

Artificial Immunity-based Security Response Model for the Internet of Things

Caiming Liu

School of Information Science & Technology, Southwest Jiaotong University, Chengdu, China
School of Computer Science, Leshan Normal University, Leshan, China
Email: liucaiming@gmail.com

Yan Zhang^{*}, Zongyin Cai

School of Computer Science, Leshan Normal University, Leshan, China
Email: zhangyan_201016@163.com

Jin Yang

School of Computer Science, Leshan Normal University, Leshan, China
School of Information Science & Technology, Southwest Jiaotong University, Chengdu, China
Email: jinnyang@163.com

Lingxi Peng

Department of Computer and Education Software, Guangzhou University, Guangzhou, China
Email: manlx@163.com

Abstract—Rapid expansion of the Internet of Things (IoT) caused more and more security problems and attacks in particular. Secure IoT needs reasonable disposition after or when being attacked. To meet the above requirements of IoT security, a security response model for IoT based on artificial immune system is proposed in this paper. IoT data packets are captured and transformed into immune antigens which are defined in the real IoT security environment. Recognizer is defined and simulative to recognize harmful antigens. The immune mechanisms of antigen match, dynamic evolution of recognizer and self elements are simulative to adapt the real-time change of IoT. Abnormal antigens are recognized and their danger value is assessed. Strategy library of security response is constructed. Based on the danger of abnormal antigens which represent specific IoT data, reasonable security response array is calculated to respond to attacks. Experiments are simulative to realize proposed model. Their results show feasibility and effectiveness in security response for IoT.

Index Terms—Internet of Things, Artificial Immune System, Security Response, Attack

I. INTRODUCTION

The Internet of Things (IoT) [1] is confronted with similar security problems to traditional computer networks [2]. In addition, it has its specific complicated security environment. A lot of sense nodes are exposed to

open surrounding [3] and not available defended. Hostile intruders can relatively easily attack IoT systems through accessing sense nodes. Massive data coming from or going to the sense layer of IoT may suffer losses. The security situation is not optimistic.

The security problems of IoT have attracted high attention of researchers. The current research is mainly focused on privacy protection [4, 5], security model [6, 7], and etc. However, these security theories and technologies were restricted to static defense concept. Flexible adaptation to real IoT security environment and reasonable response to real-time IoT security events are urgent to be solved.

The security environment of IoT is changeful in real-time. The strategy of attack detection and response is not immutable. Static response methods for attacks threatening IoT applications have changeless strategy and can not meet the requirements of security response. Reasonable response theories and technologies need to be adaptive to different situations. Intelligent computation measures are worth being taken into account to resolve above-mentioned problems. In this paper, Artificial Immune System (AIS) [8] which is one of the most active intelligent computation methods and has the attributes self-learning and self-adaptation is used to resolve the adaptive response problems for IoT.

AIS imitates the excellent principles and mechanisms of Biological Immune System (BIS). It has been a research hotspot in the fields of bionics and computation intelligence. Since 2002, International Conference on Artificial Immune Systems has been held 11 times [9]. Based on the similarity between BIS and computer security issues, AIS was introduced into information

Manuscript received January 1, 2013; revised June 1, 2013; accepted July 1, 2013.

^{*}Corresponding author, zhangyan_201016@163.com.

security by relative researchers. There was much AIS based research literature [10, 11] in the fields of information security and others in recent years. In the traditional network security fields, AIS has been applied into computer virus defense, intrusion detection, security risk assessment, etc.

II. PROPOSED SECURITY RESPONSE MODEL

The proposed Artificial Immunity-based Security Response Model for the Internet of Things (AISRM) aims at recognizing and responding to attacks against IoT. It simulates the principles and mechanisms of AIS to be adaptive to security response for IoT.

A. Architecture of Security Response

The architecture of AISRM is shown in Fig. 1. It consists of 5 modules including data preprocessing, simulation of AIS principles, attack recognition, attack danger assessment and security response. Original IoT data is preprocessed and main signature information of IoT packets is got. AISRM simulates AIS data, recognizer and mechanisms to recognize attacks. The simulation makes it run the artificial immune principles in the real environment of IoT. Furthermore, it assesses the danger of recognized abnormal antigen. Moreover, it constructs strategy library of security response. Its ultimate goal is to respond to attacks reasonably.

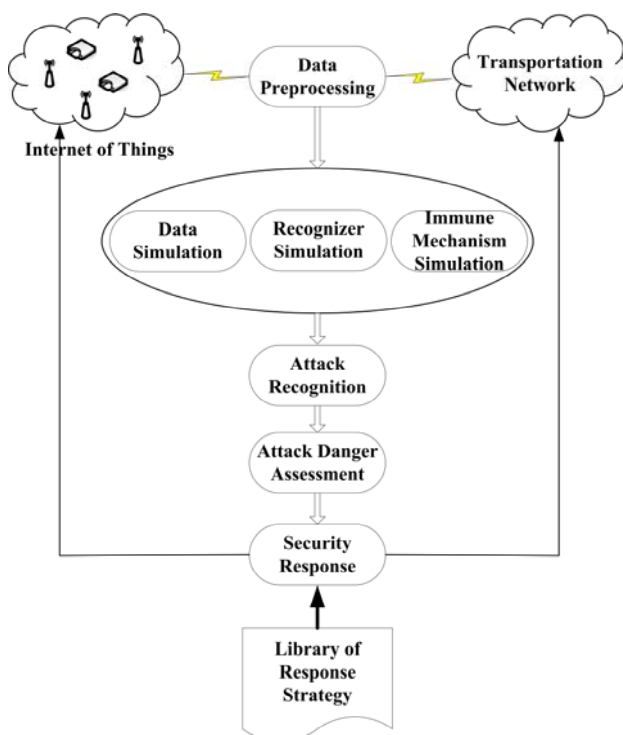


Figure 1. Architecture of AISRM.

B. Data Preprocessing

The original data to be analyzed comes from IoT traffic. Fig. 2 illustrates how IoT packets are captured and key data of IoT is got. AISRM captures IoT packets and extracts the packet head. Source IP address, target IP address, label ID of things, card reader ID, data timestamp and etc that express packet signature are extracted from the packet head.

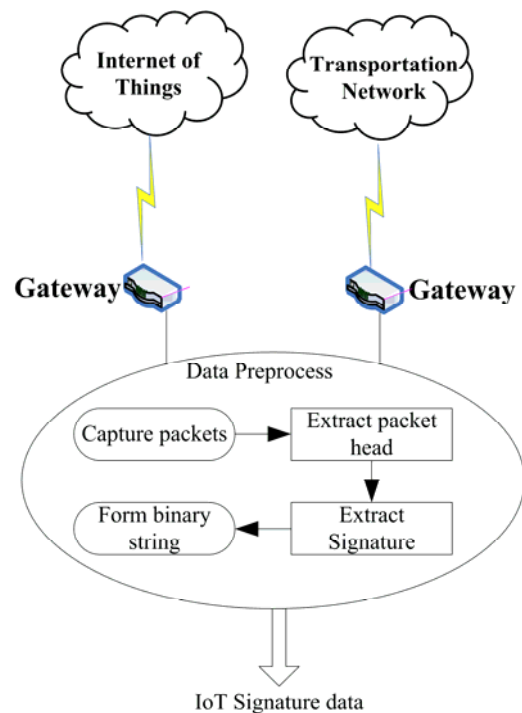


Figure 2. Process of Data Preprocessing.

Let the signature set of packet head be $SigHead$ which meets $SigHead = \{ \langle sIP, dIP, tID, rID, stmp \rangle \}$, where, sIP is the source IP address, dIP is the destination IP address, tID and rID means label ID of things and card reader ID, respectively, $stmp$ is the time when the packet is got. Let the IoT data be $IoTsig$ which is shown in Eq. (1).

$$IoT_{sig} = \{ \langle ID, i \rangle \mid ID \in N, i = s_1 \dots s_j \dots s_t \vee s_j \in \{0, 1\} \vee l \in N, i = BinaryString(h) \vee \forall h \in SigHead \} \quad (1)$$

Where, ID is the serial number, i is the primitive data and consists of binary characters, N is nature number set, the function $BinaryString()$ is used to transform the head information of IoT packets into binary strings, h is one of elements of $SigHead$.

In Eq. (1), IoT_{sig} contains the signature information of IoT packet. It comes from the original IoT data. It is generated by the process of data preprocessing which runs 4 steps including packets capturing, packet head extracting, signature extracting and binary string forming. The first step captures the IoT data which flows through IoT gateway and transportation gateway. The second step

extracts the heads of IoT packets. The third step extracts signature information of packet head. Finally, the fourth step transforms IoT signature information into binary strings which is used to judge whether IoT packets contain attacks.

C. Data Simulation

To use the principles of AIS, data in the environment of IoT needs to be simulated into antigen which is in immune style. Antigen in AISRM is defined as Def. 1.

Defenition 1. Let antigen set in IoT environment be A which meets $A = \{a \mid |a| = l, a = iot.i \wedge \forall iot \in IoT_{sig}\}$. The elements in A constitute the original data to be classified by AISRM.

Normal ones in A belongs to self set which is defined as S . Abnormal ones in A belongs to non-self set which is defined as N . Non-self antigens come from IoT data which contains attacks. They hide in all antigens. AISRM uses AIS principles to sort antigens input by the data preprocessing module into normal ones (self antigens) and abnormal ones (non-self antigens). Its final target is to respond to non-self antigens which may threaten IoT potentially.

D. Recognizer Simulation

In the immune system, immune cells are responsible for recognizing harmful antigens. AISRM uses recognizers to simulate immune cells to imitate the mechanism of the specificity recognition in AIS. Recognizers dynamically evolve to detect attacks against IoT. The data set of recognizer is defined as Def. 2.

Defenition 2. Let the data set of recognizer be R which meets $R = \{\langle ant, ag, cnt, tp, t, fam \rangle \mid ant \in U, ag, cnt, tp, t, fam \in I\}$, where, ant is the antibody string, I is nonnegative integer set, ag is the living time, cnt is the amount of recognized antigens, tp is the class, fam is the family's ID number, t is the thickness.

A recognizer have 6 domains including antibody string, living time, etc. The domain ant is the gene of recognizer. It is used to match antigen's binary string directly. The domain ag means how long the recognizer has lived since being generated. The domain cnt is added by 1 when the recognizer matches an antigen. It records how many antigens the recognizer has matched. Recognizers are sorted into three classes which include immature recognizer R_I , mature recognizer R_M and memory recognizer R_R . The domain tp indicates which class the recognizer belongs to. It is one of the class data set T which meets $T = \{i, m, r\}$. The elements in T delegate immature recognizer, mature recognizer and memory recognizer, respectively. Memory recognizers' antibody strings may be used generate immature recognizers through copy, part mutation, cross, etc. Immature recognizers may evolve into mature recognizers through immune self-adaptation mechanism. The domain fam of

the above relative memory, immature and mature recognizers is the same. It shows that they have the same ancestors. The domain t exclusively belongs to memory recognizers. It plus 1 makes the current thickness value after the recognizer recognizes a harmful antigen.

E. Immune Mechanism Simulation

AISRM adopts artificial immune mechanisms to make recognizers and self elements can be self-adaptive to the change of IoT environment. It takes advantage of dynamic strategy to evolve immune elements. It means that immune elements may be different in different moment. Let the data set Ω in the beginning be $\Omega(0)$. Let Ω at the moment t be $\Omega(t)$. The simulation of artificial immune mechanisms is described in the following.

1) Antigen Match

In immune systems, when antigens touch immune cells, immune cells recognize antigens through the antibodies spreading outside the surface of the immune cells. To simulate the mechanism, a match method that recognizers recognize antigens is needed. Presently, feasible matching methods include Hamming, Euclidean, r -Contiguous, and etc [13]. Most existing literatures on AIS based information security adopts r -Contiguous which judges whether a group binary string is the same between recognizer and antigen. Some effects of antigen matching were achieved in some ways. However, some binary characters are the same, but are not contiguous. The proposed model improves the traditional r -Contiguous and constructs grouped r -Contiguous match algorithm. It calculates the sum of groups which have the same characters and are not near to each other.

Grouped r -Contiguous match algorithm is used to judge whether recognizer matches antigen. It is shown in Eq. (2).

$$m_{group}(r, a) = \begin{cases} true, & \sum m_{r-Contiguous}(r, a) \geq \varepsilon \\ false, & Otherwise \end{cases} \quad (2)$$

Where, $r \in R$, $a \in A$, ε is the threshold of group, it meets $1 \leq \varepsilon \leq \lfloor l/\gamma \rfloor$ (See the detail of γ in Eq. (3)), $m_{r-Contiguous}()$ is a single group match function which is shown in Eq. (3).

$$m_{r-Contiguous}(r, a) = \begin{cases} 1, & \forall j \wedge k \leq j \leq k + \gamma - 1 \wedge \\ & 1 \leq k \leq l - \gamma + 1, r.ant_j = \\ & a_j, j, k, \gamma \in I \\ 0, & Otherwise \end{cases} \quad (3)$$

Where, I is nonnegative integer set, γ is the amount of binary chars of contiguous match.

2) Dynamic Evolution of Recognizer

Immature recognizers are generated randomly or by memory ones through the methods of copy, part mutation,

cross, etc. They are evolved into mature recognizers through self-tolerance [13]. Mature recognizers are activated when they reach the threshold of activation threshold and evolved into memory ones. The dynamic evolution process of recognizer is shown in Fig. 3. The lines with arrows point to the flow direction of recognizers. Deletion surrounded by a circle means the death of recognizers. Fig. 3 shows that the evolution process of recognizer is dynamical and circulatory. Recognizers are stimulated by the change of IoT security environment. It is similar to the growing progress of immune cells in BIS. Immature recognizer is used to generate diversity. Attacks against IoT are constantly changing. They may have entirely different signature information. New immature recognizers are generated to match new signature of attacks gradually. They must accept self-tolerance. Mature recognizer reflects medial stage of recognizer evolution. It hasn't been activated and can not recognize harmful antigens. Once it is activated, it will be evolved into memory recognizer which can recognize attacks.

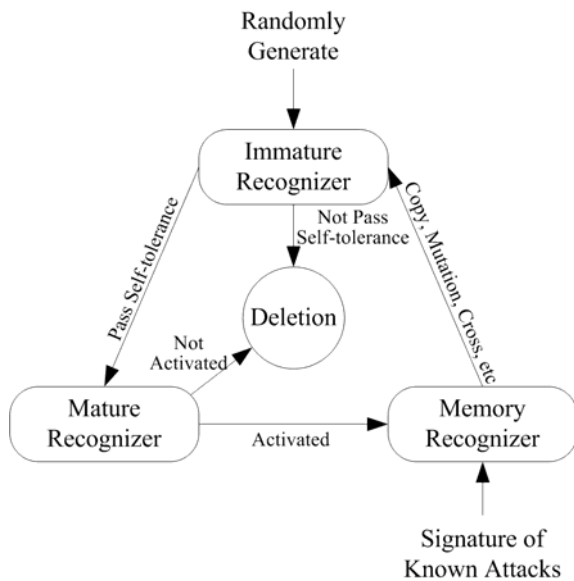


Figure 3. Dynamic Evolution Process of Recognizer.

The above dynamic evolution process of recognizer is deduced with math methods in the following.

In the beginning, the immature recognizer set is empty. After that, the proposed model generates new immature recognizers gradually. Meanwhile, it deletes some old immature recognizers which match self antigens or are out of date. Immature recognizer set at the moment t is shown in Eq. (4).

$$R_I(t) = \begin{cases} \emptyset, & t = 0 \\ R_I(t-1) - f_{tolerance}(R_I(t-1)) - \\ & R_{I_death}(t-1) \cup R_{I_new1}(t) \\ & \cup R_{I_new2}(t) \cup R_{I_new3}(t), & t > 0 \end{cases} \quad (4)$$

In Eq. (4), $f_{tolerance}()$ is the function of self tolerance. It returns the recognizer set which passed self-tolerance. The recognizers in it do not match self antigens in a period of time. They will be evolved into mature recognizers potentially. $f_{tolerance}()$ is shown in Eq. (5).

$$f_{tolerance}(R_I(t-1)) = \{r | r \in R_I(t-1), r.age \geq \alpha, \\ \forall s \in S(t-1) \wedge m_{group}(r, s) = false\} \quad (5)$$

Where, α is the period threshold of self-tolerance.

In Eq. (4), $R_{I_death}(t-1)$ is the data set of immature recognizer that did not pass self tolerance. Each immature recognizer in it matches a self antigen at least in the period threshold of self-tolerance. These immature recognizers will recognize normal antigens as attacks. They are useless to the proposed model and need to be deleted. $R_{I_death}(t-1)$ is shown in Eq. (6).

$$R_{I_death}(t-1) = \{r | r \in R_I(t-1), r.age < \alpha, \\ \exists s \in S(t-1) \wedge m_{group}(r, s) = true\} \quad (6)$$

In Eq. (4), $R_{I_new1}(t)$ is the data set of newly generated immature recognizer by common memory recognizers. Superior memory recognizers are chosen to be copied, mutated and crossed to generate new immature recognizers. $R_{I_new1}(t)$ is shown in Eq. (7).

$$R_{I_new1}(t) = \{r | \forall r' \in R_R(t), r.ant = \\ AntProduce(r'.ant), r.ag = 0, \\ r.cnt = 0, r.tp = T.i, r.fam = r'.fam\} \quad (7)$$

Where, the function $AntProduce()$ produces antibody string of new immature recognizers. The domain of antibody string of new immature recognizers comes from memory recognizers. The domain of family's ID number is set as the same of memory recognizers. The other domains are set as initial states.

In Eq. (4), the data set $R_{I_new2}(t)$ includes new immature recognizers generated by active memory recognizers that recognize harmful antigens. It is shown in Eq. (18). The data set $R_{I_new3}(t)$ contains new immature randomly generated by the proposed model.

Likewise, the initial mature recognizer set is empty. Mature recognizers are in the medial stage of self-adaptation. They have some ability to be evolved into memory recognizers. However, they can not be used to recognize abnormal antigens. Mature recognizer set at the moment t is shown in Eq. (8).

$$R_M(t) = \begin{cases} \emptyset, & t = 0 \\ R_M(t-1) - R_{M_death}(t-1) - R_{M_toR}(t-1) \\ & \cup ToMatureReg(f_{tolerance}(R_I(t-1))), \\ & t > 0 \end{cases} \quad (8)$$

At the moment t , the proposed model deletes two parts of mature recognizer which are not activated or updated. Meanwhile, it supplements new ones which are evolved into through immature recognizers.

In Eq. (8), $R_{M_death}(t-1)$ is the data set of mature recognizer that was not activated by antigens. It is shown in Eq. (9).

$$R_{M_death}(t-1) = \{r | r \in R_M(t-1), r.cnt < \delta, r.ag \geq \lambda\} \quad (9)$$

Where, δ is the activation threshold immature recognizer, λ is the lifecycle threshold of immature recognizer.

In Eq. (8), $R_{M_toR}(t-1)$ is the data set of activated mature recognizer. It will be evolved into memory recognizers. It is shown in Eq. (10).

$$R_{M_toR}(t-1) = \{r | r \in R_M(t-1), r.cnt \geq \delta, r.ag < \lambda\} \quad (10)$$

In Eq. (8), $ToMatureCell(R_{temp})$ is the data set of new mature recognizer that comes from immature recognizer. It is shown in Eq. (11).

$$ToMatureRe g(R_{temp}) = \{r | \forall r_i \in R_{temp}, r.cnt = 0, r.ag = 0, r.tp = T.m, r.family = r_i.family\} \quad (11)$$

Where, $R_{temp} = f_{tolerance}(R_l(t-1))$.

Memory recognizers are in the top stage of self-adaptation in the proposed model. They have accurate antibody strings to match abnormal antigens. The initial memory recognizer set is set by security managers and its elements come from signature information of classical attacks. It helps the proposed model have initializing recognition ability of attacks. Memory recognizer set at the moment t is shown in Eq. (12).

$$R_R(t) = \begin{cases} \{r_1, K, r_i, K, r_n\}, i, n \in I, t = 0 \\ R_R(t-1) \cup ToMemoryRe g(R_{M_toR}(t-1)), t > 0 \end{cases} \quad (12)$$

In Eq. (12), the function $ToMemoryCell()$ is used to convert activated mature recognizer into new memory recognizer which is an important achievement learned by the proposed model. It indicates that the proposed model own the new recognition ability of fresh attacks. $ToMemoryCell()$ is shown in Eq. (13).

$$ToMemoryRe g(R_{temp}) = \{r | \forall r_i \in R_{temp}, r.tp = T.r, r.fam = NewFam(\)\} \quad (13)$$

In Eq. (13), the new memory recognizers which are evolved into through activated mature recognizers have their new family's ID number which is generated by the function $NewFam()$. The values of the domain fam are new and different from existing values. It means that new family of recognizers is generated.

3) Dynamic Evolution of Self

Self antigens are normal antigens. They play an exclusive role to train recognizers to avoid recognizing normal antigens. They adopt the self-tolerance (See detail in Eq. (5)) mechanism to evolve immature recognizers into mature ones directly.

The initial self set is set by security managers. The self antigens in it are got in the pure and security environment of IoT. They must be normal ones. Or else, recognition rate of attacks will be affected negatively. Self set at the moment t is shown in Eq. (14).

$$S(t) = \begin{cases} \{s_1, K, s_i, K, s_n\}, i, n \in I, t = 0 \\ S(t-1) \cup ToSelf(A_n(t-1)), t > 0 \end{cases} \quad (14)$$

Where, $ToSelf()$ is the function to convert harmful antigens into self elements, $A_n(t-1)$ is the normal antigen set at the last moment.

After a batch of antigens is detected by recognizers, special response measures are adopted to respond to abnormal antigens (See detail in H section). Normal antigens are transformed into self antigens. It may improve the ability of self-tolerance.

F. Attack Recognition

AISRM uses recognizers and the above immune mechanisms to recognize abnormal IoT data (Attacks) from real-time antigens.

The antigen data set to be detected at the moment t is shown in Eq. (15).

$$A(t) = \begin{cases} \emptyset, t = 0 \\ \{a | |a| = l, a = iot.i \wedge \forall iot \in IoT_{sig}(t)\}, t > 0 \end{cases} \quad (15)$$

Let harmful antigen data set recognized by recognizers and normal antigen data set be A_h and A_n . They are shown in Eq. (16) and Eq. (17).

$$A_h(t) = \begin{cases} \emptyset, t = 0 \\ \{a | \forall a \in A(t), \exists i \in I_R(t) \wedge m_{group}(i, a) = true\}, t > 0 \end{cases} \quad (16)$$

$$A_n(t) = \begin{cases} \emptyset, t = 0 \\ A(t) - A_h(t), t > 0 \end{cases} \quad (17)$$

Once a memory recognizer recognizes a harmful antigen, it takes immune clonal expansion [13] mechanism to generate new immature recognizers that are shown in Eq. (18) and meet Eq. (19).

$$R_{r_new2}(t) = \begin{cases} \emptyset, t = 0 \\ \{r | \forall a \in A(t), \exists r' \in R_R(t) \wedge m_{group}(r', a) = true, r.ag = 0, r.cnt = 0, r.tp = T.i, r.fam = r'.fam\}, t > 0 \end{cases} \quad (18)$$

$$|R_{t_new2}(t)| = \lceil \tau ar \sinh(r't) \rceil \quad (19)$$

Moreover, it accumulates its thickness. The memory recognizers that recognize harmful antigens are shown in Eq. (20). In Eq. (21), they update their thickness. After be updated, the whole memory recognizer set is shown in Eq. (22).

$$R_{R_reg}(t) = \{r \mid \forall a \in A(t), \exists r' \in R_R(t) \wedge m_{group}(r', a) = true, r.ag = r'.ag, r.cnt = r'.cnt, r.tp = r'.tp, r.fam = r'.fam\} \quad (20)$$

$$R_{R_reg}'(t) = \{r \mid \forall r' \in R_{R_reg}(t), r.ag = r'.ag, r.cnt = r'.cnt, r.tp = r'.tp, r.fam = r'.fam, r.t = r'.t + 1\} \quad (21)$$

$$R_R(t) = (R_R(t) - R_{R_reg}(t)) \cup R_{R_reg}'(t) \quad (22)$$

G. Danger Assessment of Abnormal Antigen

The danger of the above abnormal antigens recognized by memory recognizers is decided by thickness of relative memory recognizers, harmfulness of relative attacks and value of target IoT asset. Let the data set of danger array be D which is shown in Eq. (23).

$$D(t) = \left\{ \langle ID, r, dan \rangle \mid ID \in N, \forall r' \in R_{R_reg}'(t), r = r', dan = f_{danger}(r') \right\} \quad (23)$$

Where, ID is the serial number of relative IoT data, dan is the danger value.

The function $f_{danger}()$ is used to compute danger value and limit it to the closed interval $(0, 1)$. It is shown in Eq. (24).

$$f_{danger}(r) = 1 - \frac{1}{1 + \ln(r.t \times Harm(r) \times v + 1)} \quad (24)$$

Where, v is the value of the target IoT asset, $Harm()$ is the function to calculate the harmfulness of relative attack. AISRM adopts the method of [14] to construct $Harm()$.

H. Security Response

Let the data set of strategy library of security response be SL that is shown in Eq. (25).

$$SL = \{ \langle sID, Strategy, Function, DanThr \rangle \} \quad (25)$$

Where, sID is serial number of security strategy, $Strategy$ is the name, $Function$ is what the strategy can do, $DanThr$ is the response threshold that is based on [14].

Strategy library of security response is listed in Table 1. The meaning of columns of Table 1 is shown in Eq. (25).

TABLE I.
STRATEGY LIBRARY OF SECURITY RESPONSE

sID	$Strategy$	$Function$	$DanThr$
1	<i>Logging</i>	Record attack events	0.4
2	<i>Alarm</i>	Send alarm information to managers	0.55
3	<i>Forensic</i>	Take the evidence of attacks	0.6
4	<i>Modification</i>	Modify the IoT data packet	0.7
5	<i>Part Deletion</i>	Delete part of the IoT data packet	0.8
6	<i>Abandonment</i>	Abandon the IoT data packet	0.9
7	<i>Isolation</i>	Disconnect network	0.98

Based on the danger of recognized abnormal antigens, one or more response strategy may be implemented. Let the data set of security response array be RA that is shown in Eq. (26).

$$RA(t) = \{ \langle ID, sID \rangle \mid \forall d \in D(t) \wedge \forall sl \in SL \wedge d.dan \geq sl.DanThr, ID = d.ID, sID = sl.sID \} \quad (26)$$

III. EXPERIMENTS AND SIMULATION

The experiments are used to test and verify the feasibility and effectiveness of AISRM. Emulational IoT network topology that is shown in Fig. 4 was constructed. The proposed model AISRM runs in AISRM server that has two network adapters. One adapter connects to simulative gateway of sense network. Another adapter connects to simulative gateway of transportation network. Two computer terminals are simulative to send and receive sense data. Moreover, they simulate attack packets.

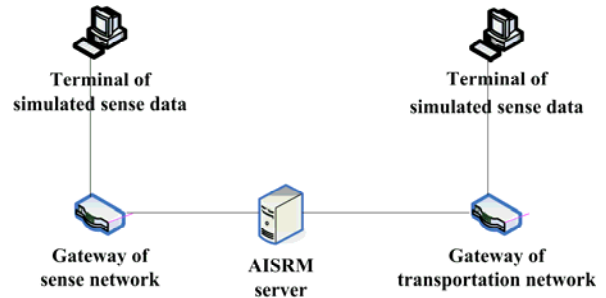


Figure 4. Emulational IoT Network Topology.

The simulation experiment continued for 5 hours. The two computer terminals of sense data simulated two

classes of attacks including cloning and denial of service [15] against IoT. They sent different number of attack packets every 20 minutes. It aimed at making different security environment in different time. Fig. 5 shows the results of attack intensity and danger. It indicates that the trend of attack danger is similar with the attack intensity. It verifies that AISRM can dynamically recognize attacks and effectively assess attack danger.

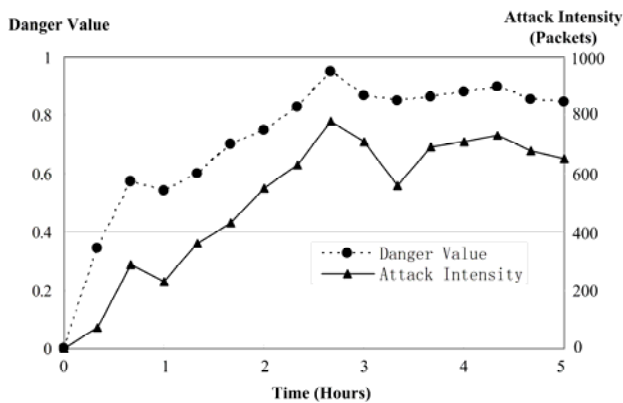


Figure 5. Results of Attack Intensity and Danger.

Table 2 shows the results of security response. The response strategy of Logging happened most often. Its reason is that the danger threshold of Logging is the lowest. Isolation strategy never happened because there were not higher danger values of attacks than its danger threshold. In this simulation experiment, more than 8,000 attack packets were simulative. However, not all danger values of them reached any danger threshold in the strategy library of security response. Therefore, response times of each response strategy were not greater than 8,000.

TABLE II.
RESULTS OF SECURITY RESPONSE

ID Number	Response Strategy	Response Times
1	Logging	7995
2	Alarm	7765
3	Forensic	7480
4	Modification	7120
5	Part Deletion	6140
6	Abandonment	1510
7	Isolation	0

IV. CONCLUSION

Attacks bring secure issues to IoT applications. They obstruct the normal running of IoT in some way. Traditional detection theories and technologies can not directly respond to attacks against IoT and adapt the changeful security environment of IoT. This paper adopts the perfect attributes of AIS to propose a security response model to meet the above security requirements. The proposed model used AIS principles and simulated AIS mechanisms to dynamically evolve recognizers and other immune elements to recognize abnormal IoT data which contains attacks. It computed the danger value and constructed strategy library of security response. Finally, it derived security response array which was directly used to respond to attacks. Results of simulation experiment show that proposed model is feasible and effective to security response for IoT attacks.

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) and the Scientific Research Fund of Sichuan Provincial Education Department (No. 13ZA0107 and 13ZB0106).

REFERENCES

- [1] ITU, ITU Internet Reports 2005: The Internet of Things, Geneva: ITU, 2005.
- [2] G. Yang, J. Xu, W. Chen, et al, "Security Characteristic and Technology in the Internet of Things," *Journal of Nanjing University of Posts and Telecommunications (Natural Science)*, vol. 30, pp. 20–29, 2010.
- [3] C. M. Medaglia, A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," *Proc. of the Internet of Things: 20th Tyrehenian Workshop on Digital Communications*, pp. 389-395, 2010.
- [4] 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, pp. 336-340, May, 2009.
- [5] G. P. Zhang, W. T. Gong, "The Research of Access Control Based on UCON in the Internet of Things," *Journal of Software*, vol. 6, pp. 724–731, 2011.
- [6] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," *Communications in Computer and Information Science*, vol. 89, pp. 420–429, 2010.
- [7] Z. Q. Wu, Y. W. Zhou, J. F. Ma, "A Security Transimission Model for Internet of Things," *Chinese Journal of Computers*, vol. 34, pp. 1351-1364, 2012.
- [8] S. A. Hofmeyr, S. Forrest, "Architecture for an artificial immune system," *Evolutionary Computation*, vol. 8, pp. 443–473, 2000.
- [9] ICARIS, <http://www.artificial-immune-systems.org/icaris.shtml>.
- [10] P. K. Harmer, P. D. Williams, et al., "An artificial immune system architecture for computer security applications," *IEEE Transaction on Evolutionary Computation*, vol. 6, pp. 252–280, 2002.

- [11] Y. W. Liang, H. Yang, J. Fu, C. Y. Tan, A. L. Liu and S. W. Zhu, "The Effect of Real-valued Negative Selection Algorithm on Web Server Aging Detection," *Journal of Software*, vol. 7, pp. 849–855, 2012.
- [12] S. Forrest, S. A. Hofmeyr, A. Somayaji, "Computer immunology," *Communications of the ACM*, vol. 40, pp. 88–96, 1997.
- [13] T. Li, "Computer immunology," Beijing: Publishing House of Electronics Industry, 2004.
- [14] Y. Zhang, C. M. Liu, C. R. Chen, "A Computation Method on Harm Degree for IoT Security Threat," *China Computer&Communication*, pp. 31–33, 2012.
- [15] A. Mitrokotsa, M. R. Rieback, A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Inf. Syst. Front*, vol. 12, pp. 491–505, 2010.

Caiming Liu obtained the master and doctor degrees in Computer Science from Sichuan University, China, in 2005 and 2008, respectively. He is an associate research fellow at Leshan Normal University, China. At the same time, he is a postdoctor at Southwest Jiaotong University, China. His research interests include network security and artificial immune system.

Yan Zhang obtained the master degree in Computer Science from Sichuan University, China, in 2008. She is a lecturer at Leshan Normal University, China. Her research interests include network security and artificial immune system.

Zongyin Cai obtained the master degree in Computer Science from University of Electronic Science and Technology of China in 2006. She is a lecturer at Leshan Normal University, China.

Jin Yang obtained the doctor degree in Computer Science from Sichuan University, China, in 2007. He is an associate professor at Leshan Normal University, China. His research interests include network security and artificial immune system.

Lingxi Peng obtained the master degree in Computer Science from Southwest Petroleum University and the doctor degree in Computer Science from Sichuan University, China, in 2005 and 2008, respectively. He is an associate professor at Guangzhou University, China.