algorithms

MDPI

Article

Adaptive and Lightweight Abnormal Node Detection via Biological Immune Game in Mobile Multimedia Networks

Yajing Zhang [1], Kai Wang [2,*] and Jinghui Zhang [1]

[1] School of Computer and Control Engineering, Yantai University, Yantai 264005, China; yajing_zh@163.com (Y.Z.); ytcola@126.com (J.Z.)
[2] School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China
* Correspondence: dr.wangkai@hit.edu.cn

Abstract: Considering the contradiction between limited node resources and high detection costs in mobile multimedia networks, an adaptive and lightweight abnormal node detection algorithm based on artificial immunity and game theory is proposed in order to balance the trade-off between network security and detection overhead. The algorithm can adapt to the highly dynamic mobile multimedia networking environment with a large number of heterogeneous nodes and multi-source big data. Specifically, the heterogeneous problem of nodes is solved based on the non-specificity of an immune algorithm. A niche strategy is used to identify dangerous areas, and antibody division generates an antibody library that can be updated online, so as to realize the dynamic detection of the abnormal behavior of nodes. Moreover, the priority of node recovery for abnormal nodes is decided through a game between nodes without causing excessive resource consumption for security detection. The results of comparative experiments show that the proposed algorithm has a relatively high detection rate and a low false-positive rate, can effectively reduce consumption time, and has good level of adaptability under the condition of dynamic nodes.

Keywords: mobile multimedia network; node security; abnormal detection; artificial immunity; game theory

check for updates

Citation: Zhang, Y.; Wang, K.; Zhang, J. Adaptive and Lightweight Abnormal Node Detection via Biological Immune Game in Mobile Multimedia Networks. *Algorithms* **2021**, *14*, 368. https://doi.org/10.3390/a14120368

Academic Editor: Lijun Chang

Received: 16 October 2021
Accepted: 17 December 2021
Published: 20 December 2021

1. Introduction

In recent years, with the development of Internet of Things (IoT) technology, IoT devices have become the mainstream devices of network terminals. Meanwhile, due to the surge in the volume of mobile multimedia services, multimedia data have become one of the most important sources of data traffic in networks [1]. To deal with the large volume of multimedia data generated by the huge amount of IoT devices in an effective and efficient way, mobile edge computing technology is becoming increasingly popular, which deploys computing and storage edge nodes in large numbers in order to improve mobile application capacity and reduce the response time of devices as well as the wireless back-trip network bandwidth pressure.

In mobile edge computing scenarios, most of the wireless or mobile networks are open physical systems that use radio frequency technology for network connectivity and transmission. Therefore, in addition to the security problems shared by wired networks, wireless networks have several unique security threats. The transmission of multimedia data in wireless networks has its inherent difficulties, such as channel quality time change, mobile terminal heterogeneity, and limited wireless resources [2]. The emergence of edge computing alleviates these problems in terms of resource utilization. However, the wireless and open nature of mobile multimedia networks makes multimedia data vulnerable to malicious attacks. An attacker can easily intercept a user's data or directly attack the network. As a result, security in mobile multimedia data transmission has received increased attention [3].

These threats manifest themselves in three areas [4], as shown in Figure 1, which are also the key concerns in the design of security mechanisms for wireless or mobile networks to support multimedia communications or other services.

(1) Physical layer. This mainly includes the threat of environment security, equipment security, and the threat caused by the malicious damage of the attackers, such as:

- Stealing a user's device: when a wireless card is lost or stolen, an illegal user can breach an access point;
- Wireless interference: interference with the normal operation of the wireless channel by transmitting a large power-to-frequency signal.

(2) Data link layer. This mainly includes spoofing based on MAC addresses, such as:

- Eavesdropping and listening: electronically eavesdropping on computer communications flowing through wireless networks;
- Spoofing attacks: redefining the MAC address of a wireless network or network card.

(3) Network layer. This includes various attacks from the network, such as:

- Inserting an attack: impersonating a legitimate user, accessing an information system through a wireless channel, and gaining control;
- Denial of service: an attacker maliciously occupies almost all resources of the host or network, making them unavailable to legitimate users;
- A network takeover: an attacker takes over a wireless network or session process, allowing all traffic to reach the attacker's machine;
- Energy consumption: the destruction of energy-saving mechanisms, such as by constantly sending connection requests, preventing the device from entering the energy-saving mode.

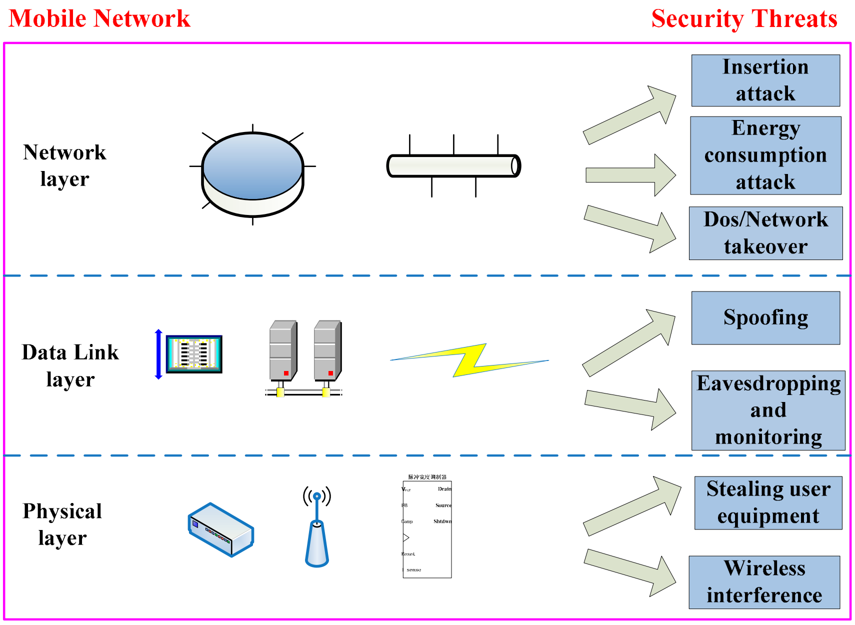


Figure 1. Security threats of mobile network.

For wireless network security threats, mobile network servers are generally sufficient to support the setup of security measures. However, the power and processing capacity of sensor nodes located within the edge networks are typically low, leaving a small power budget for security measures. A large number of low-cost, energy-limited nodes deployed in uncontrollable areas and a complex, harsh application environment can lead to a variety of failures that reduce or eliminate monitoring functions, causing economic loss to users, and even network paralysis [5]. Therefore, detection of abnormal nodes is particularly important.

For convenience of expression in the subsequent sections of this article, an abnormal node can also be called a failure node. In the field of detection of abnormal nodes research, Kumar Niteth has proposed a distributed fault detection and recovery algorithm [6], which can effectively detect relay node failure. In this algorithm, any failed relay node is identified by its neighbors according to the neighborhood table associated with them. The algorithm complexity is high. Chafiq Titouna has proposed a fault detection scheme for the identification of faulty sensor nodes [7]. In this scheme, the coordination between the two execution levels is not well structured and the simulation process is too idealized. Bill et al. has suggested a wireless sensor network hardware fault detection method using a simple Bayes framework for detecting node energy failure [8]. However, data cannot be collected in real time when a fault occurs, nor can the fault feature be extracted in real time. A cluster-based fault detection algorithm has been proposed by Wenbo Zhang, in which a node confidence mechanism is introduced [9]. The disadvantage is that only dynamic tolerance is considered, and dynamic detection is not performed.

From the perspectives of intelligence and automation, mobile multimedia network nodes have the characteristics of real-time, dynamic, and multi-source data, and node security must consider the dynamic changes of data in real time. In the literature mentioned above, most of the proposed algorithms are static detection algorithms based on data. These algorithms do not consider the difference in abnormal data characteristics caused by data dynamics and multiple sources.

The biological immune system has information processing mechanisms, such as memory learning, feedback regulation, and decentralized and distributed autonomous mechanisms. An artificial immune system established according to biological immune theory includes methods such as immune recognition, immunology learning, immune memory, and cloning selection. Both the biological immune system and a distributed self-organizing wireless sensor network maintain system stability in a changing environment. The immune system structure provides a novel solution to the problem of node security in a mobile network.

Tiong Hoo Lim has proposed an immuno-inspired algorithm for node failure [10]. The proposed immune excitation scheme that uses a multimodal mechanism has good reliability, but the operating environment it adapts to is specific, not universal. Salmon has proposed collaborative monitoring and intrusion detection mechanisms inspired by the body's immune system [11]. It allows nodes to monitor their neighbors and collaborate to identify intruders. The defect of this algorithm is that it does not consider the correlation and response mechanism between nodes, which leads to a large resource occupation. Li et al. has proposed an immune intrusion detection mechanism for a wireless sensor network tree structure [12]. Two immunization strategies, namely unified immunization and temporary immunization, are studied in sensor viruses. The algorithm is only effective for a single sensor virus attack and not for most attacks. Amir Jabbari et al. have introduced an optimized neuro-immune system to predict sensor records [13]. In this method, only the immune theory is used to establish the network model, and no further research was done on the abnormal detection of nodes. Author has done some previous work about abnormal detection with immune theory, including negative selection, clone selection, vaccine and detector's research [14]. The contribution of this literature is the construction of an IDS inspired by biological immune principles and functions, such as resisting viruses and their variations in the biological immune system. The immune idea is incorporated into the design of IDS, and an intrusion detection system that can detect novel attacks adaptively under the premise of lower data requirements is constructed. Thus, the security of the edge computing scenario is improved.

The above literature has introduced the principle of immunity to the intrusion detection system, and used the non-specific principle of immunity to effectively solve the dynamic change of data and multi-source problems. However, the randomness in immune data extraction and antibody library generation inevitably makes the data resources too huge and reduces the real-time performance of the system.

In order to solve the above problems, this paper studies the detection of abnormal edge nodes in a mobile multimedia networking scenario based on artificial immunity theory and game theory. Negative selection, clonal selection, and vaccines are used to generate an antibody library. A niche strategy is used to determine the risk area, and antibody division prevents the algorithm from falling into local optima. The antibody library can be updated online with abnormal data, and can dynamically detect nodes. The security of nodes in a networked environment depends both on themselves and on other nodes. Therefore, this paper uses the game theory method to establish the immune game model on the premise of meeting the safety performance requirements of the system. Under the premise of known abnormal nodes, the problem of resource optimization in the process of node detection and recovery is studied and solved through the game between nodes. Thus, the deployment cost of the system is reduced.

The rest of this paper is organized as follows. Section 2 presents the background of immune game theory. Section 3 describes the basic idea of the immune game algorithm. The game model is established based on the Nash game theory. An immune game mechanism is proposed for detection of abnormal nodes. Section 4 provides simulation experiments. The detection rate, false detection rate, network stability time, and reliability are compared and studied. Section 5 draws conclusions and discusses future research directions.

2. Background of Immune Game Theory

2.1. Artificial Immune Theory

Two theories are associated with artificial immunity: *self/nonself* (SNS) and danger theory (DT).

(1) SNS theory

In 1994, Forrest proposed the SNS theory [15], which strictly divides cells and molecules in the immune body into their own cells and allogeneic cell molecules, including foreign viruses, bacteria, and mutated cells. All cell molecules can be defined as a collection U, consisting of a set N of viruses, bacteria, and mutated cells from the outside world, and a set S of their own cells, satisfying

$$S \cap N = \varnothing, S \cup N = U \tag{1}$$

In the SNS mode, antibody cells in the body judge between the cells. Once the antibody cells judge a cell as a foreign cell, the corresponding elimination process will be carried out. On the contrary, if all antibody cells do not match the cell, it is judged to be an autologous cell. According to the above analysis, the SNS theory of self-body and allogeneic cells should satisfy formula (2). Let f be a binary classification function of, and define Ab as an antibody set gained by constantly learning access data in the mechanism of the immune system. If u is set to a conventional value, i.e., u∈U, then

$$f(Ab, u) = \begin{cases} u \in N,\ when\ Ab\ matches\ u \\ u \in S,\ others \end{cases} \tag{2}$$

(2) DT theory

DT theory was first proposed by Matzinger in 1994 [16]. The theory holds that the immune system produces the corresponding protective mechanism according to the sensitivity of the danger signal. Immune response is a response to the process of cell death. The generation and detection of danger signals are closely related to immune biochemical reactions [17].

As shown in Figure 2 dendritic cell (DC) in the biological immune system is an antigen-presenting cell that ingests antigens in tissues and presents antigen fragments. Immature dendritic cells (DCs) receive both safe and dangerous signals from the environment wherein antigens are present. Then, it divides into mature and semi-mature cells. The proportion of mature antigens to total antigens ultimately determines whether there is a danger.

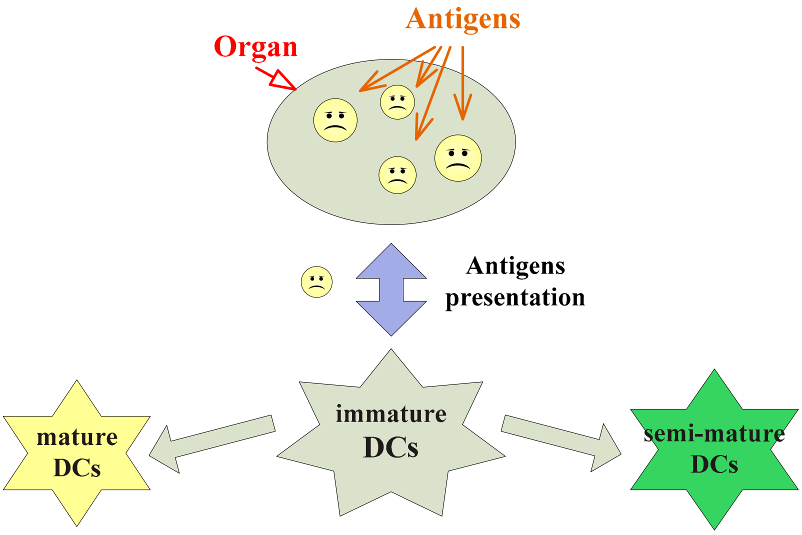


Figure 2. Danger theory of immune system.

The DT theory states that the immune system of a living organism does not distinguish all antigens as either self or foreign. In contrast, the theory of immune risk states that the immune system only responds to harmful antigens, which greatly reduces the scale of response and makes it more practical. In addition, the immune risk theory and the traditional artificial immunity theory can also recognize and immunize the mutated antigens by updating the antibody library.

DT theory holds that damaged, apoptosis, and abnormal death cells caused by an antigen attack will transmit a red flag to antigen-presenting cells (APCs), which will create a hazardous area. At the same time, antibodies that match the danger area are activated and cloned for secondary immunity. The immune process is shown in Figure 3.

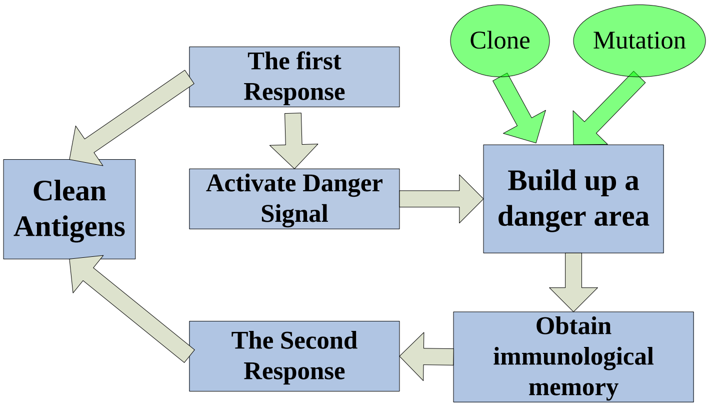


Figure 3. Immune process.

SNS theory divides matter into auto and foreign bodies, so abnormal detection requires the production of antibodies that match all foreign bodies, i.e., detectors. To cover all foreign antigens, the system requires a large number of detectors. In contrast, DT theory divides antigen substances into harmful and harmless antigens; hence measures will only be taken against antigens that may be dangerous to the body. For example, no response will be produced against food that is ingested.

In view of the huge, multi-source characteristics of mobile multimedia network data, the immune principle adopted in this paper is based on DT theory, and only the harmful antigens are immunized, which can effectively reduce resource consumption and save computation time. It ensures data security and communication fluency of network nodes.

2.2. Game Theory

Game theory studies the strategy and decision-making problems of two or more participants, emphasizing the direct interaction between the behaviors of decision subjects.

A complete game structure should contain the elements of a player, strategy set, and payoff function or utility function [18].

(1) Player

The multiple players in the game model refer to the parties involved in the game. It is the decision-making body of the game model and the maker of the game strategy. The participants have independent decision-making ability and are responsible for the corresponding consequences. P represents a set. Participants may be individuals or groups or groups with common interests.

(2) Strategy set

The strategy collection includes strategies that decision-making individuals may adopt. S_i is the policy set of participant i. It should contain at least two policies, and must be a practical action plan.

(3) Payoff function

Under the game set of specific rules, the expected income obtained by decision-making individual i is represented by payment function U_i. Utility refers to the gains and losses of participants. Decision-making individuals use different strategies to obtain different results. The result is influenced by strategies of all decision-making individuals. Utility functions represent the level of income of different decision-making individuals, and are functions of the strategies of all such individuals.

The game model is established by the attack and defense of both sides, strategy set, and utility function as

$$\mathrm{G} = \{N, \{S_i\}, \{U_i\}\}. \tag{3}$$

- Nash Equilibrium [19]

A strategy by which the Nash equilibrium can be achieved is called optimal. This occurs when no decision-making individual can increase its benefits by changing strategy.

Nash defined equilibrium [20] as follows. For a game model $G = \{N, \{T_i\}_{i\in N}, \{U_i\}_{i\in N}\}$, N is a set of players, and S_i is a strategy selected by the ith player with utility ith U_i. The decision space is $S = \times S_i,\ i \in N$, and the utility function set is U. In G, the utility of the ith player can be represented as a function of S_i: $U(S_i, S_{-i})$, or $U(S)$, where, S_{-i} is the strategy set of players other than i in N. The strategies selected by all players form a set of strategies S. $S = [s_1, s_2, \cdots, s_N]$. When S meets the formula (4), a *Nash* equilibrium is obtained [21].

$$U_i(S) \geq U_i(s_i, s_{-i}),\ \forall i \in N,\ s_i \in S_i \tag{4}$$

In a multimedia mobile network, the operation of each node is random and mobile. The network resources occupied by the security detection and recovery of the system are uncertain. The most important point of node security is to ensure the safe operation of the node. Obviously, it is not enough to be able to detect anomalies and issue safety warnings. In order to effectively allocate network resources, a novel idea in node security is to establish the order of node detection and operation by a game based on immune detection.

Self-organization, dynamic topology, and limited resources are the main characteristics of mobile multimedia network. These characteristics determine that each node has its own decision when communicating. The network nodes are correlated. Compared with dominant-strategy equilibrium and cooperative equilibrium, it is suitable to adopt Nash equilibrium because of the non-cooperative and complete information relationship between nodes in a mobile multimedia network. Therefore, Nash equilibrium is chosen as the game strategy in this paper. In the Nash equilibrium, each node can be regarded as a player making game decisions by utility calculation.

3. Immune Game–Based Abnormal Node Detection Algorithm

3.1. Basic Idea

As we know, the node security of a mobile network ultimately reflects the system's survivability, i.e., its ability to perform critical tasks in a timely manner when certain nodes fail or are attacked [22].

Edge nodes in mobile networks have the characteristics of dynamism, randomness, multiple sources, and correlation. The traditional method of judging an abnormal node often lacks real time judgement and effectiveness. An intrusion detection system can isolate abnormal nodes, so that subsequent routes no longer pass through them. At the same time, the use of a data security detection system needs more computing resources. Compared with the current situation of limited node resources, the detection system is always in the open state, which will occupy too many resources.

Based on the theory of artificial immunity, we propose an algorithm for the detection of abnormal nodes with an adaptive function. The algorithm uses the hazard trigger threshold to identify a hazard source, generates an antibody library using an immune algorithm, classifies an abnormality according to the small habitat strategy, and updates the antibody library online according to the abnormal data. The immune game model is established, and the optimal node recovery strategy is determined under the premise of known abnormal nodes.

The research idea of this paper is as follows: the monitoring region is divided in the mobile multimedia network. The node senses the information in the monitoring area. First, the node is self-immunized. In the process of immune detection, when the abnormal threshold value is exceeded, it is preliminary determined that the node occurs abnormally. At the same time, the node sends the abnormal information to the spatially related neighbor nodes for further determination. When the two diagnoses are consistent, it is judged to be an abnormal node. If no pings are received from the neighbor node, the relay node enters the abnormal diagnosis phase. Finally, it matches results with the data database to determine whether the abnormality has occurred. If it has occurred, the treatment of the immune stage is carried out. If the abnormality is determined to be unknown, the abnormal data will be processed and features will be extracted. A new abnormal detection library is generated through the processing of the immune detection algorithm. A further update of the existing abnormal detector is executed and secondary immunity carried out when such an abnormality occurs again.

When an abnormal node is detected, the system builds a game model and treats all abnormal nodes as game participants. Each participant in the game is driven by their own interests and always wants to use the optimal strategy. At the same time, there is always inevitable competition between them. Competition and game play make these nodes closely connected, and they contest each other as well as depend on each other. The final result is to determine the recovery strategy of each node, so as to obtain real-time and effective security protection.

3.2. Detailed System Model and Problem Formulation

3.2.1. Immune Detection Algorithm

For the convenience of research, this paper assumes that the distribution region of nodes is a rectangle of size A × B. The node is composed of a sink node, an ordinary node, and a regional node. A sink node is a global control node. It has the highest network control and management rights and can carry on the unified management and deployment of the common nodes and regional nodes in the network. Ordinary nodes mainly undertake the functions of data collection, aggregation, and uploading. Regional nodes are mainly used to gather regional data and upload the data to the sink node through other regional nodes. In addition, the following assumptions are made [23]:

(1) Nodes are not fluid.
(2) Regional nodes are not sparse, i.e., a regional node can cover a rectangular area, and there is no dead-end phenomenon.
(3) The sensor identification ID is unique.
(4) Ordinary nodes in a region are similar. Ordinary nodes in different regions have some incompatibilities, and regional nodes cannot manage ordinary nodes across regions.

According to the SNS and DT theories of the artificial immune system (AIS), the mapping relationship between an artificial immune system and an abnormal node detection system (NS) is shown in Table 1.

Table 1. Corresponding relationship between AIS and NS.

Artificial Immune System	Abnormal Node Detection System
Artificial immunity	Node security
B-cells	Node
Antibody	Detector
Antigen	Feature information
Affinity between antibodies and antigens	Threshold matched
Response	Match
Antibodies are killed	Lost information
Clone	Duplication/mutation
Mature detectors	Abnormal Node affirmed
Memory detectors	Abnormal Node that often occurs

We set an n-dimensional antibody: $Ab = \begin{bmatrix} ab_1 & ab_2 & \cdots & ab_n \end{bmatrix}$.

If there are m antibodies, then every antibody has an n-dimensional character, and the antibody library can be shown as a matrix:

$$Library_{A_b} = \begin{bmatrix} Ab_1 \\ Ab_2 \\ \vdots \end{bmatrix} = \begin{bmatrix} ab_{11} & ab_{12} & \cdots & ab_{1n} \\ ab_{21} & ab_{22} & \cdots & ab_{2n} \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}. \tag{5}$$

Similarly, for antigens,

$$Library_{Ag} = \begin{bmatrix} Ag_1 \\ Ag_2 \\ \vdots \end{bmatrix} = \begin{bmatrix} ag_{11} & ag_{12} & \cdots & ag_{1n} \\ ag_{21} & ag_{22} & \cdots & ag_{2n} \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}, \tag{6}$$

where $Library_{Ag}$ is a set of antigens. A_b and A_g are vector representations of antibodies and antigens, respectively. The dimension of A_b and A_g is n.

Affinity is the degree to which antibodies bind to antigens, and it must be quantified. We use Euclidean distance to represent affinity,

$$\text{Distance} = \sqrt{\sum_{i=1}^{n} (Ab_i - Ag_i)^2}. \tag{7}$$

The greater the Euclidean distance the lower the affinity. We use affinity as a criterion to judge similar antigens and identify sources of danger. As shown in Figure 4, it is assumed that ultra-2D data are projected into two-dimensional space by nonlinear mapping of high-dimensional images. On this basis, the antibody library model is simulated as two concentric circles in two-dimensional space, whose common center is that of the antibody library, i.e., the vaccine that produces the antibody bank, expressed as

$$\text{Vaccine} = \left[\frac{ag_{11} + ag_{21} + \cdots + ag_{m1}}{m} \ldots \frac{ag_{1n} + ag_{2n} + \cdots + ag_{mn}}{m}\right] \tag{8}$$

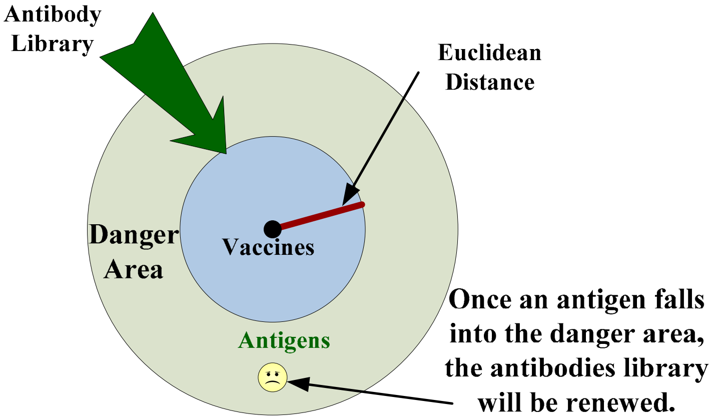

Antibody Library
Euclidean Distance
Danger Area
Vaccines
Antigens
Once an antigen falls into the danger area, the antibodies library will be renewed.

Figure 4. Mapping relation of antibody library.

The radius of the circle is based on Euclidean distance. The inner circle is the identification area, where resulting antibodies are distributed. The outer ring is the update area, and any antigens falling in this area, if conditions are met, will trigger the update of the antibody library.

- **Establishment of dangerous areas**

According to the niching strategy of biological immunity, a node is randomly identified, and the Euclidean distance from the characteristic vector of the state of other nodes is calculated. We set a small habitat threshold, and if the Euclidean distance between two nodes does not exceed the threshold, the node state is considered similar. As long as the number of nodes in the same state exceeds half the total number of nodes, such nodes are considered normal. The remaining nodes are identified as hazardous sources. The mapping relation is shown in Figure 4.

- **Fitness function**

The fitness function between Ag_i and Ab_j is

$$\text{Aff}_{i,j} = \frac{1}{\|Ab_i - Ag_j\|}\ (i = 1, 2, \cdots, N) \tag{9}$$

- **Niching strategy**

The niching strategy is to divide individuals with the same or similar adaptability. The vaccine selects only some excellent individuals and discards the rest, thus avoiding the system falling into local optimality.

- **Immune operation**

(1) Negative selection

The system extracts self-information called *self* from feature information and sets matching schemes and parameters. Information that does not match the *self* is collectively called *nonself*. Abnormal detection is done by differentiating between *self* and *nonself*.

(2) Clone, crossover, and mutation.

In biological immunity, individuals with high adaptability will be cloned as excellent genes involved in the identification of antigens. In artificial immunity, individuals with high adaptability are involved in crossovers and mutations to preserve excellent genes. Intersections are performed between two individuals, with random intersections selected for fragment exchange. Mutation is the reverse substitution of randomly selected gene points.

- **Basic idea of the algorithm**

The feature information of nodes is extracted as the measured data, and random binary data are taken as the initial population to conduct antibody training. According to the set threshold value and fitness function, a *self-nonself* operation is carried out to calculate individual fitness. According to the fitness, the corresponding string is selected for immune operation to obtain the antibody library. Antibodies in the antibody library generate vaccines through niche strategies. The vaccine responds directly to the failure node in the subsequent test. The antibody library is constantly updated in the detection process, and the vaccine is generated and replaced to form a dynamic detection mechanism.

- **Basic steps and flowchart of the algorithm**

The flowchart of the abnormal detection algorithm based on immunity is shown in Figure 5.

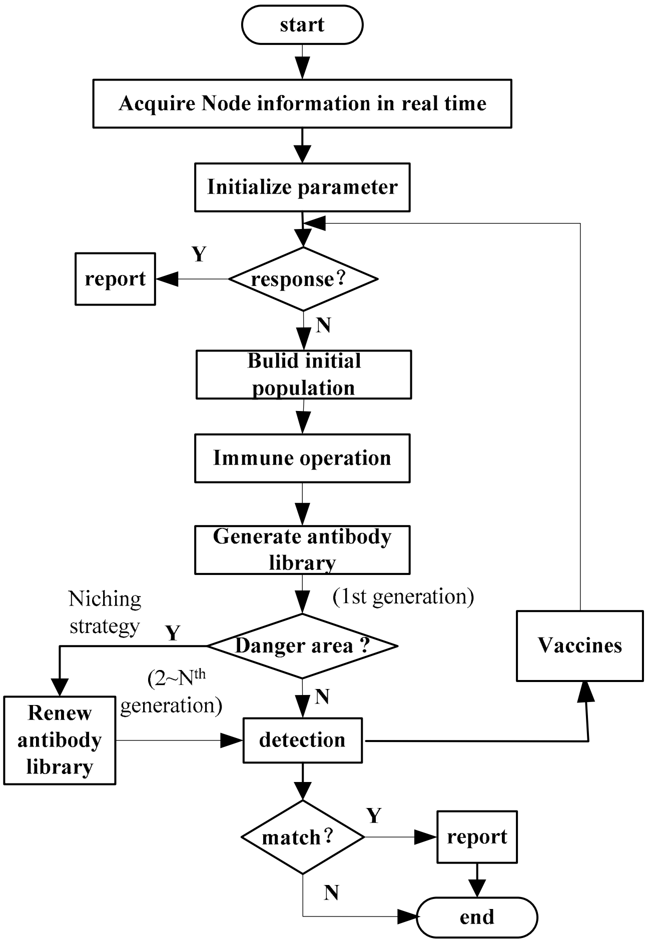


Figure 5. Flowchart of immune algorithm.

Step 1: Initialization parameters

This includes node data extraction and binary encoding. In the mobile network, the node detection area is selected. The node characteristic information can be obtained from the node key file. After the information is obtained, the data must be binary encoded.

Step 2: Obtain the initial population

A randomly coded antibody library is established. The fitness function is imputed. Negative selection and clone selection are used to respond to node characteristic data. Thus, the initial population is obtained.

Step 3: Establishment of antibody library

The individual fitness is calculated, the antibody obtained by matching with the threshold, and the qualified antibody library generated. The niche strategy starts at any time in the antibody library to eliminate antibodies that are too similar. The antibody library is updated dynamically.

Step 4: Vaccine mechanism

Detected antibodies that exceed the vaccine threshold are added to the antibody library as vaccines.

Step 5: Matching detection

Antibodies in the antibody library will start detection as required, calculate the Euclidean distance d_{ij} of the state feature vector between nodes i and j, and mark node i to trigger a danger signal. All nodes are marked whose distance from the node i state eigenvector exceeds the threshold value to trigger a danger signal. Upon successful detection, the abnormal node is reported.

3.2.2. Node Game Model

The node game is to solve the priority problem of node detection and recovery based on global considerations between abnormal nodes.

When an exception occurs on a node, it can be understood in two cases. One is that the node itself is destroyed, and the other is the node is disturbed, spoofed, or attacked. Whatever the case, once the node occurs abnormal, the node energy will be consumed. These abnormal nodes will affect the normal operation of the mobile network and cause the breakdown of the communication between adjacent nodes.

Therefore, the game uses the energy consumption of nodes as the utility index. Because the system uses artificial immune theory for abnormal detection, it is assumed that all nodes in the network structure have deployed corresponding abnormal detection agents. In the game model, there are two participants, the sensor node S (θ_s) and abnormal detection agent R (θ_R). The goal of the game translates to the abnormal detection agent providing the optimal strategy when deciding whether to adopt a defense or recovery strategy.

When the transmission bandwidth is B, the node energy consumption is satisfied:

$$E_{Etr}(B,l) = BE_{Eno} + Bl^{x}E_{Eli}, \tag{10}$$

where E_{Eno} indicates that the node's internal circuit consumes power. E_{Eli} represents the amplified power of the antenna to the current signal. l is the transmission distance correction coefficient. For a node in the region, let l_N be the stable transmission distance. That is, if the actual transmission distance l_d is less than or equal to l_N, the data transmission within this range is considered stable, and the energy consumption of node transmission is the same. If l_d is greater than l_N, $l = l_d/l_N$. In formula (10), x represents the transport model index. When the transport model exponent between nodes is 2, a direct link between the two is no longer established [20].

$$\text{x} = \begin{cases} 0 \; when \; l_d \leq l_N \\ 1 \; when \; l_d > l_N \\ 2 \; when \; l_d \gg l_N \end{cases} \tag{11}$$

According to the above assumptions, ordinary nodes in the region are similar. These ordinary and regional nodes are in a highly correlated state. As a result, the zone node can combine the upload bandwidth of k normal nodes in region *B1*, *B2*, . . . , *Bk* into the zone bandwidth *BBlo* and upload data. The energy consumption generated by the zone node, *EElo*(*BBlo*, *k*), is

$$E_{Elo}(B_{Blo},k) = B_{Blo}E_{Elo}, \tag{12}$$

where E_{Elo} is the power consumption of the circuit inside the regional node.

The number of zones is N and the correction coefficient of transmission radius of regional nodes is d. Let d_N be the stable transmission distance. That is, if the actual transmission radius d_d is less than or equal to d_N, the data transmission within this range is considered stable, and the energy consumption of node transmission is the same. If d_d is greater than d_N, $d = d_d/d_N$. Taking one region and counting the number of normal nodes, we can see that the region contains k ordinary nodes. Owing to the high correlation of nodes within the region, the upload bandwidth of normal nodes is the fixed value B_{Ble}. Regional nodes must aggregate data and transmit it to the sink node, so the overall energy consumption of the region's ordinary nodes is

$$E_{Eall}(B_{Ble}, d, k) = kB_{Ble}E_{Eno} + kB_{Ble}d^{x}E_{Eli}. \tag{13}$$

where x means the same thing as Formula (11).

Considering the short topological distance between the region node and normal nodes, the energy consumption model mainly uses the zone transmission mode.

Since the final network data must be transferred to the sink node, the node must be selected in segments. The regional and sink nodes select the optimal number of partitions and initialize the link data by routing the table. In order to reduce energy consumption caused by various data packets sent by nodes during network initialization, device switching of the regional node is carried out only when the remaining energy of regional nodes is lower than the threshold. We use this as a preparation for node recovery [24].

Game considerations between participants S and R: node S can be normal or abnormal, represented by $\theta_s = 0$ and $\theta_s = 1$, respectively. When $\theta_s = 0$, the action of R is $a_s(\theta_s = 0)$, and when $\theta_s = 1$, it is $a_s(\theta_s = 1)$. $A_s = \{a_s |\ Abnormal, \quad Normal\ \}$ an action set of S. *Abnormal* indicates that the node is abnormal and may affect other nodes. *Normal* means that the node is able to communicate normally. *Detect* shows that the system is detecting abnormalities. *Idle* indicates that the system is idle and can be used for recovery. $A_R = \{a_R |\ Detect, \quad Idle\ \}$ is an action set of R. P is the probability of node failure, and 1-p is the probability that the node is healthy.

Let G represent the benefits of nodes, using node energy consumption E as a cost. When the abnormal node is confirmed, the node yield is G_A and the node energy consumption is E_A. When a node selects a normal action, the node packet can be forwarded smoothly. In this way, the node will benefit G_C from the mobile network with a good communication guarantee, and the node energy consumption will be E_C. The abnormal node selects the normal action, i.e., waiting for recovery and earning G_B. However, in the cooperative process, receiving and forwarding packets consumes the energy of the sensor node, defined as E_B. When the abnormal detection agent selects the object action, it gains G_D because it successfully detects the failed node, and the abnormal detection agent must pay the corresponding cost for the energy consumption, expressed as E_D. The detection and false-positive rates also exist in the abnormal detection agent, and are represented by α and β, respectively. A false positive is a normal node identified as failed in normal communication, which will cause loss to the abnormal detection agent L_F. Matrices (I) and (II) are the node utility matrices, which express the utility benefit of the node. Matrix (I) is the utility benefit of the failed node, and Matrix (II) is the loss of the node.

$$\begin{array}{cc} U_S, U_R & \begin{array}{cc} \quad Detect & \quad Idle \end{array} \\ \begin{array}{c} Abnormal \\ Normal \end{array} & \begin{bmatrix} (1-\alpha)G_A - \alpha G_D - E_A & G_A - E_A \\ G_C - E_C & G_C - E_C \end{bmatrix} \end{array} \quad \text{(Matrix I)}$$

$$\begin{array}{cc} U_S, U_R & \begin{array}{cc} \quad Detect & \quad Idle \end{array} \\ \begin{array}{c} Abnormal \\ Normal \end{array} & \begin{bmatrix} \alpha G_D - (1-\alpha)G_A - E_D & -G_A \\ -\beta \cdot L_F - E_D & 0 \end{bmatrix} \end{array} \quad \text{(Matrix II)}$$

The abnormal behavior is always selected when a node belongs to a failed node. The normal behavior is always selected when it belongs to a normal node. Therefore, for the abnormal detection agent, the expected benefits of choosing detect and idle are, respectively,

$$E_{u_R}(Detect) = p \cdot (\alpha G_D - (1-\alpha) \cdot G_A - E_D) + (1-p) \cdot (-\beta \cdot L_F - E_D) \tag{14}$$

$$E_{u_R}(Idle) = -p\cdot G_A + (1-p)\cdot 0 = -p\cdot G_A. \tag{15}$$

The expected benefits of fault and cooperation for the failure node $\theta_s = 1$ are, respectively,

$$E_{u_S}(Abnormal) = \delta_k\cdot p\cdot(\theta_s = 1|(1-\alpha)\cdot G_A - \alpha G_D - E_A) + (1-\delta_k)\cdot p\cdot(\theta_s = 1|G_A - E_A) \tag{16}$$

$$E_{u_S}(Normal) = \delta_k\cdot p\cdot(\theta_s = 1|(G_C - E_C)) + (1-\delta_k)\cdot(1-p\cdot\ (\theta_s = 1|(G_C - E_C + \lambda G_c\varnothing)), \tag{17}$$

where δ_k is the probability that the normal detection agent R will take action $\varnothing$. The user can reduce the proportion of losses by detecting the abnormal node and recovering it. The weight of the environment is λ. It is used when the number of node failures exceeds the threshold.

3.2.3. Method of Immune Game

The nodes of the mobile network will see a series of actions during their work, which form the monitoring data sent to the abnormal detection agent R. Abnormal detection is carried out by the artificial immune method, which determines whether the monitoring data are normal or abnormal. The abnormal detection agent obtains the corresponding game parameters from the storage data area and initializes the game model, which will receive output data from the abnormal detection and utility matrix set by the manager based on empirical settings. We can determine the probability that the abnormal detection agent will select the actions detect and idle by the value of δ_k. R calculates p and stores it in the storage data area for the next phase.

In the second stage, the game strategies adopted by all nodes involved in the network form a strategy set. When the utility of a node is greater than or equal to the utility of the policy set, the Nash equilibrium condition is satisfied. At this point, the node makes the optimal decision. The game process of nodes is shown in Figure 6.

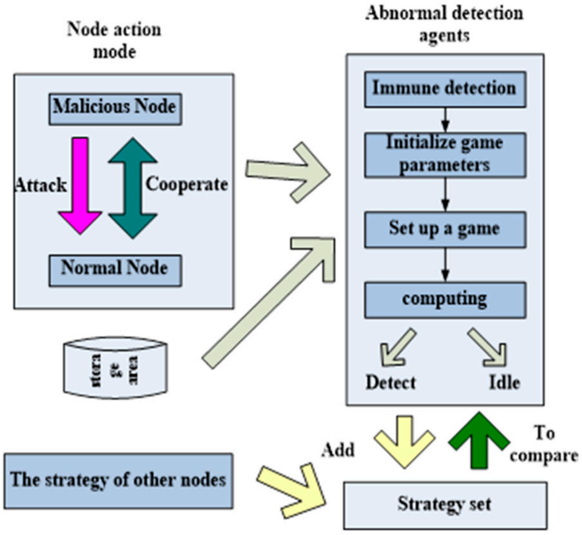


Figure 6. The game process of nodes.

4. Performance Evaluation

4.1. Evaluation Methods

In order to verify and evaluate the feasibility and effectiveness of the immune game detection algorithm proposed in this paper, a simulation experiment was carried out. There are two aspects to the experiment.

(1) Hybrid attack verification. Through comparison experiments on the proposed algorithm, extended dynamics, and LISYS (an artificial immune system model proposed by Homfeyr and Forrest (1999)) based on the AIS model, the detection rate and false detection rate of the proposed algorithm were verified.

(2) The node stability and reliability were verified, and through the comparison experiment of the immune-game model and Extended-DynamiCS, the immune-game model was found to maintain better network stability and reliability.

4.2. Simulation Background

To ensure the reliability of the experiment, the selection of experimental data is based on the principle of authority and diversity. The KDD-CUP99 dataset was selected for both the test set and training set. There are about 4.9 million records in this dataset, and all attack types are divided into 39 attack types in four major categories. Considering that the algorithm in this paper carries out abnormal detection of node behavior, the test data in the experiment contain attack types that only appear in the test set, but these attack types do not appear in the training set. The training set contains one normal identification type and 22 attack types. The dataset also provides a 10% size subset for training and testing. The data library of simulation experiment in this paper comes from these two subsets. Their sample distribution is shown in Table 2.

Table 2. Partial samples in 10% KDDCup99 dataset.

Label	Attack Type	Attack Code	Attack Name	Size of Training Set	Size of Testing Set
0	NOM-AL	0	/	97,278	60,593
1	PRO-BING		/	4107	4166
		1	Ipsweep	1247	306
		2	mscan	-	1053
		3	nmap	231	84
		4	Portsweep	1040	354
		5	saint	-	736
		6	satan	1589	1633
2	DOS		/	391,458	229,853
		7	Apache2	-	794
		8	back	2203	1098
		9	land	21	9
		10	mailbomb	-	5000
		11	neptune	107,201	58,001
		12	pod	264	87
		13	Processtable	-	759
		14	smurf	280,790	164,091
		15	teardrop	979	12
		16	UDPstorm	-	2

4.3. Experimental Environment and Parameter Settings

To evaluate the algorithm's performance, the *NS2* simulation environment was selected, the computer operating system was Win 10, the CPU's main frequency was 5.5 GHz, and there were 16 GB of memory. The mobile network simulation scene was set to a square area of 100 m × 100 m, and 20 mobile nodes were randomly set within the region. The motion of a node was based on the random waypoint motion model [25], with a maximum motion speed of 10 m/s. Each node had a communication radius of 30 m. Experimental simulation parameters are shown in Table 3. The values of the immune game model are shown in Table 4.

Table 3. Parameter set of experiment.

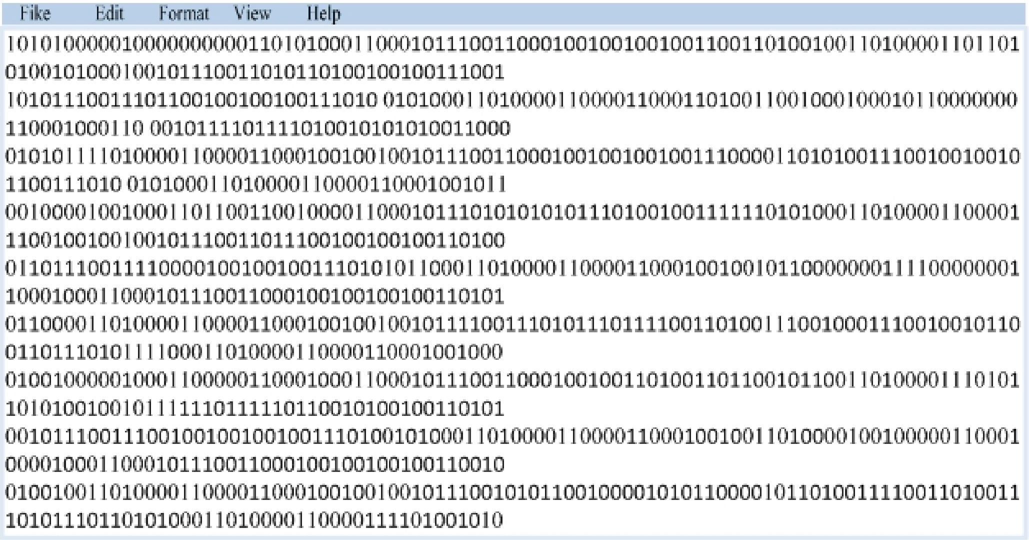
Item	Value	Item	Value
network simulation area	100 m × 100 m	size of data packet	150 bytes
Initial energy of nodes	50 J	transmission rate	500 Kbps
Node distribution	random site	communication mode	TDMA

Table 4. Values of immune game model parameters.

Parameter Type	Parameters	Value
Immune parameter	L (Size of a single detector)	64 bit
	r (Threshold of matches)	16 bit
	m (Number of alphabet symbols)	4
	P (Number of detectors)	200
Game parameter	A (Probability that node will be infected and detected)	0.8
	β (Probability that node is not infected but is detected)	0.08
	Pr (Probability that user will check alarm node)	0.8
	∅ (User detects failed node and recovers, allowing user to reduce percentage of losses)	0.5
	G_A (Benefits that can be gained when user detects an attack).	250
	G_C (Benefits of normal node communication.)	100
	G_D (Average return per test)	200
	E_D (Average cost per test)	10
	D (Node attack was not detected and user lost.)	1000
	L_F (Normal node was mistakenly alarmed and user lost)	15
	λ (Environmental weight; starts when number of node failures exceeds threshold)	0.8
	δ_k (Probability that abnormal detection agent chooses to perform detection action)	0.8

4.4. Experimental Results

The data in Table 2 must be converted to binary form. We take 64 characters as the antibody length, which makes it easy for the program to extract *self* and *nonself*. This standardized data format is shown in Figure 7.



```
1010100000010000000000011010100011000101110011000100100100100110011010010011010000110l101
0100101000100101110011010110100100100111001
10101110011101100100100100111010 01010001101000011000011000110100110010001000101100000000
110001000110 0010111101111010010101010011000
010101111010000110000110001001001001011100110001001001001001110000110101001110010010010
1100111010 0101000110100001100001100010010 11
0010000100100011011001100100001100010111010101010111010010011111101010001101000011000 01
1100100100100101110011011100100100100110100
011011100111100001001001001110101011000110100001100001100010010010110000000111100000001
100010001100010111001100010010010010 0110101
0110000110100001100001100010010010010111100111010111011110011010011100100011100100 10110
011011101011110001101000011000011000100 1000
0100100000100011000001100010001100010111001100010010011010011011001011001101000011 10101
1010100100101111110111111011001010010 0110101
001011100111001001001001001110100101000110100001100001100010010011010000100100000110001
0000100011000101110011000100100100100110010
0100100110100001100001100010010010010111001010110010000101011000010110100111100110100 11
1010111011010100011010000110000111101001010
```

Figure 7. Standardized data format.

The detection rate is

$$\mathrm{TP} = \frac{T\_count}{Attack\_count} \tag{18}$$

where *T_count* is the number of abnormal nodes detected, and *Attack_count* is the number of system attack records entered.

The abnormal-detection rate is

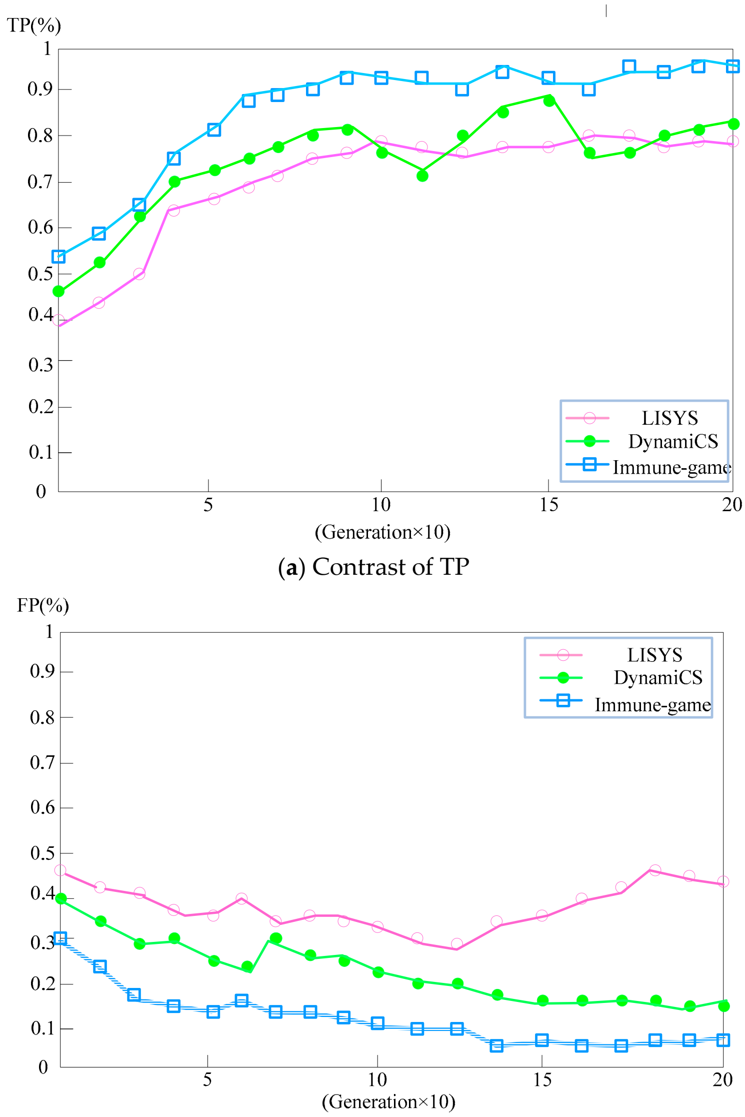
$$\mathrm{FP} = \frac{F\_count}{Normal\_count} \tag{19}$$

where *F_count* is the number of normal nodes which are considered as abnormal, *Normal_count* is the number of nodes that have legitimate behavior.

So, TP indicates true positive and FP means false positive.

The simulation experiment had training and test parts. The training part selects several records that can fully reflect various attack types from 10% of the training subset of the *KDD-CUP99* dataset. They are processed and loaded into the system. The system is trained to produce an initial set of *self*. In the test part, several records were selected from the test subset of the *KDD-CUP99* dataset to fully reflect the various attack types, and attack behavior was reproduced through the network reissue tool, so as to verify the detection and error-detection rates.

The immune-game algorithm, Extended-DynamiCS, and LISYS based on the AIS model were experimentally compared, with detection and abnormal-detection rates as shown in Figure 8. The detection rate and false detection rate of the proposed algorithm are significantly better than those of the other two algorithms. This is due to the adoption of vaccine and niching strategy in the immune detection part of the algorithm in this paper. Vaccines have made testing more efficient. Niching strategy increases the detection coverage, and thus further improves the detection efficiency and reduces the false detection rate.

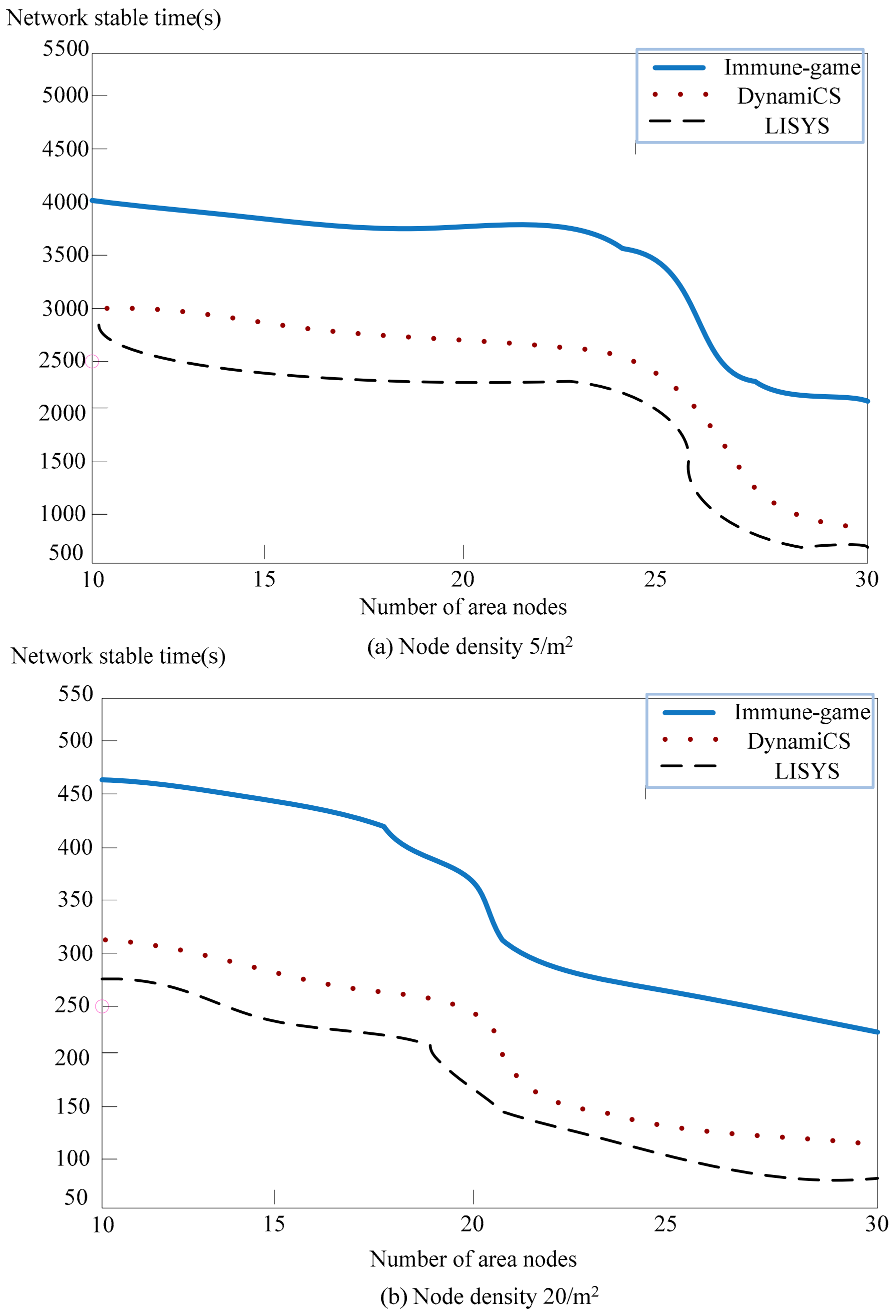


(**a**) Contrast of TP

(**b**) Contrast of FP

Figure 8. Contrast of FP and TP.

Figure 9 shows the stabilization time of the network under different numbers of nodes. The proposed algorithm considers not only the energy consumption of nodes but the influence of links on node security.



(a) Node density 5/m^2

(b) Node density 20/m^2

Figure 9. Distribution of number of nodes.

The other two algorithms take insufficient account of the link factors and do not optimize the initial process of the network region. Therefore, their network operation stability is lower than that of the algorithm presented in this paper.

Figure 9 also shows that the stabilization time decreases with more nodes. This is because the greater the amount of nodes, the more network resources are used. An increase in the coupling between nodes causes the system to sacrifice the stability time while coordinating between nodes.

To test the effect of the algorithm’s game mechanism on detection, the reliability of the network under the long-term operation of different algorithms is shown in Figure 10. The reliability of the algorithm is related to the failure rate of the attacked sensor node, number of sensor nodes in a cluster, number of cluster heads passing on a route, and number of routes available for the entire network. Therefore, the numbers of nodes and routes were unchanged in experiments, ensuring that each algorithm was tested on the same type and number of attacks. The experimental results of reliability were obtained as the time of normal sending and receiving of network data.

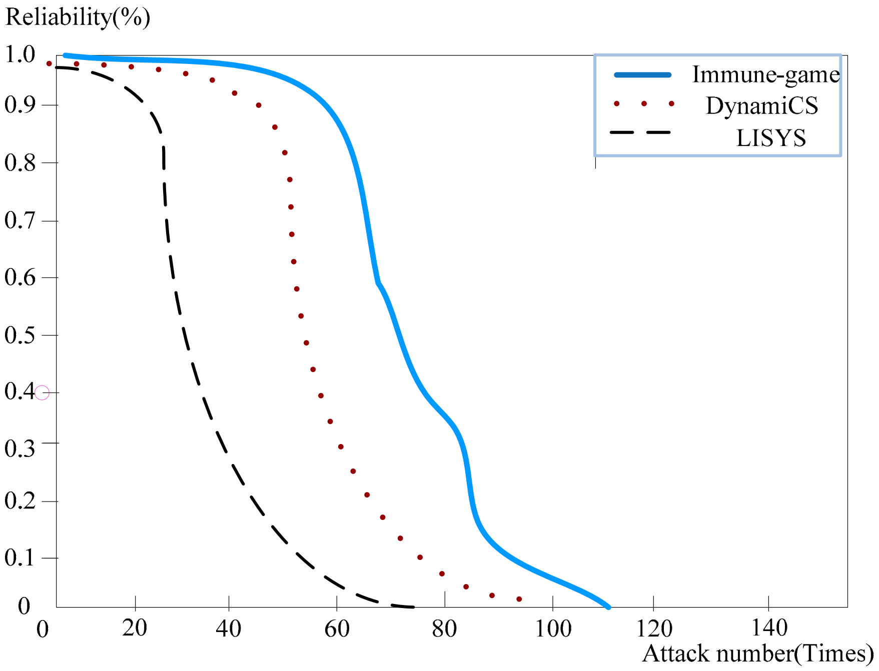


Figure 10. Reliability of algorithms.

In the experiment, the network is defined as an undirected simple network topology diagram. Graph G consists of a set of points V(G) and an edge set E(G), G = (V, E). The reliability of the network is R(G,Φ,ψ), where G = (V, E), Φ and ψ represent the probability of failure of all nodes and edges in the graph, respectively, and the value range is [0, 1]. Thus, the reliability of the network R(G,Φ,ψ) is generally defined as the probability that graph G remains connected under the possible abnormal of points and edges.

Owing to the algorithm comparison experiment, the reliability is quantified by the network reliability running time in this paper. According to the literature [26,27], this paper adopts *MTTF* of the mean fault-free time of nodes to calculate the reliability of the network. For simplicity, it is assumed that the failure rate λ is a constant during the whole period of system operation, and that each cluster of the network contains *m* nodes. That is,

$$\lambda = \frac{1}{MTTF} \tag{20}$$

Then, the reliability of a node is defined as

$$R_i(t) = \exp(-\lambda t) \tag{21}$$

Due to the fact that the probability of abnormal occurrence of each node is independent, a cluster will lose its ability to work normally only when all the candidate cluster heads are abnormal and cause faults. Therefore, the reliability of a cluster can be obtained.

$$R_{ci}(t) = 1 - \prod_{i=1}^{m}(1 - R_i(\mathrm{t})) = 1 - (1 - \exp(-\lambda t))^m \tag{22}$$

Since the failure of any cluster on a route will lead to the failure of the whole route, the reliability of a route can be obtained.

$$R_{Ri}(t) = \prod_{i=1}^{n} R_{ci}(\mathrm{t}) = \left(1 - (1 - \exp(-\lambda t))^{m}\right)^{n} \tag{23}$$

where *n* indicates the number of clusters through which a route passes. Assuming that any route to transmit data passes through the same number of clusters, the reliability of the entire network is

$$R(t) = 1 - \prod_{i=1}^{l} (1 - R_{Ri}(\mathrm{t})) = 1 - \left(\left(1 - (1 - \exp(-\lambda t))^{m}\right)^{n}\right)^{l} \tag{24}$$

where *l* represents the number of all available routes from the source node to the base station in the entire network.

In the experimental scheme, the number of nodes and routes is kept unchanged. It is important to ensure that the network is given the same type and number of attacks during each algorithm test. The experimental results of reliability are obtained by the normal transmission and reception time of network data.

It can be seen from the figure that the network reliability of the application of the immune-game algorithm was significantly higher than that of the other algorithms.

5. Conclusions

We addressed the problem of node data security in a mobile multimedia network, and used an immune method to solve the problem of abnormal detection when nodes are attacked. Game theory was used to optimally allocate mobile user resources.

Artificial immune theory uses random coding to generate the initial detector. Non-specific immunity is obtained by negative selection. The risk theory of artificial immunity provides for crossover, variation, and vaccine immune responses. This theory allows for specific immunity. An immune algorithm is used to detect abnormal nodes and to then establish an abnormal detection system for nodes. Obviously, a better theoretical basis is presented. Simulation results showed that the immune algorithm can effectively solve the problem of abnormal detection in node security.

Regarding diagnosis, the performance of the algorithm depends on the node's recognition of abnormal data. A certain consumption threshold is set in both time and energy in the diagnosis of the node itself and spatially related neighboring nodes. Through the dual mechanism of self-diagnosis and neighbor node diagnosis, as well as the middle node's diagnosis, the transient abnormal action of nodes are excluded. The accuracy of diagnosis can be effectively improved and the workload is somewhat reduced in the stage of immune computing.

The ability to restore a system to a known good state after it has been damaged is more important than making it immune to all attacks. Resilient systems can recover quickly and confidently. As a task-based network, it not only requires data transmission but data fusion and task cooperative control. Node security ensures the confidentiality of task execution, the reliability of data generation, and the security of data transmission. Therefore, detection and recovery of abnormal nodes after diagnosis are important research topics.

Due to the fact that a mobile multimedia transmission network has a large number of nodes, to repair all failed nodes in time is bound to lead to system communication difficulties. Game theory studies the strategy and decision-making problems of two or more participants, and can provide novel ideas for the study of network security. A mobile wireless network is characterized by self-organization, the lack of a control center, and dynamic topology. These characteristics determine that each node makes its own decision when communicating. When making a decision, a node may act selfishly and seek a decision beneficial only to itself, or even act maliciously and choose to degrade network performance. Through the game, an abnormal detection system can determine when to start detection, and the priority of node repair can be determined to ensure reliable system operation.

In this paper, the status of an abnormal node in the network is determined by calculating its revenue and payment. The game method is based on a Nash equilibrium, and the idea of a dynamic evolutionary game is added. This is because the nodes in the network as participants, have limited cognitive levels, and a limited ability to collect and process information and to reason. The decision-making behavior of participants will be affected by the group environment, and they can only make strategic choices through learning and imitation. Because of bounded rationality, participants in the evolutionary game will not immediately obtain the optimal strategy, and must perform self-adaptive adjustments under the influence of the environment, through continuous learning and trial and error, to find the optimal strategy. Hence, the equilibrium is not the result of a choice, and is only reached by dynamic adjustment and adaptation, and even if the equilibrium is reached, deviations may occur under the premise of environmental changes.

The algorithm in this article provides initial values for the parameters δ_k (probability of the abnormal detection agent choosing to perform the detection action) and $\varnothing$ (proportion of loss that the user can reduce when the user detects the failed node and recovers). Then, environmental factors were considered as variables. They adjust as the energy of the nodes changes. In the simulation experiment, weight fine-tuning was added according to the number of node failures. In the experiment, the weight is set by itself and improves the performance of the algorithm to some extent. In future, more methods can be studied to further improve the performance of the algorithm.

The proposed algorithm synthesizes both immune and game mechanisms. Immunization is used for abnormal detection. The essence of the game is to coordinate the work of the system, increase its stability, and reduce time consumption. But the stability of the system increases, as does the complexity of the algorithm. As a result, the response time of the system is not improved. Therefore, the game problem of the algorithm requires further study.

The simulation experiment adopted in this paper obtains the abnormal nodes through network attack. The premise of the experiment is that the node is normal before being attacked. Therefore, the feature extraction of normal behavior is not disturbed by the algorithm. This is an ideal state. In addition, the data collected by the nodes in the mobile network have the characteristics of spatial and temporal correlation. A node's working behavior has great uncertainty. Therefore, the anti-jamming performance of the algorithm requires further consideration.

Author Contributions: Conceptualization, Y.Z. and K.W.; methodology, Y.Z.; software, Y.Z.; validation, Y.Z., K.W. and J.Z.; formal analysis, Y.Z.; investigation, K.W.; resources, K.W.; data curation, Y.Z.; writing—original draft preparation, Y.Z.; writing—review and editing, K.W.; visualization, J.Z.; supervision, K.W.; project administration, Y.Z. and J.Z.; funding acquisition, K.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by [Double First-Class Scientific Research Funds of HIT in China] grant number [IDGA10002093] and [National Natural Science Foundation of China (NSFC)] grant number [61702439].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: We used the KDDCup99, which is a famous and publicly accessed dataset (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, accessed on 1 December 2021), for the evaluation of new algorithms in the proposed abnormal node detection system.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yamada, T.; Lambertsen, G.; Zhang, L. Mobile Multimedia Metropolitan Area Network. In Proceedings of the IEEE Wireless Communications and Networking, New Orleans, LA, USA, 16–20 March 2003; pp. 2047–2052.
2. Racherla, G.; Saha, D. Security and Privacy Issues in Wireless and Mobile Computing. In Proceedings of the IEEE International Conference on Personal Wireless Communications, Conference Proceedings (Cat. No. 00TH8488), Hyderabad, India, 17–20 December 2000; pp. 509–513.
3. Yamada, T. Mobile Multimedia Metropolitan Area Network; an Office LAN Extension to the 4G Mobile Network. In Proceedings of the International Telecommunications Network Strategy and Planning Symposium, Vienna, Austria, 13–16 June 2004; pp. 105–110.
4. Johnston, D.; Walker, J. Overview of IEEE 802.16 security. *IEEE Secur. Priv.* **2004**, *2*, 40–48. [CrossRef]
5. Staddon, J.; Balfanz, D.; Durfee, G. Efficient Tracing of Failed Nodes in Sensor Networks. In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, 28 September 2002; pp. 275–286.
6. Nitesh, K.; Jana, K.P. Distributed fault detection and recovery algorithms in two-tier wireless sensor networks. *Int. J. Commun. Netw. Distrib. Syst.* **2016**, *16*, 281–296. [CrossRef]
7. Titouna, C.; Aliouat, M.; Gueroui, M. FDS: Fault Detection Scheme for Wireless Sensor Networks. *Wirel. Pers. Commun.* **2015**, *86*, 549–562. [CrossRef]
8. Lau, B.C.; Ma, E.W.; Chow, T.W. Probabilistic fault detector for Wireless Sensor Network. *Expert Syst. Appl.* **2014**, *41*, 3703–3711. [CrossRef]
9. Zhang, W.; Han, G.; Feng, Y.; Cheng, L.; Zhang, D.; Tan, X.; Fu, L. A Novel Method for Node Fault Detection Based on Clustering in Industrial Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 230521. [CrossRef]
10. Lim, T.H.; Bate, I.; Timmis, J. A Self-adaptive Fault-tolerant Systems for A Dependable Wireless Sensor Networks. *Autom. Embed. Syst.* **2014**, *18*, 223–250. [CrossRef]
11. Salmon, H.M.; De Farias, C.M.; Loureiro, P.; Pirmez, L.; Rossetto, S.; Rodrigues, P.H.D.A.; Pirmez, R.; Delicato, F.; Carmo, L. Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques. *Int. J. Wirel. Inf. Netw.* **2012**, *20*, 39–66. [CrossRef]
12. Qiao, L.; Bai-Hai, Z.; Ling-Guo, C.; Zhun, F.; Vasilakos, A.V. Immunizations on small worlds of tree-based wireless sensor networks. *Chin. Phys. B* **2012**, *21*, 050205.
13. Jabbari, A.; Lang, W. Advanced Bio-Inspired Plausibility Checking in a Wireless Sensor Network Using Neuro-Immune Systems: Autonomous Fault Diagnosis in an Intelligent Transportation System. In Proceedings of the Fourth International Conference on Sensor Technologies and Applications, Venice, Italy, 18–25 July 2010; pp. 108–114.
14. Zhang, Y.J.; Wei, J.; Wang, K. An Edge IDS Based on Biological Immune Principles for Dynamic Threat Detection. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8811035. [CrossRef]
15. Forrest, S.; Perelson, A.; Allen, L.; Cherukuri, R. Self-Nonself Discrimination in a Computer. In Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, Los Alamitos, CA, USA, 16–18 May 1994; pp. 271–281.
16. Matzinger, P. The Danger Model: A Renewed Sense of Self. *Science* **2002**, *296*, 301–305. [CrossRef] [PubMed]
17. Sun, F.X.; Kong, M.R.; Wang, J.H. An Immune Danger Theory Inspired Model for Network Security Threat Awareness. In Proceedings of the 2010 Second International Conference on Multimedia and Information Technology, Kaifeng, China, 24–25 April 2010; pp. 93–95.
18. Obsborne, M.J.; Rubinstein, A. *A Course in Game Theory*; MIT Press: Cambridge, MA, USA, 1994.
19. Nash, J.F. Non-cooperative games. *Ann. Math.* **1951**, *54*, 286–295. [CrossRef]
20. Kishor, P.; Koen, T.D.; Dieter, F. A two-queue model for optimizing the value of information in energy harvesting sensor networks. *Perform. Eval.* **2018**, *119*, 27–42.
21. Zbigniew, L. Routing algorithm for maximizing lifetime of wireless sensor network for broadcast transmission. *Wirel. Pers. Commun.* **2018**, *101*, 251–268.
22. Amir, A.H. Analysis of incremental LMS adaptive algorithm over wireless sensor networks with delay delinks. *Digit. Signal Process.* **2019**, *88*, 88–89.
23. Xu, F.; Wang, J. Link stabilization algorithm for WSN based on virus-antibody immune game. *Comput. Eng.* **2020**, *46*, 206–212, 235.
24. Sergiu, H.; Andreu, M. Cooperation: Game-Theoretic Approaches. 1997. Available online: https://www.springer.com/gp/book/9783642644139 (accessed on 1 December 2021).
25. Camp, T.; Boleng, J.; Davies, V. A survey of mobility models for ad hoc network research. *Wirel. Commun. Mob. Comput.* **2002**, *2*, 483–502. [CrossRef]
26. Shen, S.G. Game Theory Based Research on Several Key Problems of Wireless Sensor Networks Security. Ph.D. Thesis, Donghua University, Shanghai, China, 2013.
27. Buzacott, J.A. Markov Approach to Finding Failure Times of Repairable Systems. *IEEE Trans. Reliab.* **1970**, *19*, 128–134. [CrossRef]