(A) = P(X=0) = (1-P')^{N_s}$. In the event B, the times of detectors matching with undescribed selves satisfy the binomial distribution, $Y \sim b(N_{Self} - N_s, P)$. Then, $P(B) = 1 - P(Y=0) = 1-(1-P')^{N_{Self}-N_s}$. Therefore, $P_d = P(A)P(B) = (1-P')^{N_s} \cdot (1-(1-P')^{N_{Self}-N_s})$.

Set event E is "the given non-self matches at least one detector in the set of detectors". In the event E, the times of non-selves matching with detectors satisfies the binomial distribution $Z \sim b(N_d \cdot (1-P_d), P')$. Then, $P_{tp} = P(E) = 1-P(Z=0) = 1-(1-P')^{N_d \cdot (1-P_d)}$, $P_{fn} = 1-P_{tp} = (1-P')^{N_d \cdot (1-P_d)}$.

Set event F is "the given self does not match any detector in the set of detectors". In the event F, the times of selves matching with detectors satisfies the binomial distribution $W \sim b(N_d \cdot P_d, P')$. Then, $P_{tn} = P(F) = P(W=0) = (1-P')^{N_d \cdot P_d}$, $P_{fp} = 1-P_{tn} = 1-(1-P')^{N_d \cdot P_d}$.Proved.

Fig. 4 and **Fig. 5** is the matlab simulations of Theorem 1. The detector rate $DR=P_{tp}$ and the false alarm rate $FAR=P_{fp}$ are related to the detector self-reaction rate P', the number of mature detectors N_d, the number of training selves N_s and the number of selves N_{self}. For specific matching rules, P' is a constant [29]. In particular, for r-continuous bit matching rule, $P' = 0.025625$ [29,30]. For the identified problem space, N_{self} can be viewed as a fixed value. So, we mainly consider influences of N_s and N_d on P_{tp} and P_{fp}. As can be seen from the figures, when N_s and N_d are smaller, P_{tp} is smaller and tends to 0, and P_{fp} is larger. With the increases of N_s and N_d, P_{tp} gradually increases and P_{fp} gradually decreases.

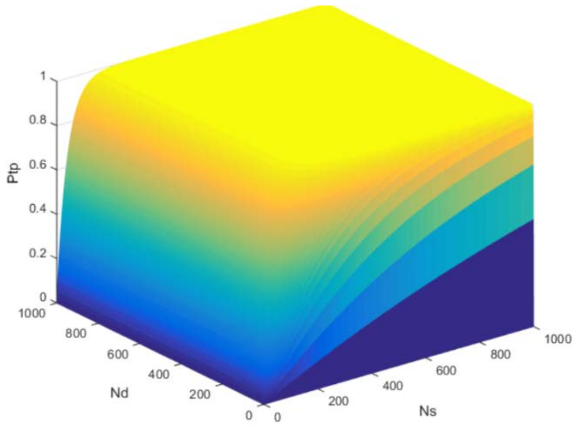


Fig. 4. The influences of N_s and N_d on P_{tp}

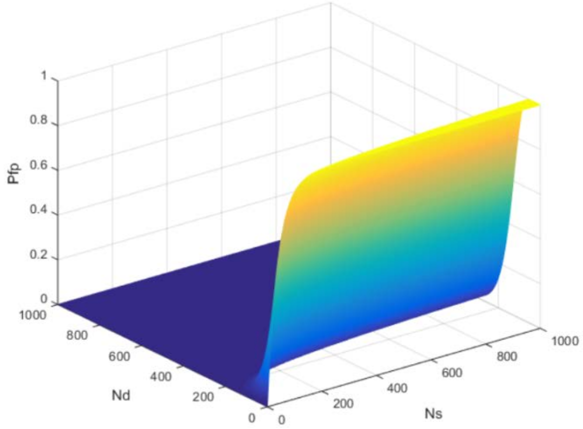


Fig. 5. The influences of N_s and N_d on P_{fp}

5. Experimental Results and Analysis

This section verifies the validity of the model through simulation experiments. Experiments use TOSSIM as the simulator for tests. It is a component-based and modular discrete event simulation tool, which is from TinyOS and suitable for the simulation of wireless sensor networks [22,23]. Sensor nodes are randomly distributed in the network and the network parameters are shown in **Table 3**.

Table 3. Experimental network parameters

parameters	defaulted values
Size of network deployment area(m^2)	1000*1000
Radius of node communication(m)	100
The number of nodes	200
MAC protocol	IEEE802.15.4
Routing protocol	LEACH
Communication rate(kbps)	250
Length of data packets(byte)	128
Interval of detection time(s)	60

Attacks on the wireless sensor network are mostly one or several-mixed types. We choose several common attacks for the experiments, including resource depletion attack, sybil attack, selective forwarding attack, wormhole attack, sinkhole attack, etc. Experiments are performed under the above five kinds of attacks, each attack runs 10 times for simulations, changes of the network within 2 hours are collected, and averaged results were acquired.

Experiments use the detection rate *DR*, the false positive rate *FAR* and the system energy consumption index *EC* to measure the performance of the model, and compare with the SNS model. The SNS model [14] is a wireless sensor network intrusion detection model based on the artificial immune, which adopts the traditional theory of self-nonself, and runs an intrusion detection system on each node. The SNS model judges whether the invasion occurs through the clone selection algorithm, and each node judges separately. SNS model's parameters are set as follows. The matching length r=7, the size of self-library is 256, the size of detector collection is 128, the initial value of matching threshold is 8, and the initial value of detector survival is 2.

5.1 Deployment of the Proposed Model on 802.15.4

IEEE 802.15.4 is a wireless communication network with low energy consumption, simple structure and easy implementation [29]. It provides a detailed description of the physical layer and MAC layer of wireless sensor networks. In this network, according to the communication capability and hardware condition of the device, it can be divided into full-function device (FFD) and reduced-function device (RFD). Compared with RFD, FFD is much better than RFD in terms of hardware. For example, FFD uses direct power, while RFD uses battery power; in terms of communication, FFD can communicate with all other FFD and RFD, while RFD can only communicate with FFD associated with it. In general, we call this FFD a coordinator for the RFD device. Throughout the network, an FFD acts as the network coordinator.

It can be seen that there is a natural stratified structure in IEEE 802.15.4. We can use the point-to-point topological structure to cluster the network. RFD can be regarded as the cluster member, FFD can be regarded as the cluster head, and the PAN coordinator can be regarded as the sink node. According to the proposed model architecture, the risk perceiving module and antigen presenting module can be deployed on RFD and FFD, and decision and response modules can be deployed on the PAN coordinator.

IEEE 802.15.4 includes the following requirements. Four different transmission rates are realized at different carrier frequencies. The CSMA/CA mechanism is used to solve the channel collision problem, and the ACK feedback mechanism is used to ensure reliable transmission of data. Therefore, the environmental status required to extract the danger signals and the data packets used for presenting antigens can be obtained locally by RFD and FFD.

ZigBee technology is based on the IEEE 802.15.4 [30]. According to the specifications of ZigBee alliance, ZigBee extended the network layer and application layer on the basis of IEEE 802.15.4. Therefore, the proposed model can also be conveniently deployed on the ZigBee network.

5.2 Parameter Settings

Table 4 lists comparisons of detection rates and false alarm rates of the model under different danger thresholds ε when a node is attacked in the network. **Table 5** lists the performance comparisons of the model when 16 nodes in the network are attacked. The comparison here is to obtain a reasonable parameter value, and the system is in the learning stage. We examine the system status in the cases of fewer nodes under attacks and more nodes under attacks, and the system can get better results with parameters in a certain interval. 16 is not an absolute number, but to show more nodes being attacked. In the real network, a case of more than 10 attack nodes can be seen more. It is shown that when the danger threshold is small, the model has a high detection rate and the false alarm rate is basically zero. At this time, the sink node receives more danger signals, and sensor nodes and the sink node communicate frequently, which increases the system's energy consumption. When the danger threshold is large, the detection rate of the model decreases. At this time, when the number of attacked nodes is less, the false alarm rate is nearly zero, and when the number of attacked nodes is more, the false alarm rate increases. Danger signals from each sensor node have been accumulated over a long period of time. Although it can reduce energy consumption, it affects the real-time of the system. Therefore, the danger threshold is more appropriate between 0.3 and 0.5.

Table 4. Effects on the model of different danger threshold 1

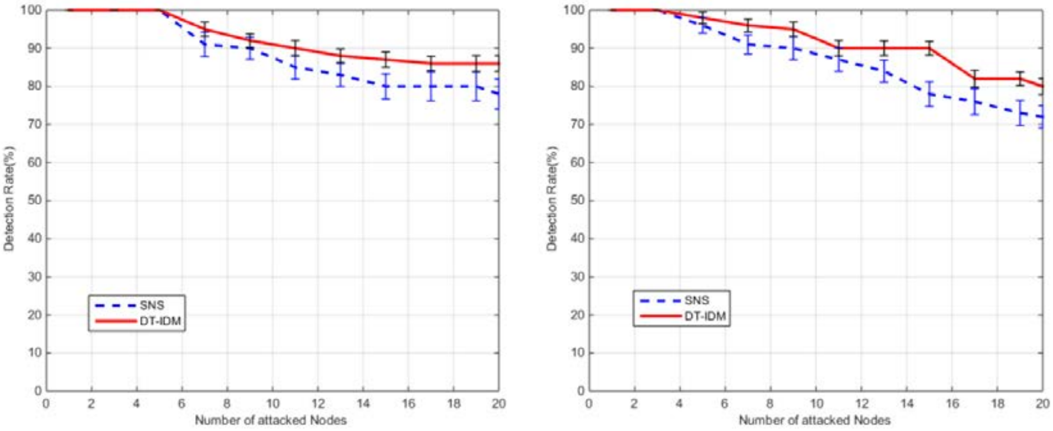
Attack types		Danger thresholds ε							
		0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
Resource depletion attack	DR%	100	100	100	100	99.11	96.24	92.16	90.37
	FAR%	0	0	0	0	0.21	0.13	0.63	1.20
Selective forwarding attack	DR%	100	100	100	100	100	94.21	89.12	88.45
	FAR%	0	0	0	0	0	3.25	2.32	4.56
Sybil attack	DR%	100	100	100	100	98.20	95.43	92.47	88.32
	FAR%	0	0	0	0	0.65	0.79	2.34	4.89
Sinkhole attack	DR%	100	100	100	100	100	100	99.33	98.43
	FAR%	0	0	0	0	0	0	1.21	1.80
Wormhole attack	DR%	100	100	100	100	96.44	94.31	92.12	89.46
	FAR%	0	0	0	0	0.63	0.99	2.86	3.75

Table 5. Effects on the model of different danger threshold 2

Attack types		Danger thresholds ε							
		0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
Resource depletion attack	DR%	100	93.04	90.54	88.0	87.32	80.12	70.39	69.18
	FAR%	0	2.10	4.91	7.90	8.11	11.76	15.33	20.92
Selective forwarding attack	DR%	100	96.33	92.55	90.03	88.32	85.66	80.13	76.65
	FAR%	0	2.02	3.23	4.54	5.49	10.87	15.61	15.33
Sybil attack	DR%	100	90.54	85.14	82.63	79.15	76.20	70.11	65.38
	FAR%	0	3.67	4.17	8.23	9.78	12.74	16.20	25.78
Sinkhole attack	DR%	100	96.21	95.14	90.47	90.08	86.81	80.11	79.41
	FAR%	0	2.05	3.08	5.28	5.0	8.22	13.64	15.62
Wormhole attack	DR%	100	90.07	82.17	80.23	75.63	74.11	65.44	60.10
	FAR%	0	5.14	8.09	10.14	12.77	12.79	18.91	28.49

5.3 Comparisons of Detection Rates

Fig. 6 shows *DR* contrasts of the DT-IDM model and the SNS model under the selective forwarding attack and the sybil attack. The short vertical lines are standard variations. As can be seen from the figure, the DT-IDM model has better detection performance. When the number of attacker nodes is small, the DT-IDM model and the SNS model can accurately detect the invasion. While the number of attacker nodes increases, two models' *DRs* decline. But in the DT-IDM model, multiple nodes within the scope of the danger zone work together to present antigens, and can accurately capture the invasion flow. So, it has better detection rate in the massive invasion.



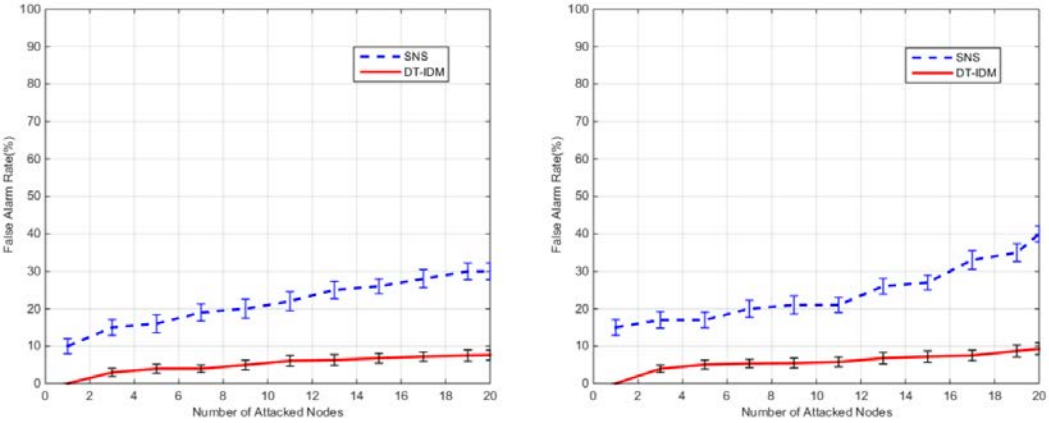
(a) Under the selective forwarding attack

(b) Under the sybil attack

Fig. 6. Comparisons of detection rates of DT-IDM and SNS

5.4 Comparisons of False Alarm Rates

Fig. 7 shows *FAR* contrasts of the DT-IDM model and the SNS model under the sinkhole attack and the resource depletion attack. The short vertical lines are standard variations. As can be seen from the figure, the DT-IDM model has better detection performance. When the number of attacker nodes is small, *FARs* of the DT-IDM model and the SNS model are low. While the number of attacker nodes increases, two models' *FARs* increase. In the intrusion detection process, sensor nodes of the DT-IDM model send danger signals, and then sink node gathers comprehensive global information to make decisions and calculate the danger zone, and finally antigen presenting is implemented. Before the antigen presenting, the sink node performs the global investigation. So, the false alarm rate of the DT-IDM model is lower.



(a)Under the sinkhole attack

(b) Under the resource depletion attack

Fig. 7. Comparisons of false alarm rates of DT-IDM and SNS

5.5 Comparisons of Energy Consumptions

In the SNS model, sensor nodes need to monitor network traffic constantly, so they are set in promiscuous mode and the energy is consumed all the time. In the DT-IDM model, danger perceiving module and antigen presenting module do not take up the special data transmission, only run in the normal working time. Research shows that the energy consumption of implementing commands for the sensor is far less than the energy consumption of transmitting data [1-5]. So, we mainly consider the energy consumptions of sending and receiving data, which can be calculated by the following equation.

$$Energy\ Comsumputation = N_{byte}*V*(N_{send}*I_{send}+N_{recv}*I_{recv})/Rate \tag{20}$$

N_{byte} is the number of bits of each packet, V is the voltage of sensors, I_{send} is the sending current, I_{recv} is the receiving current, $Rate$ is the network transmission rate, and N_{send} and N_{recv} are the numbers of packets which the node sends and recives.

Fig. 8 describes the energy consumption contrasts with or without a detection system in the wireless sensor networks. The first column shows the value of the energy consumption without invasion and without the detection system, the second shows the value under the intrusion detection system and without invasion, the third shows the value under the invasion and without the intrusion detection system, and the fourth shows the value under the invasion and the intrusion detection system. The invasion of the network is the resource depletion attack on a node. As can be seen from the figure, a 147% increase is shown when IDS is applied in the network which is from a low base and nearly does not affect the system, whereas when an attack is initiated the whole network increases with 2195% energy consumption. Finally, applying the proposed IDS saves an energy consumption of more than 1902%. When the network is deployed the DT-IDM model, the system energy consumption increases slightly with no invasion, and the consumption is greatly reduced under invasion.

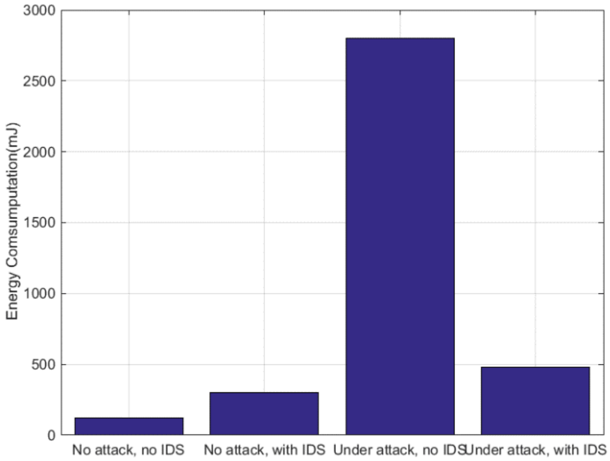


Fig. 8. The energy consumption contracts

Fig. 9 describes the energy consumption contrasts of the DT-IDM model and the SNS model under the resource depletion attack. The short vertical lines are standard variations. As can be seen from the figure, while the number of attacker nodes increases, the energy consumptions of two models increase. When an attack is initiated, a 78% decrease is shown when DT-IDM is applied in the network compared with SNS. When 9 nodes are attacked, energy consumption of DT-IDM is decreased by 32% compared with SNS. And this value is 22% when 20 nodes are attacked. So, the DT-IDM model has obvious advantages.

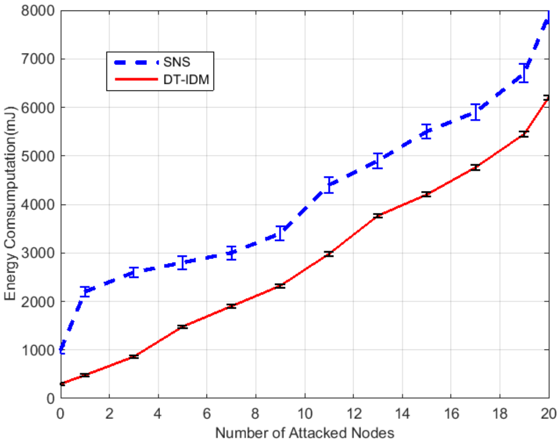


Fig. 9. The energy consumption contracts of DT-IDM and SNS

6. Conclusions and Future Works

To ensure the safety of WSNs is one of the bases that wireless sensor networks can be widely applied. This paper first analyzes the typical attacks, intrusion detection characteristics and the security research status of wireless sensor networks. Existing research on intrusion detection technology in WSNs is not very mature, and most detection systems are transplanted from traditional networks. Then, the paper proposes a distributed intrusion detection model based on danger theory for wireless sensor networks. The model simulate immune processes to eliminate external invasions. When the network perceives abnormity, the model produces danger signals. Danger signals build a danger area around them, where immune cells will be activated to participate in immune responses. At last, the performance of the model is analyzed and experimental results show that the model has good detection performance and reduces energy consumption.

The intrusion detection technology in wireless sensor networks is an important research subject, and there are many practical problems. In this paper, the next step is to apply the model to the real wireless sensor networks and to perform further validation and improvement, in order to make the model more meaningful.

Acknowledgement

The authors would like to thank the associate editor and the anonymous reviewers for their valuable comments, and to thank Sichuan provincial education department funded project (035Z2258) for providing financial aid.

References

[1] S. Biswas and S. Adhikari, “A survey of security attacks, defenses and security mechanisms in wireless sensor network,” *International Journal of Computer Applications*, vol. 131, no. 17, pp. 28-35, 2015. Article (CrossRef Link)

[2] E. Sharifi, M. Khandan, and M. Shamsi, “MAC protocols security in wireless sensor networks: a survey,” *International Journal of Computer and Information Technology*, vol. 3, no. 1, pp. 105-109, 2014. Article (CrossRef Link)

[3] P. Kour and L. C. Panwar, “A review on security challenges and attacks in wireless sensor networks,” *International Journal of Science and Research*, vol. 3, no. 5, pp. 1360-1364, 2014. Article (CrossRef Link)

[4] H. Ali, A. A. Mamun, and S. Anwar, “All possible security concern and solutions of WSN: a comprehensive study,” *International Journal of Computer Science and Technology*, vol. 6, no. 4, pp. 64-74, 2015. Article (CrossRef Link)

[5] D. Singla and C. Diwaker, “Analysis of security attacks in wireless sensor networks,” *International Journal of Software and Web Sciences*, vol. 14, pp. 26-30, 2014. Article (CrossRef Link)

[6] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, “Self-nonself discrimination in a computer,” in *Proc. of the IEEE Symposium on Research in Security and Privacy*, Oakland: IEEE Computer Society Press, pp. 202-212, 1994. Article (CrossRef Link)

[7] J. Balthrop, F. Esponda, S. Forrest, et al, “Coverage and generalization in an artificial immune system,” in *Proc. of he the 4th Annual Conference on Genetic and Evolutionary Computation*, New York, Morgan Kaufmann Publishers Inc, pp. 3-10, 2002. Article (CrossRef Link)

[8] I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in *Proc. of IEEE International Conference on Wireless & Mobile Computing, Networking & Communications*, vol. 3, no. 4, pp. 587-594, 2005. Article (CrossRef Link)

[9] R. Roman, J. Zhou, and J. Lopez, “Applying intrusion detection systems to wireless sensor networks,” in *Proc. of IEEE Consumer Communications & Networking Conference*, vol. 1, pp. 640-644, 2006. Article (CrossRef Link)

[10] D. Martynov, J. Roman, S. Vaidya, and H. Fu, “Design and implementation of an intrusion detection system for wireless sensor networks,” in *Proc. of IEEE International Conference on Electro/Information Technology*, Chicago, vol. 3, no. 5, pp. 507-512, 2007. Article (CrossRef Link)

[11] M. Drozda, S. Schaust, and H. Szczerbicka, “AIS for misbehavior detection in wireless sensor networks: performance and design principles,” *IEEE Congress on Evolutionary Computation*, Singapore, pp. 3719-3726, 2007. Article (CrossRef Link)

[12] S. Schaust, and H. Szczerbicka, “Applying antigen-receptor degeneracy behavior for misbehavior response selection in wireless sensor networks,” *Artificial Immune Systems, ICARIS 2011*, Lecture Notes in Computer Science, vol. 6825, Springer, Berlin, Heidelberg. Article (CrossRef Link)

[13] J. Kim, P. Bentley, C. Walenta, et al, “Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm,” *Artificial Immune Systems, ICARIS 2006*, Lecture Notes in Computer Science, vol. 4163, Springer, Berlin, Heidelberg. Article (CrossRef Link)

[14] M. Wazid, and A. K. Das, “An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks,” *Wireless Pers Commun*, vol. 90, pp. 1971-2000, 2016. Article (CrossRef Link)

[15] T. Ma, F. Wang, J. Cheng, et al, “A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks,” *Sensors*, vol. 16, no. 10, pp. 1701-1724, 2016. Article (CrossRef Link)

[16] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, “Real-time multi-agent system for an adaptive intrusion detection system,” *Pattern Recognition Letters*, vol. 85, pp. 56-64, 2017. Article (CrossRef Link)

[17] P. Matzinger, “The danger model: a renewed sense of self,” *Science*, vol. 296, pp. 301-305, 2002. Article (CrossRef Link)

[18] S. X. Wu, and W. Banzhaf, “The use of computational intelligence in intrusion detection systems: a review,” *Applied Soft Computing*, vol. 10, no. 1, pp. 1-35, 2010. Article (CrossRef Link)

[19] U. Aickelin, P. Bentley, S. Cayzer, et al, “Danger theory: the link between AIS and IDS?,” *Artificial Immune Systems, ICARIS 2003*, Lecture Notes in Computer Science, vol 2787. Springer, Berlin, Heidelberg, 2003. Article (CrossRef Link)

[20] M. Gunasekaran and S. Periakaruppan, "GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN," *Security and Communication Networks*, vol. 2017, Article ID 9863032, 10 pages, 2017. Article (CrossRef Link)

[21] Y. B. Chen, C. Feng, Q. Zhang, et al, "Integrated artificial immune system for intrusion detection," *Journal of Communications*, vol. 33, no. 2, pp. 125-131, 2012. Article (CrossRef Link)

[22] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: accurate and scalable simulation of entire TinyOS applications," in *Proc. of SenSys '03 Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, ACM Press, pp.126-137, 2003. Article (CrossRef Link)

[23] V. C. Chandanashree, U. P. Bhat, P. Kanade et al, "Tinyos based WSN design for monitoring of cold storage warehouses using internet of things," in *Proc. of 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, 2017. Article (CrossRef Link)

[24] Z. Lai, M. Wang, and J. Yin, "Survey on wireless sensor network security," *Electronic Measurement Technology*, vol. 12, pp. 78-84, 2010. Article (CrossRef Link)

[25] V. C. Sekhar, and M. Sarvabhatla, "Security in wireless sensor networks with public key techniques," in *Proc. of International Conference on Computer Communication & Informatics*, pp. 1-16, 2012. Article (CrossRef Link)

[26] R.W. Anwar, M. Bakhtiari, A. Zainal, et al, "A survey of wireless sensor network security and routing techniques," *Research Journal of Applied Sciences Engineering & Technology*, vol. 9, no. 11, pp. 1016-1026, 2015. Article (CrossRef Link)

[27] Q. Shi, L. Qin, L. Song, et al, "A dynamic programming model for internal attack detection in wireless sensor networks," *Discrete Dynamics in Nature and Society*, vol. 2017, Article ID 5743801, 9 pages, 2017. Article (CrossRef Link)

[28] M. Zeeshan, H. Javed, A. Haider, et al, "An immunology inspired flow control attack detection using negative selection with r-contiguous bit matching for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 169654, 7 pages, 2015. Article (CrossRef Link)

[29] IEEE 802.15.4, http://standards.ieee.org/findstds/standard/802.15.4e-2012.html

[30] ZigBee, http://www.zigbee.org/

[31] Y. Li, C. Tang, S. Peeta, et al, "Nonlinear Consensus-Based Connected Vehicle Platoon Control Incorporating Car-Following Interactions and Heterogeneous Time Delays," *IEEE Transactions on Intelligent Transportation Systems*, 2018. Article (CrossRef Link)

[32] Y. Li, C. Tang, K. Li, et al, "Consensus-Based Cooperative Control for Multi-Platoon Under the Connected Vehicles Environment," *IEEE Transactions on Intelligent Transportation Systems*, 2018. Article (CrossRef Link)

[33] Y. Li, C. Tang, S. Peeta, et al, "Integral-Sliding-Mode Braking Control for Connected Vehicle Platoon: Theory and Application," *IEEE Transactions on Industrial Electronics*, 2018. Article (CrossRef Link)

Xin Xiao (http://orcid.org/0000-0001-8703-4243 (ORCID ID))
She received B.S., M.S., Ph.D. degrees in School of Computer Science from Sichuan University in 2004, 2009, and 2015 respectively. Her current research interests include network security, wireless sensor networks, and artificial immune systems.

Ruirui Zhang (http://orcid.org/0000-0003-1898-1487 (ORCID ID))
She received B.S., M.S., Ph.D. degrees in School of Computer Science from Sichuan University in 2004, 2007, and 2012 respectively. Her current research interests include network security, wireless sensor networks, and artificial immune systems.