Network Layer Security Detection Model of Internet of Things Based on Immune System

Bo Yang
School of Information Management, JiangXi University of Finance and Economics Nanchang, China.
Email: yangbo@jxufe.edu.cn

Abstract. The traditional network security detection model use attack samples of known types to train the security detection model offline. Although it has a high detection rate for the known attack types, it cannot identify the new attack types on the network layer. At present, detection system has disadvantages of slow speed of system construction and high cost of model update. Facing increasingly expanding network and endless attacks, the detection system lacks self-adaptability and expansibility. In this paper, the integrated use of immunology theory and complex adaptive system theory and computational experiment technology, based on Internet network layer security detection model of the immune system, existing Internet network layer security, the new type of attack occurred in the process of on-line detection of immune learning, realize the dynamic extension of network security detection model, and through calculating experiment and example analysis verify the scientific nature and feasibility of the model.

1. Introduction
Most of the traditional detection systems build detection models based on the known pattern matching method. Through learning and training of the known samples, the detection models are applied to the network layer security detection of the Internet of things to detect the known network attacks. This kind of detection model has the problems of slow system construction speed and high cost of model update, so it is difficult to detect the complex and changeable attack types on the network layer of the Internet of things. Faced with the ever-expanding network and endless attacks, the current detection methods lack of self-adaptability and expansibility, so it is necessary to study more automatic and intelligent methods to build a detection model with strong adaptability and dynamic expansibility.

Human immune system is an effective and adaptive defense system which has been proved by biological evolution. It is also a large-scale parallel adaptive information processing system. In terms of biological mechanism, the natural immune system and the network layer security detection of the Internet of things are very similar. The natural immune system's defense against virus invasion in human body is a process of constantly detecting and dealing with network layer attacks. However, studies on Internet of things security detection system with immune system as reference system are rare. This paper refers to the immune system information recognition mechanism, the network layer security attack event of the Internet of things is simulated as antigen, according to the principle of immune response, building the network layer security detection model of the Internet of things, providing a new method to explore the immune response and network security attack detection of network security attack, enriching the research system of Internet of things network security management.
2. Formatting the Title, Authors and Affiliations

The immune system is a robust defense system, and the overall performance of the immune system is the product of "emergent" interactions between many individuals performing small and specific tasks. The immune system is actually a large, complex and highly coordinated system.

Ö. Can put forward a Markov model based on implicit, anomaly detection technology to monitor network data inconsistency, this method is based on historical events, using hidden Markov model from the deployment area of self-organization critical point to obtain prior knowledge, to identify the abnormal network behavior[1]. A. AGAH regards the problem of network attack and defense as a non-zero-sum game between the sensor network and the attacker, so as to provide defense strategies for the construction of sensor network[2]. Some literatures also proposed a distributed BOUNDHOLE routing detection model, which built the routing around the routing hole, Routing holes are areas of network connection, bounded by all stuck nodes, and these hole-surrounded routes provide surrounding with large amounts of data for routing, information storage, and network security detection[3]. There are also literatures that analyze the security requirements of Internet of things, propose the security architecture based on network layer, and elaborate its key technologies[4][8].

Then, scholars at home and abroad apply the principle of artificial immune system to intrusion and detection of sensor network [6][9]. Although such models can provide global network communication data, they prevent network nodes from sleeping and force them into idle state, thus greatly reducing the efficiency of network security detection. Literature 5 proposes intrusion detection technology based on network topology and sensor configuration information, which can determine abnormal intrusion behaviors at specific network locations[5][7]. In the literature, an autologous and allogeneic detection model based on biological immune system was proposed. Although it predicted the network attack situation of the Internet of things, the self-collection was too large and the immune tolerance took too long.

In this paper, the detection capability of traditional detectors cannot be dynamically improved, and there is a lack of self-adaptability. The network layer security detection model of the Internet of things is constructed by referring to the dynamic, active and adaptive defense thoughts of biological immune system against pathogen.

2.1. Network Layer Security of Internet of Things

Considering the various and complex protocols of network layer, network layer is the target of intrusion in both traditional network and wireless sensor network. Intruders can perform a variety of attacks on the network layer, for example, Sink black hole attack, witchSybil attack, black hole attack, hello flood attack, spoiling tamper routing attack, selective forwarding attack and so on. The following is a detailed discussion and analysis of various types of attacks.

In a Hello flooding attack, most routing protocols require sensor nodes to periodically send Hello packets to neighboring nodes to declare themselves as neighbors of these nodes. However, if a powerful malicious node USES enough power to broadcast the Hello packet, the node receiving the packet will mistakenly believe that the malicious node is its neighbor node. In subsequent routes, these nodes may use this path to send packets to malicious nodes.

In a wormhole attack, it is usually necessary to collude two malicious nodes to launch a joint attack. Generally, one malicious node is near the sink node, while the other malicious node is far away from the sink node. The distant node claims that it can establish a communication link with the node near the sink node with low delay and high bandwidth, so as to attract its neighboring nodes to send packets to this point. In this case, the malicious node far from sink is actually a sinkhole. This type of attack is often used in conjunction with other attacks.

2.2. Principles of Immune System Theory

The biological immune system is the process by which organisms defend themselves against harmful external substances. External harmful substances invade the body and activate immune cells, inducing the process of immune response in the body called immune response. Substances that induce the immune system to produce an immune response are called antigens, and immune cells that specifically bind to antigens are called antibodies. When the antigen enters the body, the body is protected by the
immune system, and the immune recognition mechanism of the immune system can recognize the antigen. Antigens pose a danger to the immune system, which generates an immune response, just as an external attack on the network layer poses a threat to the Internet of things. This paper assumes that antigen Agent represents the external attack on the network layer of the Internet of things, which is the target of network security detection Agent and pre-control scheme Agent. Network security detector Agent and pre-control scheme Agent will generate the attack types of the network layer of the Internet of things respectively, and continue to eliminate the ones with low affinity and supplement the ones with higher affinity through the cloning and selection function, until they get the best evolved security detector and pre-control scheme of the network layer of the Internet of things.

To study the behavior of a complex immune system, the state of the system is usually described in terms of the concentration or number of immune cells or molecules. Complex system subject adaptability predates complexity. Concentration mainly involved in the immune response is antigen attacks (network layer) and antibody (network layer security detectors), the number of the antigen and antibody affinity is a major operation control concentration factor, is the basis for the system with adaptive feature, this article USES the affinity, the number of antigens, the number of network security detector as Internet network layer security detection index. However, the network layer security detection model of the Internet of things lacks an indicator to directly describe the system state. The result is a scientific system that includes affinity, number of antigens, number of network security detectors, and detection power.

Affinity: Affinity is obtained based on the structural similarity between antibodies and antigens and through the algorithm of distance and matching mode. The higher the affinity is, the better the detection effect of antibodies will be.

Antigen-scavenging effect: Network security detector antibody, in the case of affinity to meet a certain threshold, will eliminate the antigen. The faster the antigen is eliminated, the less the range and frequency of fluctuation, indicating the better the elimination effect of the system and the effective control of network attack events.

Detector number: The network security detector is an effective antibody for detecting antigens, whose number represents the number of antibodies possessed by the system at a certain degree of affinity. In general, the higher the number of antibodies, the more serious the attack event, the greater the risk of antigen, the need to use more resources.

Energy: The internal cause of cyber attacks is the accumulation of internal energy, and the evolution process is the transfer, accumulation and sudden large-scale release of energy. By calculating evolution, the energy fluctuation of network attack time system in a certain period is simulated, and the energy value of the system and its evolution curve are taken as the main basis to judge the attack event.

3. Network Layer Security Detection Model Based on Immune Theory

3.1. Model Building

3.1.1 Affinity. Assuming that the antigen(a) and antibody(b) are isomorphic, this paper USES binary string to represent the gene, it includes self, detector (antibody) and Internet of things network layer attack (antigen), all of which are binary string combinations with length of n. The affinity of antigen and antibody is related to the distance between them, which can be calculated by Hemingway distance. Affinity is calculated as a formula 1.

$$ D_t = \sum_{i=1}^{n} \theta_i, \begin{cases} \theta_i = 1, & a_i \neq b_i \\ \theta_i = 0, & a_i = b_i \end{cases} $$

Among them, $D_t$ is the affinity of the t period. Firstly, the initial affinity is set as Aff0, and then the optimal affinity of the above period is taken as the cardinal number. When the current period is larger than the previous period, the current value is the optimal affinity, otherwise the previous period value is retained.$a_i$ and $b_i$ is the value of the i position of the antibody gene and the antigen gene.$\theta_i$ is the distance between $a_i$ and $b_i$. 

3.1.2 Number of Antigen. Among them, Num(a)_t is the numbers of antigen of the t period; M(a)_t−1 is number of antigens cleared by t−1 period. If the antigen antibody affinity is greater than the threshold Aff, the antigen is cleared; C(a)_t is New antigens produced every period, Assume constant C_t.

\[
\text{Num}(a)_t = \text{Num}(a)_{t-1} - M(a)_{t-1} + C(a)_t
\]  
(2)

3.1.3 Detector Number. After the self-tolerance test of the immune system, the network layer security detector of the Internet of things binds to the antigen and clears the antigen. Then, the detector is divided and mutated to evolve, and the detector with high affinity is selected for cloning and inheritance to the next period. The next period generates a fixed number of random network layer security detectors.

\[
\text{Num}(b)_t = \text{Num}(b)_{t-1} - M(b)_{t-1} + C(b)_t
\]  
(3)

Among them, Num(b)_t is the number of detectors in period t; M(b)_{t−1} is the number of detectors which affinity is less than the threshold Aff, and the affinity threshold Aff can vary according to the optimal affinity of the current period; C(b)_t is newly generated detectors per period, formula is as follows:

\[
C(b)_t = \mu \cdot (\text{Num}(b)_t - M(b)_{t-1}) + C_0
\]  
(4)

Among them, Num(b)_t is the number of detectors in period t; \( \mu \) is the coefficient of cloning; \( C_0 \) is the number of newly generated detectors per period. The network layer security detection model of the Internet of things simulates the antibody diversity of the immune system. These newly generated detectors come from the detectors whose affinity is higher than the threshold after the elimination of antibody mutations.

3.1.4 Energy. In this paper, based on the detection model of the immune system, the information entropy theory is fused to convert the antibody concentration into the information entropy of gene sequence. The network layer security detection energy model based on the immune information entropy is shown as follows.

\[
E_t = \frac{2}{1 + e^{-\sum_{i=1}^{N_g} (C_T i - C_T i - 1)}} - 1
\]  
(5)

Among them, \( E_t \) is the energy of the antibody with the optimal affinity in the t period; \( N_g \) represents the number of genetic classifications; \( C_T i \) represents the information entropy of the i bit string in \( N_g \); and represents the chaos degree of the gene of network attack event, as shown in the formula.

\[
C_T i = -\frac{1}{\ln c} \sum_{k=1}^{m} S_j \ln S_j (i = 1, ..., N_g; k = 1, 2, ..., n)
\]  
(6)

\[
C_T t = \sum_{i=1}^{N_g} \frac{C_T i}{t}
\]  
(7)

Among them, \( S_j \) is the ratio of the value number of the i gene to the total number of genes at the same position in the whole event, and represents the probability of occurrence of such genes. The formula is as follows.

\[
S_j = \frac{\sum_{k=1}^{m} g_{0,i} \land g_{k,j}}{n} (i = 1, ..., n; k = 1, ..., m)
\]  
(8)

Among them, ‘ represent non-operation; \( \land \) Stands for an exclusive or operation; \( g_{k,j} \) represents the value of the i gene in the kth antigen; \( g_{0,i} \) represents the gene value of antigen iposition. When \( S_j = 0 \), Show that Blind spots appear.

In order to describe the energy change trend of the system, the average energy is adopted as the measuring factor in this paper. The average energy of the current cycle is shown in the formula.

\[
E_T = \sum_{t=1}^{T} \frac{E_t}{T}
\]  
(9)
In this paper, the Internet network layer security detection model input data expressed as a binary string, according to different detection areas in practical application, set different threshold, which every string by refinement of the grain size smaller unit, makes the index data input connected to the network layer of reactants of a more comprehensive safety inspection of the actual situation, and by using the method of parallel computing can provide complete solution for complex social issues research, illustrate the extensibility and completeness of the model.

3.2. Simulation Experiment

3.2.1 Simulation Process. Multi-agent-based complex system modeling is an effective method to solve complex social systems, which is very suitable for dynamic simulation of network layer attack events in the Internet of things. In this paper, guided by the "artificial societies, computational experiments, and parallel execution", the immune system as in terms of fuzzy statistics network layer of Internet of Things attacks immune response, get evolution law of system testing index, thus into comprehensive testing standards. The simulation process is as follows.

Procedure Network layer security detection simulation of Internet of things
Begin
    t = 0
    Initialization: random generation of a certain number of antigens, through the cross transformation of mutation into a characteristic antigen;
    While t <Simulated total period do
        Small amounts of random antigens are produced and mutated
        Produce a fixed number of antibodies
        Antigen antibody binding, affinity calculation
        if(Optimal affinity in this period < The optimal affinity of the previous period) then The antibody disappears
            else The clone selects the antibody and inherits it, eliminating the antigen
                The number of residual antigens, the number of preserved antibodies, and the optimal affinity were obtained,
                Calculate the energy $E$ and $E_T$
        $t = t + 1$;
    end
3.2.2 Computational Experiments. According to the immune system gene principle, the length of gene detection fragment was set as $3(N_s$ is 3); The binary string length is set to $9(n$ is 9). Due to the binary expression mode, the input can be fuzzy index data, and the network layer security monitoring of the Internet of things is mainly realized through complex immune response and dynamic evolution, which reduces the requirement for data accuracy and improves the availability of data. The model parameters proposed in this paper can be dynamically set according to real needs. In this article, the parallel computing simulation language is Java, the tool is JCreator, and the Swarm toolkit is installed.

Unknown attack events in the network layer of the Internet of things have a high probability of change, and such events are generally of small probability, which may have unpredictable changes. Therefore, it can be assumed that the probability of encoding 1 of antigen gene is 0.8 and the probability of mutation is 0.5, indicating that most of the indicators of attack events have reached the threshold and need urgent treatment. The calculated experimental results are shown in the figure 1.
The simulation results show that the affinity fluctuates at a high level, indicating that the stability of the model is good. The initial antigen clearance speed is slow, but it can be basically cleared in the later stage, indicating that the network layer of the Internet of things is attacked by unknown, and the detector needs to clone and select antibodies with high affinity to clear the unknown antigen continuously. With the increase of antigen, the number of detectors also increases, and the energy of attack event is at a high level, indicating that this attack event requires more resources to deal with. The above conclusions are consistent with the experimental results in this paper, and further verify the scientific nature and feasibility of the proposed model.

4. Conclusion
In this paper, the integrated use of immunology theory and experimental technology, draw lessons from the immune system to intrusion detection system, the Internet network layer attacks and attacks detector likened to antigen and antibody, respectively, according to the principle of immune response, construction of Internet network layer security detection model. This study provides new ideas and methods for the study of "situational response" network layer attack event management of the Internet of things.

It is a new attempt to study the network layer security detection of Internet of things by using immunology theory and computational experimental technology. The refinement of immune gene indexes for Internet of things security events, selection and optimization of computational experimental parameters, and improvement of network attack event detection standard system and model need to be further studied.

5. Acknowledgment
This work was financially supported by Jiangxi Provincial Department of Education Science and Technology Research Key Project (GJJ180249); National Natural Science Foundation project (71640022, 71361011); Jiangxi university humanities and social science research project (GL18103).

6. References
[1] Ö. Can, "On-shelf product detection: Post-processing with a hidden Markov model", IEEE, vol. 7, no. 3, pp. 1304–1313, Oct. 2017.
[2] A. AGAH, K. BASU, "Intrusion detection in sensor networks: a non-cooperative game approach" IEEE International Symposium on Network Computing and Application, vol. 12, no. 7, pp: 1120-1129, 2004.

[3] Greensmith J, Aickelin U, Tedesco G. Information fusion for anomaly detection with the dendritic cell algorithm[J]. Information Fusion, 2012, 11(1):21-34.

[4] X. Feng, L. Qi, and J. Pan, “A novel fault location method and algorithm for DC distribution protection,” IEEE Trans. Ind. Appl., vol. 53, no. 3, pp. 1834–1840, May Jun. 2017.

[5] C. Haiming, C. Li, "Design and Model Checking of Service Oriented Software Architecture for Internet of Thing: A Survey" Chinese Journal of Computers, vol. 39, no. 5, pp. 853–871, May 2016.

[6] M. Hong, H. Gang, "A method of software architecture modeling in the whole lifecycle", Science in Chinese: Information Science, vol. 44, no. 5, pp. 564-587, 2014.

[7] L. Zhen, W. Ban, "Environmental emergency decision support system based on Artificial Neural Network", Safety Science, vol. 20, no. 1, pp. 150-163, 2012.

[8] Y. Yahui, H. Haizhen, "Research on intrusion detection based on incremental GHSOM", Chinese Journal of Computers, vol. 37, no. 5, pp. 1216-1223, May 2014.

[9] H. Honggui, W. Lidan, "Hierarchical extreme learning machine for feedforward neural network", Neurocomputing, vol. 128, no. 27, pp. 128-135, 2014.

[10] K. Satpathi, Y. M. Yeap, A. Ukil, and N. Geddada, “Short-time Fourier transform based transient analysis of VSC interfaced point-to-point DC system,” IEEE Trans. Ind. Electron., vol. 65, no. 5, pp. 4080–4091, May 2018.