ATLANTIS PRESS
Advances in Computer Science Research, volume 44
3rd International Conference on Wireless Communication and Sensor Network (WCSN 2016)

Perception and Response Model of Danger Signal Based on Immune Peril Principle

Min-Sheng Tan
[1] School of Computer Science and Technology, University of South China
Hengyang, Hunan, 421001, China
tanminsheng65@163.com

Zhi-Guo Zhao
School of Computer Science and Technology, University of South China
Hengyang, Hunan, 421001, China
545832754@qq.com

Chen-Cheng Wang
School of Computer Science and Technology, University of South China
Hengyang, Hunan, 421001, China
wangchencheng93@163.com

Ting Xiang
School of Computer Science and Technology, University of South China
Hengyang, Hunan, 421001, China
15096025554@163.com

Miao Guo
School of Computer Science and Technology, University of South China
Hengyang, Hunan, 421001, China
guomiao91@126.com

***Abstract*—Danger signal perception and response model of perception layer in IoT based on immune peril principle (DSPRM-IPP) and related algorithms were proposed. DSPRM-IPP model includes immunologic tolerance module, danger perception and accumulation module and response module. Immunologic tolerance module's duty is screening detector which is not matching with autologous collection at the beginning of the sensing layer node deployment, it also constantly adjust to the current detector according to the working environment in process of perception. Danger perception and accumulation module is responsible for the danger signal recognition and accumulation, and detector set generated by immunologic tolerance module is used to determine whether the current signal is danger signal or not. Appropriate response strategy will be taken according to the results of comparing potential cost and response cost in response module. The experimental results show that DSPRM-IPP effectively detects the danger with a low rate of false positives, it also has good adaptability that could adjust constantly according to the working environment and node proportion of residual energy.**

Keywords-Immune peril principle; Internet of Things perception layer; danger degrees of signal; perception, response

I. INTRODUCTION

The Internet of Things (IoT) mainly includes the perception, network and application layer. There are many nodes in perception layer, and the cost of a single node is generally low, so its computing power, storage capacity and energy supply are restricted. The perception layer has a high level of anti-tracking and confidentiality requirements. The perception layer is large scale, and need to maintain stability long-term; With the wide application of network technology, the security problem of perception layer emerges gradually. The perception layer often suffers attacks, such as Dos attacks, replay attacks, integrity attacks, impersonation attacks, Sinkhole attacks and so on. These attacks may control nodes in the perception layer and force it to run out of its own energy and even lead to physical damage [1-3].

Immune identification, immune memory, rapid response and diversifications [4] [5] are characteristics of the Biological Immune System (BIS). Professor Forrest [6] of Mexico University firstly introduced the Biological Immune System into the security area of the computer system, and put forward the Intrusion Detection Model and the Negative Selection Algorithm. Recognition or non recognition principle of the Negative Selection Algorithm can be applied to distinguishing information of itself from others. But it will spend the Negative Selection Algorithm much computing time and storage space on building huge self set and non self set, and the rate of missing or misleading report is unacceptable.

Matzinger [7] and Uwe Aickelin et al [8] made an important contribution to the Immune Response Mechanism. They established a computational model based on Immune Danger Theory, the main ideas of the computational model are listed as follows: (1) What the Immune System should distinguish is not the difference between itself or non itself, but the danger signals; (2) The immune cells in the immune system can send out danger signals to launch the immune response when they get damages or die unusually; (3) Cells in the immune system do not attack their host.

II. The Model of Danger Signal Perception and Response Based on the Immune Danger Theory

A. *The Basic Ideas of the Model*

According to the Immune Danger Theory, nodes of the perception layer, to a certain extent, will not give off danger signals until they are attacked. The releasing of danger signals indicates that these nodes detected outside invasion--Antigen. A moment generated danger value cannot be used to judge whether nodes are being attacked or not, because many reasons can result in moment generated danger value. Only the data transmission amount exceeds the warning value continuously, it is believed that the system is under attack. According to the above ideas, this paper gives the model of danger signal perception and response of IOT's perception layer based on the Immune Danger Theory (Fig. 1). The model mainly consists of the immunologic tolerance module, the danger signal perception and accumulation module and response module.

In the biological immune system, immunologic tolerance is a phenomenon that the system will not make response to its autologous antigen; it is also a normal physiological reaction that means immune competent cells will make no action when it is exposed to autologous antigen. Immunologic tolerance module picks out detectors that do not match the self set at the early deployment stage of the perception layer's nodes, and the current detectors should be adjusted to the working environment.

The model's core is the Danger Signal Perception and Accumulation module, which is mainly composed of two parts: the Danger Signal Perception and Danger signal Accumulation. If the collected, processed and forwarded data of the perception layer node in its process can be matched with the elements of the detector collection, the detector corresponding with this element will be activated. In the perceptual process, Immunologic Tolerance Module updates the current detector continuously according to the current working environment and danger accumulation, to ensure the validity of the detector, and saves valuable storage space of perception layer.

After detecting a danger, response module will make the appropriate treatment. After the alien attack last a period of time, the danger accumulation value is higher than the security threshold preset, and then appear the warning danger to response. If the danger value is lower than the security threshold, it indicates that the danger has been eliminated. Save the danger value and the response is to the end; if the danger value is still higher than the security threshold after a round of feedback, a further response should be made.

B. *Calculation of the Danger Signal's Danger Degree*

Classify the danger signal of IoT's perception layer; the greater the danger rank value indicates that the higher the degree of danger, danger level is used to calculate the danger signal accumulation. The attack danger grades of Dos, replay, integrity, impersonation, Sinkhole are 1, 2, 2, 3, 3 respectively.

If it is detected abnormality at the time of t+1, the danger degree of the node at this moment is:

$$x(t+1)=x(t)+\mu\times e^{-1.0/\theta} \tag{1}$$

$x(0)=0$, μ is the incentive factor, whose value refers to the danger grade of danger factors; the danger grade is used to indicate the risk level of the Internet perceived level for danger signals. θ is the danger signal at the initial time, its value is similar to μ. For some values of the discrete danger signal, numerical differentiation can be used to handle quantitatively for the discrete value. Formula (1) shows that, when the perception layer is attacked constantly, the danger signal produced by the detector trend to linear growth.

In contrast, between the T and $t+1$, no abnormality is detected, and then the danger degree of the node at $t+1$ is:

$$x(t+1)=x(t)\times e^{-y(t+1)} \tag{2}$$

$x(0)=0$, the expression $-y(t+1)$ refers to the danger degree of the corresponding danger factors, generally is the arithmetic sequence. Formula (2) shows that, when the sensing layer is no longer under attack, the detector detects no attack antigen at the moment, the accumulative value is reduced. If no attack antigen is detected during the continuous P (P is a positive integer) time periods, danger accumulation value is reduced continuously. If greater P and smaller danger value, it indicates the danger is decreasing. When $p\rightarrow l$, $x(t+1)\rightarrow 0$, this kind of danger will be cleared. The value of l refers to corresponding danger factors.

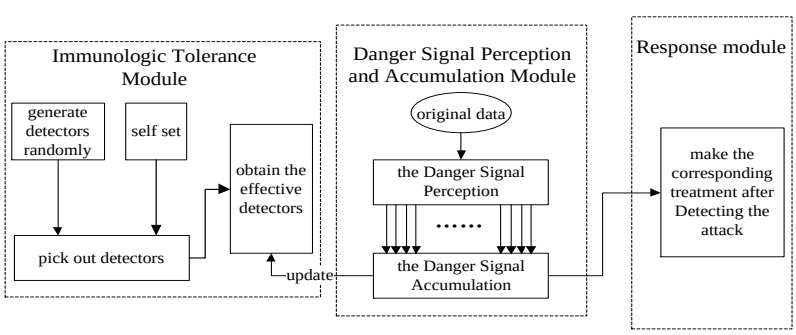

Figure 1. The danger signal perception and response model

C. Calculation of Response Cost and Loss Cost

The response cost is related with nodes' consumption rate of unit energy, nodes' sleeping time and the nodes' identity. The response cost at a moment is:

$$R\_Cost = \bar{v} \times m \times \omega \tag{3}$$

R_Cost is the response cost, $\bar{v}$ is the node's consumption rate of unit energy, m is the sleeping time of node, ω is the coefficient, ω's value depends on node's identity, if the node is a normal node, set $\omega = 1$; if the node is a special node, can set $\omega < 1$.

The loss cost is related with nodes' consumption rate of unit time, nodes' sleeping time and the nodes' proportion of residual energy during the accumulation of the danger. At a moment, response cost is:

$$P\_Cost = \bar{v}_o \times m \times \varphi \tag{4}$$

P_Cost is the loss cost, $\bar{v}_0$is nodes' consumption rate of unit time during the accumulation of the danger, m is the sleeping time of node, φ's value depends on the node's remain energy, the reference range of φ's value is (0.5, 2). The greater the node's proportion of residual energy is, the smaller φ's value is.

D. Core Algorithm

The Algorithm of Immunologic Tolerance. Node modules are in random tests of immunologic tolerance in the early deployment of filtering and collection matching in the effective detection devices. Considered that the node compute power, storage capacity and energy supply of the level of consciousness are restricted, the algorithm shouldn't be too complicated, the number of the stored effective detector can't be much, a single detector is not too big. Effective detectors are sensing nodes under attack (malicious and non-malicious attack) to measure changes in performance, through collecting the normal data of this period on this standard, from the analysis we get the conclusion. A kind of attack corresponds to a detector. according to pre-determined number of detectors at this stage you need to generate, when it build an efficient detector, the detector must be added to a pre-set collection , so this stage will generates a set of detectors eventually. In the danger signal sensing and accumulation phase, the detector based on changes in working conditions and danger accumulation to update, to ensure the effectiveness of detectors.

Danger Perception and Accumulative Algorithm. Consider of the characteristics of the Internet of Things perceived danger signal is discrete, the original data must be quantified before the test, after quantified, the data can be tested in the next step. When data collected at a certain time is match with the elements of the collection in the detectors, then the element corresponding to the detector will be activated. The activated detector is under the working condition, over the next period of time, it collect and activate the data of itself repeatedly, the collected data is used for accumulate, the method of calculating the danger accumulate reference to Formula (1). When accumulated danger is greater than the preset value, then we will think that the nodes have been attacked by outside way, issuing a danger alert and updating the corresponding detector. Accordingly, if this exception is only momentary, this part of information collected in the ensuing time period is normal, not match with collected elements of the detector, the cumulative danger would gradually reduce, the method of calculating the danger accumulate reference to Formula (2). When danger cumulative value falls below the minimum threshold, we can identify that the node is not affected by this type of attack, the detector was activated before will enter a dormant state, waiting for the next time to be activated. Form of algorithm description is as follows:

```
Input: raw data; Output: hazard
alerts
1. init();//Initialize
2. detectors[]←auto_tolerance
();//get detector set
3. quantize(date);//quantify the raw
data
4. If (has_danger (i))//detect an
exception
5. {wake_up(detectors[i]);//activate
the detector
6.  danger_values[i] ← 0;//danger
accumulation begins
7.  danger_values[i] ←
danger_accumulate(danger);}
8. while (true)
9. {if (has_danger (i));
10.  danger_values[i]←
danger_accumulate(danger,danger

_type,danger_values[i]);//calls
formula(1)
11. else danger_values[i]←
danger_reduce (danger_type,
      danger_values[i]); //call the
formula(2)
12. if (danger_values[i] <
safe_thresholds[i])
13.   sleep(detectors[i]);
14. if (danger_values[i] >
danger_thresholds[i])
15. {warn ();//danger is detected,
alerts
16.  Update (detectors[]);//Update
detector
17.  sleep(detectors[i]);
break;}}//end while
```

Active Response Algorithm. Exotic attack continued after a period of time, danger accumulation is higher than the safety valve set before, danger warning, start responding. Before carry on the specific responding actions,

according to the Formula (3) and Formula (4), we calculate the response costs (R_Cost) and penalty costs (P_Cost) separately, on the basis of this, compare R_Cost and P_Cost, if you R_Cost>P_Cost, no further response, accumulated danger value; otherwise, then further responses. After a round of response, calculating the danger value again, if danger value below safety valve, it showed that danger was relieved, save this danger value, then response terminated; if after a round of feedback, danger value still higher than safety valve value, it needs further of response, there has two kinds of practices: one is repeated the former round of response; the other is calculate R_Cost and P_Cost, And according to the relationship of the value of two costs to take further response. This article adopt the latter method, at the same time, in order to avoid an infinite loop, saving the valuable resources of the node, we take the former approach as a complement to the latter. Setting a limit of cycle time, if cycle times haven't reach the upper limit, we'll take the latter responds. After the cycle times reach the maximum limit, do the first response. Form of algorithm description is as follows:

```
Input: original data;Output: response
1. init ();//initialize
2. do_count ← 0;//danger
accumulation
3. danger_value ←
danger_accumulate(danger);
4. if (danger_value < danger_max);
5. goto step 3;
6. else  warning();//alert
7. r_cost ← r_cost();//call the
formula (3)
8. p_cost ← p_cost();//call the
formula (4)
9. if (r_cost < p_cost) goto step 2;
10.while (do_count <Number);//Number
is response cycles
11.{danger_value ← do();
12. do_count ++;
13. if danger_value >danger_max;
14. {if do_count < Number
15.   {end while;goto step 7;} //end
while of step 10
16.   else goto step 11;}
17. else end while;}//end while of
step 10
18.save(danger_value);
19.do_count ← 0; exit();//response
cycle reset to 0
```

III. Experiments and Results Analysis

A. Danger Signal Sensing Experiment

In order to validate the effectiveness of the model and algorithm proposed, regard single node in the IOT's sensing layer as the experimental object, to apperceive and response to Dos attack. To immunologic tolerance in the Initial deployment of node, generate effective detector. In the process of danger perception and accumulation, repeatedly test 100 times, and estimate the existence of alien attack by comparing danger accumulation and the relief value initially set. The total time is divided into 100 parts, according energy consumption of the node at the sampling time. To calculate the danger signal value, the normal environment's and suffered Dos attacks environment's results are shown in Table 1 and Table 2.

Table 2 show that, under the circumstances of suffering from DOS attack, using the model proposed in this paper can effectively detect the danger, and send out an alert; However, Table 1 show that in the case of no suffer from the attack, due to small changes in the environment and the increasing amount of data collected at the time, the energy consumption is slightly higher.

TABLE 1. VALUE OF DANGER ACCUMULATION UNDER NORMAL ENVIRONMENTAL

Time	Value of Danger Accumulation	Time	Value of Danger Accumulation
5	0.017671660	10	0.351170176
15	0.362711446	20	0.002443931
25	0.000016500	30	0.346440486
35	2.180672823	40	0.145225680
45	0.000978523	50	0.000065900
55	0.113424313	60	0.000764247
65	0.000005150	70	0.958915016
75	0.006461119	80	0.018163446
85	0.000122384	90	0.000000825
95	0.015180277	100	0.000102284

TABLE 2. VALUE OF DANGER ACCUMULATION UNDER DOS ATTACK

Time	Value of Danger Accumulation	Time	Value of Danger Accumulation
5	1.123328951	10	1.094477605
15	1.821867208	20	3.696965084
25	0.846384594	30	2.212977152
35	2.618527124	40	4.622481591
45	1.404495189	50	3.510856436
55	1.221063527	60	1.739441154
65	0.597933141	70	4.086109514
75	1.058085740	80	1.291265024
85	4.860370245	90	1.447800039
95	3.173275407	100	5.708903183

The rate of false positives under normal circumstances: 18 false positives appear in the negative selection model. The high rate of false positives indicates that the adaptability of the negative selection model is relatively poor. DSPRM-IPP model, when the danger threshold is set 1, under normal circumstances, 8 misstate appeared, and under attack environment, the alarm sounded firstly is the second time; When the danger threshold is set 2, under normal circumstances 1 false appeared, and under attack environment the alarm sounded firstly is the 16th time; When the danger threshold is set 4, under normal circumstances 0 false appeared, and under attack environment the alarm sounded firstly is the 21th time. The size of danger threshold represents the degree of tolerance

to danger. Lower danger threshold can detect danger quickly, but tends to increase the rate of false positives. While higher danger thresholds at the same time reduce the rate of false positives, reduces the speed of detection. Considering synthetically the rate of false positives and detection speed, 4 is more appropriate for the initial danger threshold.

B. *Active Response Experiment*

During the experiment, when the danger value reaches the danger threshold, the measures taken are to make nodes enter the sleeping state. During the node's sleeping, gradually reduce the danger value, but when the node enters working state at the end of node sleeping, still maintain a certain danger value, so that can quickly respond when the danger signal is detected next time. Assume that the initial energy of node is 10,000 units. Each transmission of information according to the amount of information consumes its energy proportionally. Assume that power consumption every information transmission is between 0 and 1 unit under normal conditions, the consumption of every information transmission power is between 0.6 and 1 unit under exceptional conditions. The experimental results are shown in Table 3.

From the Table 3, it can be found that, in the early nodes, the differences of energy consumption are small, but it becomes larger after the early stage. This phenomenon is caused by the relationship of nodes' safety threshold and the current nodes' remaining energy. The lower nodes' remaining energy have, the lower nodes' safety threshold be, and it can lead to security alarm for that the danger accumulation value easily exceeded the safety threshold. At this time, the nodes' energy is lower, too. The potential loss cost can be increased in order to prolong the nodes' life cycle, and it's bigger than the response cost when the response cost not changed. Considering the two aspects above, when the nodes come to the response time in the mid-last time, the longer the nodes' sleeping time is, the lower nodes' danger accumulation value can be, the longer nodes' life cycle could be, and the ratio of the sleeping time and working time will be bigger.

As the Dos attacks could reduce the nodes' life cycle, it needs to adapt the corresponding measures to prolong the life cycle when attacked and reduce the loss. But compared to the normal working conditions, the energy would consume faster when the nodes are attacked. Comparing with these results, it can be seen that when n=16, the nodes consume almost the same energy both in the normal environment and suffering from Dos attack. When n = 8, and n = 4, in the middle-last environment, the nodes' energy consumption is slower in normal environment than nodes suffering from Dos attack. While in the practical application, if some nodes' life cycle is focus considered, it need to set the nodes' parameters n to 16. If you pay attention to the life cycle, and to ensure the gathering information's high continuity and accuracy when nodes works, it can be set n as 8, and even 4. The setting of parameter n can be before or later the nodes' putted into application. In the nodes' working time, when nodes' residual energy is low, increase the value of n to extend the life cycle; or reduce the value of n which sacrifice part of life cycle to collect and forward information better.

IV. SUMMARY

In this paper, the Immune Danger Theory into the field of Internet of Things' induction layer to build a danger signal perception and response model (DSPRM-IPP model) was introduced. In this model, the perception of the main performance index in perception layer was extracted as danger signals, and determined whether the perception may face attack by those danger signals. When detected the danger, it can adapt the corresponding methods though the results of cost analysis, which can reduce the rate of false positives and increase the adaptability.

With the computing ability, storage capacity and the energy supply constraints of nodes in IOT's perception layer, the DSPRM-IPP model do not need to generate a large number of detector in advance, and small computation in working process. And it also can overcome the defect of larger storage space and larger computation in the traditional security model. Meanwhile, the danger signals were cumulatively quantified, promoted the danger perception from qualitative to quantitative, that improved the sensitivity and accuracy of the danger perception.

TABLE 3. COMPARISON OF NODE LIFETIME.

Energy	Time in normal	Time with Dos(n=24)	Time with Dos(n=16)	Time with Dos (n=8)	Time with Dos (n=4)
10000	0	0	0	0	0
9000	2013	1303	1333	1195	1193
8000	4035	2677	2623	2480	2419
7000	6068	4236	4041	3831	3677
6000	8017	5875	5634	5213	4961
5000	10043	8244	7494	6651	6316
4000	12075	10834	9543	8306	7751
3000	14563	14671	12196	10214	9339
2000	17802	20208	16078	12660	11212
1000	23344	28967	22259	16166	13671
0	35992	47995	35213	23061	17827

ACKNOWLEDGMENTS

This Research was supported by the National Natural Science Foundation of China under Grant 61403183, key Project of the Hunan Provincial Education Office Science Research of China under Grant 14A121, the Construct Program of the key Laboratory in University of South China (computer science and technology).

REFERENCES

[1] Rolf, H.: Internet of Things - Need for a New Legal Environment. J. Computer Law & Security Review. 25(4), 522-527 (2009)

[2] Liu, Y.B., Hu, W.P., Du, J.: Network Information Security Architecture Based on Internet of Things Technology Journal. J. ZTE Technology Journal. 17(1), 17-20 (2011)

[3] Xu, D.W., Cai, J.X.: The Internet of Things and Its Application Analysis. J. Computer Engineering and Application. 47(15), 229-231 (2011)

[4] Floerkemeier, C., Langh, E.M., Fleisch, E.: The Internet of Things. In: Proceedings of the First International Conference for Industry and Academia, pp. 49-52, 2008

[5] Li, T.: An Immunity Based Network Security Risk Estimation. J. Science in China Ser. F Information Science. 48, 557-578 (2005)

[6] Forrest, S., Perelson, A.S, Allen, L.: Self-Nonself Discrimination in a Computer. In: Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202-202, 1994

[7] Matzinger, P.: Tolerance, Danger, and the Extended Family. J. Annual Review of Immunology. 12(1), 991-1045 (1994)

[8] Lee, W.B, Tang, C.Y.: Inferring a Plausible Mouse Immune Response Network from Microarray Time Series Data. J. Journal of Computers (Taiwan). 21(4), 3-10 (2011)