Research Journal of Applied Sciences, Engineering and Technology 5(22): 5255-5259, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: October 22, 2012 Accepted: December 19, 2012 Published: May 25, 2013

Distributed Danger Assessment Model for the Internet of Things Based on Immunology

[1]Run Chen, [1]Jiliu Zhou and [2, 3]Caiming Liu
[1]School of Computer Science, Sichuan University, Chengdu 610065, China
[2]School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China
[3]Laboratory of Intelligent Information Processing and Application, Leshan Normal University, Leshan 614000, China

Abstract: The Internet of Things (IoT) confronts complicated and changeful security threats. It harms IoT and brings IoT potential danger. However, the research achievements of the danger assessment technology for IoT are rare. To calculate the danger value of IoT with many dispersive sense nodes, the theoretical model of distributed danger assessment for IoT is explored in this paper. The principles and mechanisms of Artificial Immune System (AIS) are introduced into the proposed model. Data packets in IoT are captured in each gateway and converted into antigens in the simulated immune environment. Detectors use self-learning and self-adaptation mechanisms in AIS to evolve themselves to adapt the local IoT environment and detect security threats. The mechanism of antibody density is simulated to reflect the intensity of security threats which are happening. Through the detected security threats and their intensity, the values of IoT property and security threats' harm are combined to assess the quantitative value of danger for IoT. Theoretical analysis shows that the proposed model is significative of theory and practice.

Keywords: Artificial immune system, danger assessment, internet of things, security threat

INTRODUCTION

Along with the fast development of the Internet of Things (IoT) (ITU, 2005), security threats which harm IoT seriously are paid close attention to. The security threats bring IoT potential danger. It is very necessary to detect what security threat is happening in IoT and assess the situation confronted with danger. On the research of traditional computer network, the assessment technology of security situation was studied (Chen *et al*., 2006; Wei *et al*., 2009). It discovers danger and evaluates the quantitative or qualitative security situation according to the current and potential security threats. However, the danger assessment technology for IoT is rare. It can make the administrators be clear of the security situation and risk (Feng *et al*., 2004) of IoT. Furthermore, it may help the administrators work out the target-oriented and reasonable security defense strategy of IoT to change the passive situation of security defense.

The user ends in IoT do not limit to computers. They are expanded to Thing to Thing (T2T), Human to Thing (H2T) and Human to Human (H2T) (ITU, 2005). A lot of polygenetic and style-different data which is massive is enabled to access to the sense layer of IoT. Although IoT breaks through the applications Internet, mobile communication and sensor networks and improves them, hidden dangers of potential serious security exist in IoT because of the access, transport and treatment way of the IoT information. The randomly distributed and ubiquitous access way makes attackers implement security threats more easily and conveniently. At the same time, the wireless sensor network is largely applied to IoT. It makes the transport networks of IoT unsteady. In view of the foregoing, IoT confronts a lot of complicated security threats which not only impact the normal applications of IoT but also are bound to cause some severe problems such as user privacy leak, denial of service, system fault, system failure, and etc (Juels, 2006; Liu and Hu, 2010; Oleshchuk, 2009; Padmavathi and Shanmugapriya, 2009; Karygiannis *et al*., 2007; Kavitha and Sridharan, 2010; Karygiannis *et al*., 2006). Therefore, it is significative of theory and practice application value to survey the security threats in IoT and establish an effective danger assessment technology of IoT.

The danger assessment technology for IoT can greatly improve the traditional security technology for IoT. Presently, the research on the technology is still in the starting stage. It was covered by few documents in the recent years. The key technologies include surveying of security threat, computation of security threat

Corresponding Author: Caiming Liu, Department of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China

intensity, and etc. To resolve the first problem, Mirowski and Hartnett (2007) proposed an intrusion detection method according to the last visit frequency of a thing tag. His detection method can only discover the IoT attacks which aim at the change of a tag ownership and cannot do anything against other attacks. Besides that, most researchers proposed some basic ideas or simple concepts for the IoT intrusion detection. Furthermore, their ability of attack detection limits. Their ideology is based on the traditional intrusion detection technology of Internet and cannot adapt the special security requirements of the IoT environment entirely. To resolve the second problem, there still lacks research achievements for the computation of IoT security threat intensity. In addition, the literature which introduces the computation of IoT security threat intensity is rare. Many difficult points exist in the research of the computation of IoT security threat intensity.

To overcome the problems confronted by the danger assessment for IoT, the excellent mechanisms of Artificial Immune System (AIS) (Xiao and Wang, 2002; Jiao and Du, 2003; Li, 2004; Mo and Zuo, 2009) are introduced into this paper to explore an effective way to survey IoT security threats and calculate the intensity of security threats. AIS has the good attributes of distributed and parallel treatment, diversity, self-organization, self-adaptation, robustness, and etc. It attracted a lot attention of many researchers in recent years. Because the problems found in an information security system are quite similar to those encountered in a biological immune system (Li, 2004), AIS is broadly applied to resolve the problems of information system security. Especially, it has indicated the effective ability in the fields of intrusion detection (Kim and Bentley, 2002; Dasgupta, 2002; Hofmeyr, 1999) and security risk assessment (Li, 2005; Wang *et al*., 2005).

This study proposes a Distributed Danger Assessment Model for the Internet of Things Based on AIS (DDAM). It opens up a new effective way to calculate danger value for IoT. In the following, the artificial immune principle will be introduced into DDAM and the theory model of DDAM will be established, good mechanisms in AIS will be simulated, the realization way of IoT security threats surveying, security threat intensity computation and quantitative danger assessment will be deduced with math methods.

DESCRIPTION OF DDAM

Architecture of DDAM: The architecture of DDAM is shown in Fig. 1. DDAM adapts the distribution mechanism. It is made up of Security threat Detection Node (SDN) and Danger Assessment Center (DAC). SDN is deployed in local IoT environment and connected to the gateway by pass. In SDN, the datagram in IoT is captured by the system and is transformed into

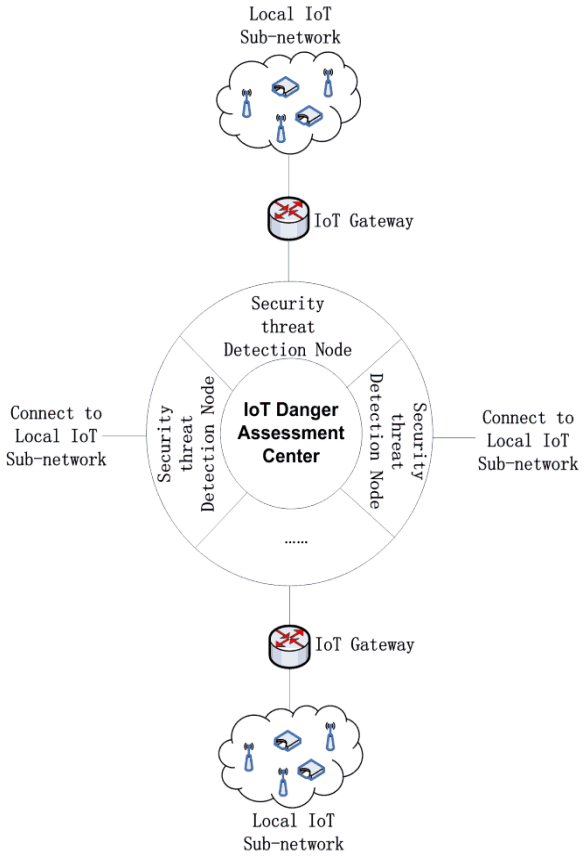

Fig. 1: The architecture of DDAM

the data in immune style. The data is probed by immune elements with the immune principles and mechanisms to judge whether it contains security threats which do harm to IoT. At the same time, the immune elements which detect IoT security threats accept self-adaptation in local IoT environment. Each SDN works independently to realize distributed and parallel detection of security threats. Then, it sends the information of detected security threats to DAC. In DAC, the detection data of security threats in all SDNs is gathered and used to calculate the quantitative danger value.

Security threat detection node:

- **Information simulation:** The signature information in IoT sense layer is used to simulate the antigens in an immune system. Let the antigen set be $Ag = \{ag| ag \in U, |ag| = l\}$, where, $Ag \subset U$, $U = \{0, 1\}^l$. The antigen *ag* is made up of *l*-long (*l* is a nature number) binary strings which are extracted from the signature information of datagram. Let the normal datagram and abnormal datagram with security threats in the sensor layer of IoT be *S* and *N*, separately. *S* and *N* meet $S \cup N = Ag$, $S \cap N = \emptyset$.

The detector is defined to simulate the immune cells in an immune system. Let the detector set be D =

{(gene, age, count, type, family)|gene ∈ Ag, age, count, type, family ∈ N, where, gene is the detector's gene, it is a binary string which matches antigens, *N* is a nature number set, count is the number of antigens matched by the detector, age is the life generations of the detector, type denotes the type of the detector, type ∈{i, m, r}, the three elements delegate immature detector, mature detector and memory detector respectively, family is the serial number of the detector ethnic group, it is corresponding to the ID number of an IoT attack.

The detector set includes immature, mature and memory detectors. Let the data set of them be D_I, D_M and D_R, respectively.

The function $f_{match}()$ is constructed to computer whether a detector matches an antigen. Presently, feasible matching methods include *r*-Contiguous, Hamming, Euclidean, and etc. Let a detector be d and an antigen be *ag*. $f_{match}()$ is shown in Eq. (1):

$$f_{match}(d, ag) = \begin{cases} 1, & \text{match} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

where, the return value 1 denotes that d matches *ag*, and vice versa.

- **Dynamical evolution of detector and self:** After the immature detectors passed the process of self-tolerance, they take possession of the initial ability to detect IoT security threats and will evolve to mature ones. Partial captured antigens in *Ag* are proportionally selected to be input into the proposed model to train mature detectors. The mature detector set at the moment t is shown in Eq. (2):

$$D_M(t) = \begin{cases} \varnothing, & t = 0 \\ D_M(t-1) - D_{M\_death}(t-1) - \\ D_{M\_toR}(t-1) \cup ToMatureCell(\,), & t > 0 \end{cases} \quad (2)$$

where, D_{M_death}(t-1) denotes the mature detectors which failed to be activated, D_{M_toR}(t-1) denotes the mature ones which were activated, the function of ToMatureCell() is to transform immature detectors into mature ones, the parameter of ToMatureCell() is the immature detector set which succeeded to pass self-tolerance (Li, 2004).

After the mature detectors are activated, they have owned enough detection ability against security threats. In the proposed model, a message about the activation event of a mature detector is sent to the security administrator of IoT. The administrator co-stimulates the mature detector and confirms that it is switched to a memory detector. The memory detector is immortal. When it matches a harmful antigen (security threat), it enters the status of activation and new immature detectors proliferate with it. Through the above mechanism, the activated memory detector expands the amount of its ethic group. The memory detector set $D_R(t)$ at the moment *t* is shown in Eq. (3):

$$D_R(t) = \begin{cases} \{r_1, \ldots, r_i, \ldots r_n\}, & i, n \in N, t = 0 \\ D_R(t-1) \cup \\ ToMemoryCell\left(D_{M\_toR}(t-1)\right), & t > 0 \end{cases} \quad (3)$$

where, the function of ToMemoryCell()is to transform D_{M_toR}(t-1) into memory detectors, ToMemoryCell (D_{M_toR}(t-1))) returns the memory detectors newly generated.

After being detected, the antigen set *Ag* is classified into IoT attacks and normal antigens. To improve the self-adaptation ability of the proposed model to the IoT environment, the validated normal antigens will be switched into self elements to train the immature detectors newly generated. Let the set of the validated normal antigens be Ag_{normal}(t-1) at the moment *t*-1. The self set S(t) at the moment t is shown in Eq. (4):

$$S(t) = \begin{cases} \{s_1, \ldots, s_i, \ldots, s_n\}, & i, n \in N, t = 0 \\ S(t-1) \cup ToSelfCell\left(Ag(t-1)\right), & t > 0 \end{cases} \quad (4)$$

where, the function of ToSelfCell is to transform the validated normal antigens to self elements.

Synchronization technology of SDN: In a Security threat Detection Node, detectors detect and accept the training of the input antigens. With the mechanisms of self-adaptation and self-learning, antigens can train some enough good detectors to recognize mutated, even new unknown security threats. These good detectors which own the accurate detection ability to recognize harmful antigens and are good at adapting IoT environment are new memory detectors. In the local SDN, it takes the cost of much resource and time to generate new memory detectors. The other SDNs are not necessary to consume some cost to train the same memory detectors. Therefore, the learning achievements (new memory detectors) in a local SDN are needed to be shared with the other SDN to improve the global detection ability of IoT.

The following will describe the process of SDN synchronization whose principle is shown in Fig. 2. The process of SDN synchronization includes two stages: vaccination and self-tolerance in local IoT environment.

- **Vaccination:** In the biological immune system, the conception of vaccination is that a vaccinum is injected into biological bodies to make the biological bodies be immune to special pathogens. In this paper, the above mechanism is simulated to vaccinate all the SDNs in the global scope of IoT. It can make all the SDNs have the recognition ability of new security threats.

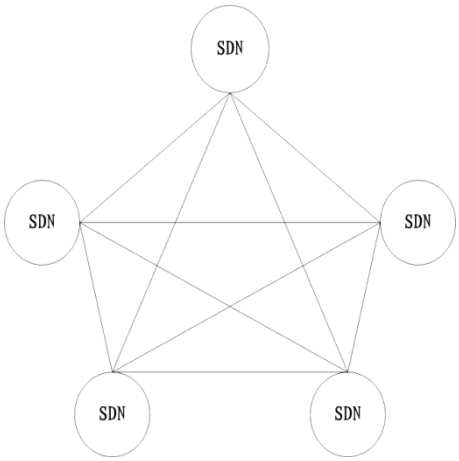

Fig. 2: The synchronization of SDN

- **Self-tolerance in local IoT environment:** Once a vaccinated SDN accepts a vaccinum, it decomposes the vaccinum as the information of a new memory detector r_{new} which will be saved in the local SDN. The memory detector r_{new} owns excellent ability of security threat detection. However, it was trained in the different local IoT environment relative to the vaccinated SDN. It may not adapt the IoT environment of the vaccinated SDN. It is possible to recognize self antigens in local environment. Therefore, r_{new} must accept the process of self-tolerance in the vaccinated SDN. After r_{new} passes the process of self-tolerance, it will be transformed to a memory detector which will join the memory detector set D_R and start the detection and recognition job of security threats in local IoT.
- **Forming mechanism of security threat intensity:** The key question of quantitative danger assessment for IoT is how to compute the intensity value of security threats confronted by IoT. In this paper, the intensity formulation mechanism of immune cells in an immune system is simulated to quantificationally express the security threat intensity in IoT. In the biological immune system, when recognizing specific pathogens, the activated immune cells quickly perform the process of clonal expansion. They generate plasmacytes to form a lot of antibodies. The new antibodies expand the scale of ethic group of the activated immune cells to eliminate massive pathogens. Through the above mechanism, memory detectors in the proposed model use the clonal expansion to form the intensity of security threats which are relative to their corresponding memory detectors.

Let the memory detector which recognizes an harmful antigen be r_{detect}. The proposed model uses r_{detect} to implement the process of clonal expansion. It takes advantage of the gene of r_{detect} to generate new immature detectors with the operations of cross, mutation and recombination. The new immature detectors inherit the serial number of r_{detect}. In the process of ethic group expansion of r_{detect}, when r_{detect} recognize an antigen, the amount of new immature detectors cloned by r_{detect} is $\zeta = [\tau ar\sinh(d_{detect}.count)]$, where, τ is a coefficient of ethic group expansion. Along with the constant growth of harmful antigens detected by r_{detect}, the number of ethic group increases sharply to form the intensity of security threats in IoT.

If r_{detect} does not detect any harmful antigens in the period ψ, the number of new immature detectors cloned by it declines gradually. Let the time quantum in which r_{detect} didn't recognize any harmful antigens be t_{no_detect}. In t_{no_detect}, r_{detect} clones new immature detectors whose amount is:

$$\xi' = \left\lfloor \tau ar\sinh\left(d_{detect}.count - \left\lceil \frac{t_{no\_detect}}{\psi} \right\rceil \right) \right\rfloor$$

The clone process does not stop until $d_{detcet}.count-[t_{no\_detect}/\psi] \leq 0$. After this moment, r_{detect} does not clone any new immature antigens. New immature antigens which fail in self-tolerance and new mature detectors which are not activated will die little by little. The number of ethic group of r_{detect} will fall to the lowest value.

Danger assessment center: The above mechanism of ethic group change of a memory detector reflects the real-time intensity change of security threats in the IoT environment. The coned immature detectors which succeed to accept self-tolerance will evolve to new mature detectors. Therefore, the number of ethic group of r_{detect} is equal to the number of immature and mature detectors whose ethic group number is $r_{detect.}$family.

The intensity of security threats confronted by IoT is expressed by the number of ethic group of r_{detect}.

Let the harmfulness value of a security threat be h_i (i is the ID number of the security threat). Let the importance value of an IoT gateway be v_j (j is the ID number of the IoT gateway device). The danger value R_j of the IoT gateway and the danger value R of the global IoT are shown in Eq. (5) and (6), respectively:

$$R_j = 1 - \frac{1}{1+\ln\left(v_j \sum_{i=1}^{m} \left(h_i \left(Count\left(d_I.family = i \right) + Count\left(d_M.family = i \right) \right) \right) + 1 \right)} \quad (5)$$

where, m is the sum of the security threats confronted by the IoT gateway, $d_I \varepsilon D_I$, $d_M \varepsilon D_M$, d_I.family = d_M.family = i, the function Count()counts the sum of detectors according to the condition in accordance with its parameter:

$$R = \sum_{j=1}^{n} \left(\frac{v_j}{\sum_{i=1}^{n} v_i} * R_j \right) \quad (6)$$

where, n is the sum of all the IoT gateway devices

CONCLUSION

To resolve the problems confronted by the danger assessment technology for IoT, a theoretical Danger Assessment Model (DDAM) is explored in this paper. The principles and mechanisms of Artificial Immune System are introduced into the proposed model. The realization ways of IoT's security threat surveying, security threat intensity computing and quantitative danger assessment assessing are deduced with math methods. The mechanism of antibody density is simulated to reflect the intensity of security threats which are happening. Through the detected security threats and their intensity, the real-time and quantitative danger of IoT is assessed. The proposed model in this paper can provide accurate danger for IoT administrators and let them know the current security status of IoT clearly. It can help the active and positive security defense strategy for IoT be worked out. It is significative of theory and practice application value to have the initiative of the IoT security defense.

ACKNOWLEDGMENT

This study 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. 10ZC106) and the Scientific Research Fund of Leshan Normal University (No. Z1065).

REFERENCES

Chen, X.Z., Q.H. Zheng, X.H.G. Xiao and C.G. Lin, 2006. Quantitative hierarchical threat evaluation model for network security. J. Softw., 17(4): 885-897.

Dasgupta, D., 2002. An immunity-based technique to characterize intrusions in computer networks. IEEE T. Evolut. Comput., 6(3): 281-291.

Feng, D.G., Y. Zhang and Y.Q. Zhang, 2004. Survey of information security risk assessment. J. China Inst. Commun., 25(7): 10-18.

Hofmeyr, S.A., 1999. An immunological model of distributed detection and its application to computer security. Ph.D. Thesis, University of New Mexico.

ITU, 2005. ITU internet reports 2005: The internet of things. ITU, Geneva.

Jiao, L.C. and H.F. Du, 2003. Development and prospect of the artificial immune system. Acta Electron. Sinica, 31(10): 1540-1548.

Juels, A., 2006. RFID security and privacy: A research survey. IEEE J. Sel. Areas Comm., 24(2): 381-394.

Karygiannis, A., T. Phillips and A. Tsibertzopoulos, 2006. RFID security: A taxonomy of risk. Proceeding of the 1st IEEE International Conference on Communications and Networking in China (ChinaCom'06). Beijing, China, pp: 1-7.

Karygiannis, T., B. Eydt, G. Barber, L. Bunn and T. Phillips, 2007. Guidelines for Securing Radio Frequency Identification (RFID) Systems: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST). Technology Administration U.S. Department of Commerce, Special Publication 800-98.

Kavitha, T. and D. Sridharan, 2010. Security vulnerabilities in wireless sensor networks: A survey. J. Inform. Assur. Secur., 5: 31-44.

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

Li, T., 2004. Computer Immunology. Publishing House of Electronics Industry, Beijing.

Li, T., 2005. An immunity based network security risk estimation. Sci. China Ser. F. Inform. Sci., 48(5): 798-816.

Liu, Y.B. and W.P. Hu, 2010. Security model and key technology on Internet of Things. Digital Commun., 4: 28-33.

Mirowski, L. and J. Hartnett, 2007. Deckard: A system to detect change of RFID tag ownership. Int. J. Comput. Sci. Netw. Secur., 7(7): 89-98.

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

Oleshchuk, V., 2009. Internet of things and privacy preserving technologies. Proceeding of 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology. Aalborg, Denmark, pp: 336-340.

Padmavathi, G. and D. Shanmugapriya, 2009. A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. Inform. Secur., 4(1-2).

Wang, Y.F., T. Li, X.Q. Hu and C. Song, 2005. A real-time method of risk evaluation based on artificial immune system for network security. Acta Electron. Sinica, 33(5): 945-949.

Wei, Y., Y.F. Lian and D.G. Feng, 2009. A network security situational awareness model based on information fusion. J. Comput. Res. Dev., 46(3): 353-362.

Xiao, R.B. and L. Wang, 2002. Artificial immune system: Principle, models, analysis and perspectives. Chinese J. Comput., 25(12): 1281-1293.