2013 Ninth International Conference on Computational Intelligence and Security

A Novel Approach to IoT Security Based on Immunology

Caiming Liu[1, 2], Yan Zhang[2, *], Huaqiang Zhang[2]
1. School of Information Science & Technology, Southwest Jiaotong University, Chengdu 610031, China
2. School of Computer Science, Leshan Normal University, Leshan 614000, China
*: corresponding author, zhangyan_201016@163.com

***Abstract*—The security situation of the Internet of Things (IoT) is serious. IoT encounters security problems more than traditional computer networks does. The attributes of dispersity and mass of IoT require that approaches to IoT security should be dynamic. Inspired by immunology, a novel approach to IoT security is proposed in this paper. Traditional network security models are used for reference and special requests of IoT security are taken into account. A dynamic defense frame for IoT security is formed in the proposed approach. The links in the frame are correlated with relative data of IoT security. Performance in biological immunology is applied into some links to make the proposed approach be adaptive to IoT environment. The immunity-based antigen, self and detector in the real IoT environment are simulated. They are adopted to imitate the mechanisms which are used to recognize pathogens in biological immune systems. Simulation experiment results show that the proposed approach may provide a novel effective method to ensure IoT security.**

Keywords- IoT Security; Immunology; Detection; Detector; Security Defense

I. INTRODUCTION

The application of the Internet of Things (IoT) [1] increased sharply in recent years [2-5]. However, IoT has its special security requests other than the traditional problems harming computer, Internet and mobile communication network. The terminals in the sense layer have wide varieties and are massive and widely distributed. It makes that the security problems are amplified and affect IoT more severely [6]. Meanwhile, it causes that IoT is faced with more serious potential security threats than in the other networks. Traditional security architectures can not fully satisfy the security requests. A specifical approach to IoT security is in urgent need to cope with the complicated and changeful security situation of IoT.

In the interest of resolving the problems of information security, researchers introduced Artificial Immune System (AIS) [7-10] into the research field of information security. AIS imitates the excellent mechanisms of Biological Immune System. It has attracted much attention widely and been a research hotspot in the fields of bionics and computation intelligence. Since 2002, International Conference on Artificial Immune Systems (ICARIS) has been held 12 times [11]. Researchers applied AIS into research fields of information security and network security and got many outstanding achievements [12-16].

In the following of this paper, the research background of IoT security is surveyed in the second section. The state of security architecture research for traditional networks and IoT is discussed. In the third section, this paper will propose a novel approach to cope with the complicated and changeful IoT environment based on immunology. The proposed approach is expected to provide scientific reasons for the active defense strategy and effective defense measures.

II. RESEARCH BACKGROUND

The current technologies for IoT security primarily come from the concepts of tradition network security. Most of them focus on identity authentication, access control, privacy protection, encryption, security protocol, and etc [17-21]. The security ways are in the stage of passive defense. To construct effective defense measures for IoT security, researchers proposed some methods and models of active defense. Mirowski et al [22] developed a system of intrusion detection according to the past access frequency of thing labels. Yang et al [23] presented a distributed intrusion detection method for nodes of wireless sense networks. Wu et al [24] proposed a security transport model for IoT confidentiality. The above-mentioned system, method and model solved one aspect of the IoT security problems. However, they don't form an effective IoT security architecture and can not provide an appropriate approach to resolve problems of IoT security.

Standard and commercial organizations put forward a series of architectures and models for traditional network and information security. These security architectures include ISO/OSI security system, TCP/IP security system, time-based PDR (Protection, Detection, Response) model, P2DR (Policy, Protection, Response, Recovery) model, P2DR2 (Policy, Protection, Detection, Response, Recovery) model, etc. They realize the guarantee strategy of network security through the aspects of management and technology. However, the traditional security architectures neglect entire construction of networks and information security system. They emphasize simple protection measures and do not make full use of the other links of network security system [25]. They can not be copied blindly to construct the IoT security system because of the special attributes of IoT. It is necessary to study a novel dynamical theoretical approach for IoT security to specially adapt the IoT network environment.

978-1-4799-2548-3/13 $31.00 © 2013 IEEE
DOI 10.1109/CIS.2013.168

Dynamical approach to IoT security can use the traditional network security models for reference. But it has to take the special requests of IoT security into account. It must adopt effective ways to deal with the attributes of dispersity and mass in IoT. In consideration of the excellent AIS attributes such as self-learning, self-adaptation, robustness, distribution, etc [10], it is valuable to use bionics principles of AIS to construct a novel dynamical approach to IoT security.

III. APPROACH TO IOT SECURITY

The proposed approach adopts immune principles and mechanisms to simulate real defense environment of IoT security as an immune system. It transforms its strategies of security defense along with the change of the security environment of IoT. It makes the proposed approach be adaptive to real IoT. The proposed approach is described in the following.

A. Frame of IoT Security

To resolve the problems of static defense strategies, the proposed approach adopts dynamic and circular defense processes against security threats. Its frame is shown in Fig. 1. It consists of five links. The first link *Security Threat Detection* collects and analyzes original IoT network packets. The other links perform based on the analysis results provided by the previous link. All links serve IoT security.

Figure 1. Frame of proposed approach.

B. Simmulation of Immune Principles and Mechanisms

The proposed approach captures original data from IoT traffic and analyzes the data to judge whether it contains security threats. It simulates the principles and mechanisms of AIS to detect security threats in the original data. The principles and mechanisms have the attributes of self-learning, self-adaptation, etc. They make that the proposed approach can adapt the dynamic IoT security environments and discover mutated security threats. The proposed approach simulates the following principles and mechanisms.

1) Antigen simulation

In immune systems, antigen is the original data to be recognized. In the proposed approach, the original data of IoT traffic is simulated into antigen.

The original data comes from real-time IoT traffic. The proposed approach captures IoT packets and gets their head data which is the signature. Let the data set of antigen be A which is shown in (1). The elements in A constitute antigen set to be recognized by the proposed approach.

$$A = \{a \,||a| = l, a = toString(Original\ Data\ Set)\} \tag{1}$$

Where, l is the length of an antigen, $l \in N$, N is the nature number set, *toString*( ) is a function to convert the original data set of IoT into binary strings.

A contains normal antigens and abnormal antigens which threaten IoT system. Normal ones belong to self set which is defined as S. Abnormal ones belongs to non-self set which is defined as N. The antigens in N are abnormal and hide in all antigens. The proposed approach uses immune principles and mechanisms to recognize the abnormal ones (non-self antigens). Eventually, it maintains the IoT to be safe.

2) Detector simulation

To imitate the recognition mechanism in immune systems, detection elements of security threats are simulated into detectors. Let the data set of detector be D which is shown in (2).

$$D = \{\langle ant, ag, cnt, tp, t, fam \rangle\} \tag{2}$$

where, *ant* is the antibody string, *ag* is the living time, *cnt* is the amount of recognized antigens, *tp* is the class, *t* is the thickness.

3) Match mechanism

To simulate the match mechanism, a match method is needed to judge whether a antigen or detector matches another. Presently, feasible matching methods include Hamming, Euclidean, *r*-Contiguous, etc. The proposed approach adopts an improved match method of *r*-Contiguous. It is shown in (3)

$$f_{r-improved}(d,a) = \begin{cases} true, & \sum f_r(d,a) \geq \gamma \\ false, & Otherwise \end{cases} \tag{3}$$

Where, $d \in D$, $a \in A$, γ is a threshold, it meets $1 \leq \gamma \leq \lfloor l / r \rfloor$, r is the amount of binary chars of contiguous match, $f_r()$ is a single group match function of *r*-Contiguous. If d matches a, $f_r()$ returns 1. Otherwise, it returns 0.

4) Evolution mechanism of detector

To simulate the evolution process of immune cells, detectors are classified into immature detector D_I, mature detector D_M and memory detector D_R. The domain *tp* indicates which class the detector belongs to. It is one of the class data set T which meets $T = \{i, m, r\}$. Detectors adopt artificial immune mechanisms to evolve dynamically to adapt IoT security environment. Immature detectors are generated with the mutation and recombination of gene sections or randomly. They pass the detection of self-tolerance to evolve into mature detectors. They can improve the diversity of detectors. Mature detectors come from immature detectors. They get the training of antigens. If they do not match any harmful antigens in a period of time, they get the opportunity to evolve into memory detectors. This embodies the process of self-learning and self-adaptation. Memory detectors come from mature detectors and

signature data of known IoT security threats. They contain the precise signature information to recognize security threats.

5) Self tolerance mechanism

In immune systems, the mechanism of self tolerance is used to avoid that immune cells recognize self antigens. In the proposed approach, new detectors may recognize self elements. They can not be used to detect security threats directly. They must accept the training process of the self-tolerance.

Let the function of the self-tolerance be $f_{tolerance}()$ which is shown in (4).

$$f_{tolerance}(D_I(t-1)) = \{r \mid r \in D_I(t-1), r.ag \geq \alpha, \forall s \in S(t-1) \wedge f_{r-improved}(r,s) = false\} \quad (4)$$

Where, t is the current moment, α is the period threshold of self-tolerance, D_I is immature detector set, S is self set.

$f_{tolerance}()$ returns the detector set which passed self-tolerance. The detectors in it do not match self antigens in a period of time. They evolve to mature ones after they succeed to pass the self-tolerance. In the process of the self-tolerance, new immature detectors are trained by all self elements. If an immature one is matched by a self cell in a special period time, it fails to accept self-tolerance.

6) Evolution mechanism of self

Changeful IoT security environment cause that self set changes along with the dynamic security threats. The initial self elements are gathered in a safe IoT environment. When the proposed approach recognize new abnormal antigens, potential normal antigens are generated. Therefore, self set should be expanded. The expansion process is shown in (5). It make that self set evolutes.

$$S = S_{init} \cup toSelf(A_{Normal}) \quad (5)$$

Where, S_{init} is the data set of initial self elements, $toSelf()$ is the function to convert normal antigens into self elements, A_{Normal} is the normal antigen set recognized by detectors.

C. Dynamic Links of IoT Security

1) Detection of security threats

Detectors and the simulative immune mechanisms are used to recognize abnormal antigens from real-time antigens in the proposed approach. The detection process is shown in (6).

$$A_{Harm} = \{a \mid \forall a \in A, \exists d \in D_I \wedge f_{r-improved}(d,a) = true\} \quad (6)$$

Where, A_{Harm} is a data set recognized by memory detectors.

A memory detector is activated when it detect a harmful antigen. It begins to copy itself and accumulate its thickness.

2) Danger computation

In this link, the quantitative danger caused by security threats is computed. It needs the elements of harmfulness of security threats, asset cost and memory detectors' thickness which is generated in the previous link. The danger computation process is shown in (7).

$$f_{danger}(r) = f(r.t,\ r.h,\ c) \quad (7)$$

Where, r is a memory detector, $r.h$ is the harmfulness of a security threat, c is the cost of IoT asset.

3) Security Response and Defense

The process of response and defense for IoT security is shown in Fig. 2.

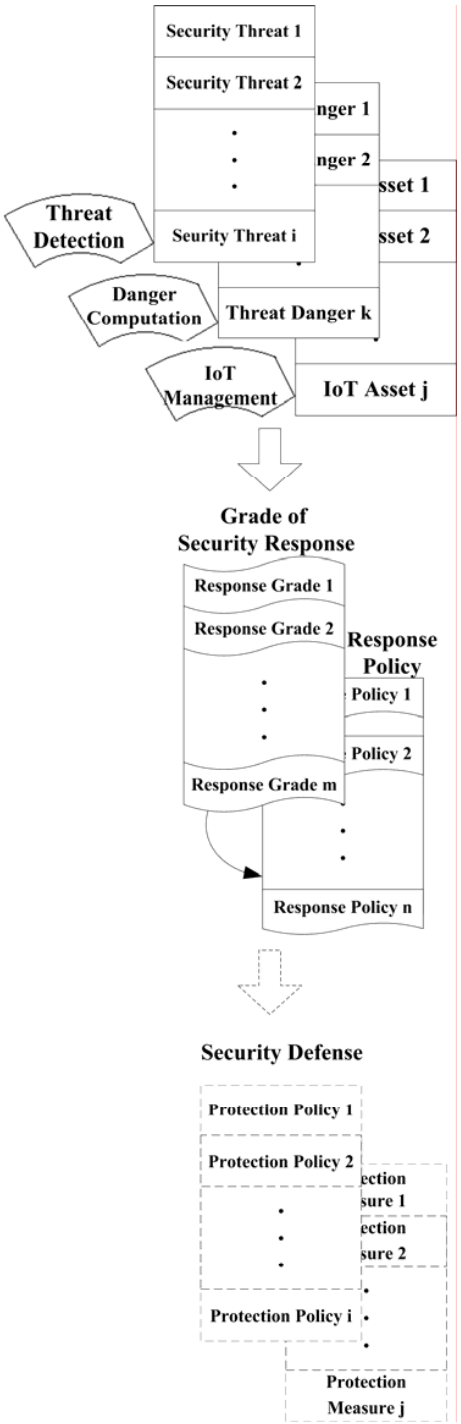

Figure 2. Process of Security Defense.

Fig. 2 illuminates the association relationship of IoT security threats, IoT asset, danger of threats, IoT security response grade and response policy. The broken lines indicate how the proposed approach provides scientific reasons for policies and measures of IoT security defense. The proposed approach produces security response grades and chooses security response polices. Furthermore, it serves security defense.

IV. Simulation Experiments

In the experiments, simulation software and devices were used to construct the simulation experiment environment which is shown in Fig. 3. The simulated network consisted of sense network, IoT gateway and a computer server which runs the proposed approach. In the sense network, cloning attacks, mutated cloning attacks, replay attacks and mutated replay attacks were simulated. The simulated server used AIS principles and mechanisms to detect security threats, compute danger, save security defense strategy library, respond to security threats and defend the security.

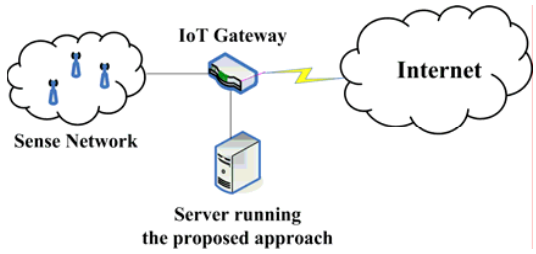

Figure 3. Simulation Experiment Environment.

The sense network kept safe for three hours to collect initial self data set. The simulated server detected simulated attacks and adopted defense measures. Simulation experiment results are shown in Table I.

TABLE I. Simulation Experiment Results

ID Number	Defense Measures	Implementation Times
1	*Logging*	500
2	*Alarm*	309
3	*Forensic*	231
4	*Modification*	132
5	*Part Deletion*	95
6	*Abandonment*	53

Table I shows that the proposed approach can detect security threats and change detectors to adapt the dynamic IoT environment. Meanwhile, it indicates that appropriate defense strategies and measures can be adopted to deal with the relative security threats.

V. CONCLUSION

IoT has some special security requests. Traditional security models for computer networks can not be applied in IoT security directly. The proposed approach uses traditional security models for reference and adopts circular links to construct a dynamic defense system for IoT security. The first link performs based on recognition of security threats. The other links use the real data provided by its previous link. The whole process for IoT security is dynamic. Furthermore, principles in immunology are simulated and applied into the key links. It makes that the proposed model can be adaptive to the IoT environment. The proposed approach changes the defense ways for IoT security and provides a novel effective method to ensure IoT security.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 61103249), the Open Fund of Artificial Intelligence Key Laboratory of Sichuan Province (No. 2011RYJ01), the Scientific Research Fund of Sichuan Provincial Education Department (No. 13ZA0107, 13ZB0106 and 13TD0014) and the Construction Project of Science Research Innovation Team of Leshan Normal University.

References

[1] International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things, Geneva: ITU, 2005.

[2] H. Kopetz. Real-Time Systems. Springer, 2011, pp. 307-323.

[3] A. Luigi, I. Antonio, M. Giacomo. The Internet of Things: A survey. Computer Networks, 2010, 54(15): 2787-2805.

[4] L. Yan, Y. Zhang, L. T. Yang. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

[5] S. B. Shen, Q. L. Fan, P. Zong, Q. Y. Mao and W. Huang. Study on the Architecture and Associated Technologies for Internet of Things. Journal of Nanjing University of Posts and Telecommunications (Natural Science) , 2009, 29(6): 1-11.

[6] IDC. http://www.idc.com.cn/about/press.jsp?id=NTY5. 2011.

[7] H. W. Mo and X. Q. Zuo, Artificial Immune System, Beijing: Science Press, 2009.

[8] R. B. Xiao and L. Wang. Artificial immune system: principle, models, analysis and perspectives. Chinese Journal of Computers, 2002, 25: 1281–1293.

[9] S. A. Hofmeyr, S. Forrest. Architecture for an artificial immune system. Evolutionary Computation, 2000, 8(4): 443–473.

[10] T. Li. Computer immunology, Beijing: Publishing House of Electronics Industry, 2004.

[11] http://www.artificial-immune-systems.org/icaris.shtml.

[12] S. Forrest, A. S. Perelson. Self-nonself discrimination in a computer. Proc. of IEEE Symposium on Security and Privacy, Oakland, CA, May, 1994.

[13] P. K. Harmer, P. D. Williams, et al. An artificial immune system architecture for computer security applications. IEEE Transaction on Evolutionary Computation, 2002, 6(3): 252-280.

[14] S. A. Hofmeyr. An immunological model of distributed detection and its application to computer security, Ph. D. dissertation, department of computer sciences, University of New Mexico, 1999.

[15] D. Dasgupta. Immunity-based intrusion detection system: a general framework. Proc. of the 22nd National Information Systems Security Conference (NISSC), 1999.

[16] J. Kim, P. J. Bentley. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection. Proc. of the Congress on Evolutionary Computation, 2002, pp. 1015-1020.

[17] T. Kavitha, D. Sridharan. Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security, 2010, (5): 31-44.

[18] V. Oleshchuk. Internet of things and privacy preserving technologies. Proc. of 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology(Wireless VITAE), Aalborg, Denmark, May, 2009, pp. 336-340.

[19] Y. Zhou, Y. G. Fang, Y. C. Zhang. Securing wireless sensor networks: a survey. IEEE Communications Surveys and Tutorials, 2008, 10: 6-28.

[20] A. Juels. RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381–394.

[21] Y. B. Zhou, D. G. Feng. Design and Analysis of Cryptographic Protocols for RFID. Chinese Journal of Computers, 2006, 29 (4) : 581-589.

[22] L. Mirowski, J. Hartnett. Deckard: A system to detect change of RFID tag ownership. International Journal of Computer Science and Network Security, 2007, 7(7): 89-98.

[23] Y. Yang, X. Wang, S. Zhu, G. Cao. Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks. Proc. of 26th IEEE International Symposium on Reliable Distributed Systems, IEEE Computer Society, 2007, pp. 219-228.

[24] Z. Q. Wu, Y. W. Zhou, J. F. Ma. A Security Transmission Model for Internet of Things. Chinese Journal of Computers, 2011, 34(8): 1351-1364.

[25] C. Y. Zhang. Architecture of Network Security. Chengdu: University of Electronic Science and Technology Press, 2006.