Research Journal of Applied Sciences, Engineering and Technology 5(21): 4988-4993, 2013
DOI:10.19026/rjaset.5.4386
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2013 Maxwell Scientific Publication Corp.
Submitted: July 31, 2012 Accepted: September 17, 2012 Published: May 20, 2013

Research Article

ENSREdm: E-government Network Security Risk Evaluation Method Based on Danger Model

Xiaoting Jin
College of Public Administration, Henan University of
Economics and Law, Zhengzhou 450002, China

Abstract: In this study, we propose a danger model based security risk evaluation method to ensure the security of E-government networks. With the concepts and formal definitions of antigen, antibody, danger signal and detection lymphocyte presented, the architecture is given. Following that, the method of E-government network intrusion detection is described. And then, the security risk evaluation method is discussed. Theoretical analysis and experimental results show that the proposed method is valid. Thus, it provides a novel security guarantee solution to E-government networks.

Keywords: Danger model, e-government, risk evaluation

INTRODUCTION

Today, biological principle based methods have become an increasing popular computational intelligence paradigm in the field of information security (Sun, 2010). The problems of computer system are quite similar to those encountered in a Biological Immune System (BIS), since both of them have to maintain stability in a changing environment (Klarreich, 2002; Castro *et al.*, 2003). Inspired by the numerous desirable characteristics of the natural immune system, such as diversity, self tolerance, immune memory, distributed computation, self-organization, self-learning, self-adaptation and robustness, the BIS based Artificial Immune Systems (AIS) have become an increasing popular computational intelligence paradigm within information security (Sun *et al.*, 2008; Li, 2008; Sun and Zhang, 2009; Sun and Xu, 2009; Zhang *et al*., 2009).

The main task of traditional AIS based method for E-government network security based on antibody concentration (Sun and Wu, 2009) is to discriminate between self and non self and the central challenge of E-government network security is determining the difference between normal and harmful activities. However, it is difficult for AIS to distinguish accurately between self and non self and the size of self library and the time of self tolerance will grow exponentially with time goes by. Moreover, the phenomena of the natural immune system, such as the non self Intestinal Lactobacillus can live within human gastrointestinal, but there is no immune response to them, can't be explained by the AIS of Self-Non Self (SNS) discrimination.

In this study, we propose a danger model based security risk evaluation method to ensure the security of E-government networks. With the concepts and formal definitions of antigen, antibody, danger signal and detection lymphocyte presented, the architecture is given. Following that, the method of E-government network intrusion detection is described. And then, the security risk evaluation method is discussed. Theoretical analysis and experimental results show that the proposed method is valid. Thus, it provides a novel security guarantee solution to E-government networks.

DANGER MODEL

The danger model is presented and developed by Matzinger (1994), (2001), (2002), Aickelin and Cayzer (2002) and Timmis *et al.* (2003). Mat zinger states that adaptive immune systems can't distinguish self from non-self but danger signal; immune response will be triggered when danger signals are generated by damaged cells; the cells of the adaptive immune system in danger model are incapable of attacking their host. On the one hand, the immune response of danger model is as a reaction to a stimulus which the body considers harmful, but not the reaction to non-self. On the other hand, the foreign and immune cells of danger model are allowed to exist together and this point is reverse to the traditional AISs. Figure 1 shows the main principles of the danger model.

Figure 1 illustrates that cells distressed or died unnaturally may release an alarm signal which disperses to cover a small area around that cell, Antigen Presenting Cells (APCs) receiving this signal will become stimulated and in turn stimulate cells of the adaptive immune system. Within danger model, the foreign proteins in the injection are not harmful and so

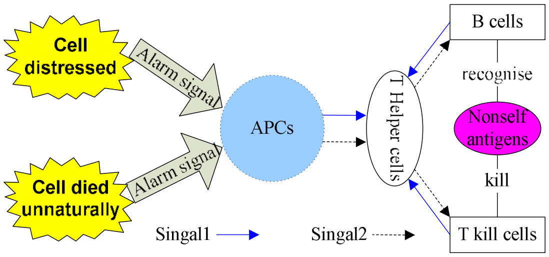

Fig. 1: Principles of danger model

are ignored, likewise tumor cell is not undergoing necrotic cell death and therefore not releasing alarm signals, hence there is no immune reaction occurred. Because of the danger signals only activate APCs; the B and T cells are stimulated into action according to Signal1 and Signal 2. Signal 1 is the binding of an immune cell to an antigenic pattern or an antigen fragment which is presented by an APC and Signal 2 is either a "help" signal given by a T-helper cell to activate a B-cell or a co-stimulation signal given by APC to activate T-cells.

With the danger model introduced, the danger theory inspired paradigms were proposed for data processing (Secker *et al.*, 2005), worm response and detection (Kim *et al.*, 2005), computer network intrusion detection (Zhang and Liang, 2008), network security threat awareness (Sun *et al.*, 2010a), network security monitoring (Sun *et al*., 2010b) and so on.

THEORETICAL MODEL

Within ENSREdm, it considers that the computer network attacks, which are dangerous, will induce the generation of danger signals by simulating cellular distress or cell unnatural death and the comparison between danger model and ENSREdm is illustrated in Table 1 (Sun, 2011).

Formal definitions: The state space of ENSREdm is defined with set S and $I \subset [0,1]^N$, where N represents the length of a E-government network packet. The antigen (ag) of ENSREdm is regarded as a presented Internet Protocol (IP) packet, which is consisted of the source IP address, destination IP address, source port number, destination port number, protocol type, IP flags, IP overall packet length and IP data. The antibody (ab) is used to recognize antigens. Obviously, the structure of ab is the same as that of ag. Non-self patterns (Non self) represent IP packets from network attacks and self patterns (Self) are normal network service transactions and non-malicious background clutters, where Nonself ∩ Self = ϕ.

Table 1: Comparison between danger model and ENSREdm

Danger model	ENSREdm
Cell distress or unnatural death	Net host paralysis or deny of service
Bacterium/virus	Computer network attacks
Danger signals	Abnormal parameters related with network activity
Danger area	Network space suffering attacks
Antigens	Presented IP packets
B cells	Mature detectors
T kill cells	Memory detectors
APCs	IP packets capture and analysis

Within E-government networks, all IP network packets are composed of the same segments. In point of this fact, the formal definitions of the sets of ag (S_{ag}) and ab (S_{ab}) of ENSREdm are respectively defined as follows:

$$S_{ag} = \begin{bmatrix} ag_{11} & ag_{12} & ag_{13} & \cdots & ag_{1n} \\ ag_{21} & ag_{22} & ag_{23} & \cdots & ag_{2n} \\ ag_{31} & ag_{32} & ag_{33} & \cdots & ag_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ag_{m1} & ag_{m2} & ag_{m3} & \cdots & ag_{mn} \end{bmatrix} \qquad (1)$$

$$S_{ab} = \begin{bmatrix} ab_{11} & ab_{12} & ab_{13} & \cdots & ab_{1n} \\ ab_{21} & ab_{22} & ab_{23} & \cdots & ab_{2n} \\ ab_{31} & ab_{32} & ab_{33} & \cdots & ab_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ab_{p1} & ab_{p2} & ab_{p3} & \cdots & ab_{pn} \end{bmatrix} \qquad (2)$$

In ENSREdm, each segment of *ab* and *ag* can be considered as a gene snippet. According to the principles of AIS, the antigen and antibody organization technique proposed in ENSREdm can fit E-government network well with reason. So, there exists $S_{ag} \subseteq I$, $S_{ab} \subseteq I$ and Nonself ∪ Self = S_{ag}.

In ENSREdm, the detection lymphocytes *is* used for network attacks detection and it is classified into immature, mature and memory detection lymphocyte. The mature detection lymphocyte is the detector that is tolerant to self but not activated by antigens. The memory detection lymphocyte evolves from a mature detection lymphocyte matched enough antigens in its lifecycle. While the immature ones are generated from the process of antigen depository or randomly generation. Let S_{imm}, S_{mat} and S_{mem} denote the set of immature detection lymphocytes, mature detection lymphocytes and memory detection lymphocytes, respectively. Therefore, $S_{imm} \cup S_{mat} \cup S_{mem} = S_{ab}$ and $S_{imm} \cap S_{mat} \cap S_{mem} = \Phi$.

Architecture of ENSREdm: According to the prevalent deployment of AIS, the architecture of ENSREdm is designed by distribution and it is mainly composed of sensors and a risk assessment center. The sensor of ENSREdm can be located in each E-government sub-network and it is in charge of the detection of network attacks. The functions of the risk assessment center include two aspects: bacterin distribution and network security risk evaluation through calculating danger degree.

Method of intrusion detection: In ENSREdm, the sensor, which can be located in each host or subnet work, is in charge of the network intrusion detection and it is realized by detection lymphocytes. To describe the intrusion detection methods of the mature and memory detection lymphocytes, formal definitions are defined as below.

Let d denote detection lymphocyte, a represent the age of d, n is the antigen number matched by d, s is the danger degree of network attacks which is detected by d and the intrusion detector set (S_{ab}) is defined as follows:

$$S_{ab} = \{\langle d, \alpha, n, s\rangle\} \mid d \in S \wedge \alpha, n \in N \wedge s \in [0, 1]\} \quad (3)$$

where, *N* represents the set of natural number.

For the convenience using the fields of a lymphocyte *x*, the operator "." is used to extract a specified field of *x*, where *x*. field name represents the value of field fieldname of *x*. According to the concepts of detection lymphocyte above, the formal definitions of the memory detection lymphocyte, mature detection lymphocyte and immature detection lymphocyte are described as below:

$$S_{mem} = \{a \mid a \in S_{ab}, \forall b \in Self(a.n \geq \beta \wedge match(a,b) = 1)\} \quad (4)$$

$$S_{mat} = \{a \mid a \in S_{ab}, \forall b \in Self(1 \leq a.n < \beta \wedge match(a,b) = 1)\} \quad (5)$$

$$S_{imm} = \{\alpha \mid \alpha \in S_{\alpha b} \wedge \alpha.n = 0 \wedge \alpha.s = 0\} \quad (6)$$

where, β denotes the activation threshold and match (*a*, *b*) is a matching function, which can be r-contiguous bits matching function, Hamming distance matching function and etc. In ENSREdm, the matching function is defined as in formula (7):

$$match(a,b) = \begin{cases} 1 & otherwise \\ 0 & \exists i, j(j - i \geq r \wedge (b_k = a.d_k, \\ & y \in S_{ag}, x \in S_{ab}, i \leq k \leq j)) \end{cases} \quad (7)$$

In ENSREdm, the mature detection lymphocyte simulates a B cell and the memory detector lymphocyte is mapping to a T kill cell. Moreover, the computer network attacks within E-government are detected by memory and mature detection lymphocytes through calculating the affinity between the antibody and the antigen.

The mature detection lymphocytes, which match enough antigens (β) in their lifecycle, will evolve into memory detection lymphocytes and this procedure is illustrated in formula (4). Formula (5) illustrates the generation method of mature detection lymphocytes which generate from immature detection lymphocytes. Please note that the immature detection lymphocyte who matches to any element in Self during the process of negative selection will be eliminated and those immature detection lymphocytes that pass through the negative selection will evolve into mature lymphocytes. The immature detection lymphocytes are generated from antigen depository or randomly generation, so they are described in formula (6).

For ∀ $d_m \in host_i.\ D_{mem} \cup host_i.\ D_{mat}$, if it detects a network attack (antigen) from time t to t + 1, $d_m.\alpha + 1 \rightarrow d_m.\alpha$ and $d_m.n + 1 \rightarrow d_m.\ n$. At the same time, the danger degree of d_m at time t + 1 is calculated by formula (8) and (9):

$$d_m.s\ (t+1) = \eta \times d_m.s\ (t) + \eta_0 \quad (8)$$

$$d_m.s(t) = \frac{d_m.cn(t) - d_m.cn(t-1)}{\Gamma} \quad (9)$$

where, η represents the encouragement factor which is used to monitor the continuous similar network attacks, η_0 denotes the initial danger degree and Γ represents the period from time t to t + 1.

Formula (8) and (9) shows that danger degree of the memory and mature detection lymphocyte will increase persistently with the enhancement of network attack intensity.

On the contrary, for ∀ $s_m \in host_i.S_{mem} \cup host_i\ S_{mat}$, if it doesn't detect any non-self antigen during the period of Γ (from time *t* to *t* + 1), s_m a will increase 1 if and only if s_m finishing one time antigen detection and s_m. s at time *t* + 1 is calculated by formula (10):

$$s_m.s\ (t + 1) = s_m.\ s\ (t) \times e\text{-}s_{m.}{}^{\alpha\ (t + 1)} \quad (10)$$

To simulate the danger signal of ENSREdm, it is defined that the danger signal of the *i*th host at time *t* can be calculated by summation. Let $V_{hosti.ds}$ denote the danger signal of $host_i$ and the calculation method of $V_{hosti.ds}$ (t) is defined by formula (11):

$$V_{host_i.ds}(t) = \sum_{j=1}^{N} x_j.ds(t) \quad (11)$$

where, *N* denotes the total lymphocytes' number of $host_i$ and $x_j \in host_i.\ S_{mem} \cup host_i.S_{mat}$.

Method of risk assessment: Because of the distributed architecture of the proposed model, the E-government network security risk assessment includes two parts. One is the host risk calculation which is realized by sensor and the other is completed by the risk assessment center. The detailed computation and assessment methods are described as follows.

There is a sensor in each network host, so the host risk can be calculated by the field of danger degree. In order to exponentially describe the security risk for $host_i$, let $host_i$.risk (t) denote the security risk of $host_i$.ds at time *t*, μ_j represent the damage weight, which denotes the danger degree of the j^{th} detection lymphocyte. The $host_i$.risk (t) is calculated by formula (12):

$$host_i.risk(t) = 1 - \frac{1}{1 + Ln(\sum_{j=1}^{n} \mu_j \times s_{m_j}.s(t))} \qquad (12)$$

where, n = $\|host_i.S_{mem} \cup host_i.S_{mat}\|$ and $\forall S_m \in host_i.S_{mem} \cup host_i.S_{mat}$.

In formula (12), $host_i$ risk (t) → 0 represents that $host_i$ has no danger at time *t* and $host_i$.risk (t) → 1 denotes the host $host_i$ is in extremely danger.

From the above, the algorithm for E-government Network Security Risk Evaluation (ENSRE) for $host_i$ at time *t* is described as follows:

Algorithm 1: ENSRE

```
Begin
  Loop: capture a network packet;
  Present ag;
  For each $d_m(d_m \in host_i.D_{mem} \cup host_i.D_{mat})$
     If (match ($d_m$, ag) = 1)
      {
       Compute $V_{hosti.ds}$ (t) ≥θ;
     If $V_{hosti.ds}$ (t) ≥θ then
      {
            Give an alarm;
            Goto Loop;
        }
      }
   Else
     Goto Loop;
End.
```

In ENSREdm, the whole network risk at time *t* is realized by the assessment center through averaging the risk of all the network hosts.

Theoretical analysis: In the abstract, ENSREdm is feasible and the theoretical analysis is given as follows.

Firstly, according to the formal definitions of S_{ab}, S_{mem} and S_{mat}, the artificial immune detection lymphocyte simulates the detection rule of the traditional network intrusion detection systems. So, network attacks can be detected in real-time; the more the lymphocyte, the more accurate the result.

Secondly, from the distributed framework of the proposed model and host-based deployment of sensors, it can be concluded that each host of the tested network can detect what "disease" it suffers (by checking the type of the artificial immune detection lymphocyte). Furthermore, by the risk assessment center of ENSREdm, network managers can know where the "disease" occurs (by checking the IP address of the host) and what the current "epidemics" are (by checking the maximal *n* of the detectors).

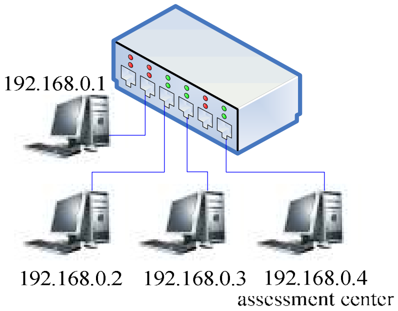

Fig. 2: Experiment topology structure

Finally, formula (8), (9), (10) and (11) illustrate that the danger signal of hosts is calculated quantitatively and the computation method is exponential. Equation (12) shows that when network attacks occur and the attack intensity increases, the danger signal also increases and follows the trend of the real attack intensity; as the real attack intensity decreases, the apperceived attack intensity decreases as well.

In a word, ENSREdm is feasible; not only can it find out where the most serious disastrous area is, but also it can apperceive the current situation of the local hosts and the whole network in quantification. Moreover, the higher attack frequency and intensity, the higher the danger signal and the situation awareness result of the network security is sensitive whether the "disease" is serious or not.

SIMULATION AND EXPERIMENTAL RESULTS

In order to verify the validity of ENSREdm, simulations were carried out and the topology structure is illustrated in Fig. 2.

In the experiments, the antigen is extracted from network packets, including destination IP, source IP, port number and protocol type. Therefore, the length of antigen is fixed. The match function used in ENSREdm was r-contiguous-bits matching rule and we defined *r* = 8. As limited by the size of our computer memory, computation speed and etc., the number of lymphocytes in ENSREdm was restrained, the proportional under 600 (theoretically, the more the lymphocytes, the more accurate the result).

Within the simulations, the values of activation threshold *β* were used as in the method of Forrest *et al.* (1997), where $\mu_j = \mu_k = 1$ (j ≠ k), $\eta = 1$, $\eta_0 = 0$. Within the experiments, the network intrusion of land, teardrop and smurf attacks were tested, there was one non-self packet among 20 packets and the network attacks were from 192.168.0.1 to 192.168.0.2 and 192.168.0.3. Partly experimental results are listed as follows.

The land attack intensity (packets per second) of the simulations was listed in Table 2 and the

Table 2: Land attack intensity (packets per second)

Time	1	2	3	4	5	6	7	8	9	10	11	12
Packets	111	121	134	118	141	149	123	136	144	152	161	162
Time	13	14	15	16	17	18	19	20	21	22	23	24
Packets	156	119	121	131	150	145	148	131	134	161	164	164
Time	25	26	27	28	29	30	31	32	33	34	35	36
Packets	155	143	153	159	133	154	141	149	132	135	161	168
Time	37	38	39	40	41	42	43	44	45	46	47	48
Packets	164	154	145	155	158	133	154	143	148	132	134	160
Time	49	50	51	52	53	54	55	56	57	58	59	60
Packets	167	165	156	145	152	158	133	155	143	148	131	133

Table 3: Teardrop attack intensity (packets per second)

Time	1	2	3	4	5	6	7	8	9	10	11	12
Packets	121	132	136	127	151	152	123	143	155	161	153	171
Time	13	14	15	16	17	18	19	20	21	22	23	24
Packets	164	123	130	123	171	163	156	141	147	171	162	171
Time	25	26	27	28	29	30	31	32	33	34	35	36
Packets	159	162	171	170	164	171	161	161	177	116	125	135
Time	37	38	39	40	41	42	43	44	45	46	47	48
Packets	116	121	128	165	161	118	123	127	143	147	141	159
Time	49	50	51	52	53	54	55	56	57	58	59	60
Packets	126	151	125	144	134	137	155	149	143	166	163	142

Table 4: Attack intensity (packet per minute)

Time	1	2	3	4	5	6	7	8	9	10	11	12
Packets	111	125	138	118	145	151	127	138	145	154	161	160
Time	13	14	15	16	17	18	19	20	21	22	23	24
Packets	155	117	121	134	154	143	149	132	134	161	167	165
Time	25	26	27	28	29	30	31	32	33	34	35	36
Packets	154	145	154	159	134	154	143	149	132	134	161	167
Time	37	38	39	40	41	42	43	44	45	46	47	48
Packets	165	154	145	154	159	134	154	143	149	132	134	161
Time	49	50	51	52	53	54	55	56	57	58	59	60
Packets	167	165	154	145	154	159	134	154	143	149	132	134

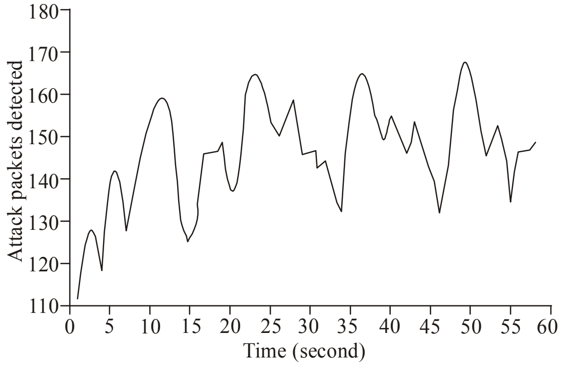

Fig. 3: Risk of land attack

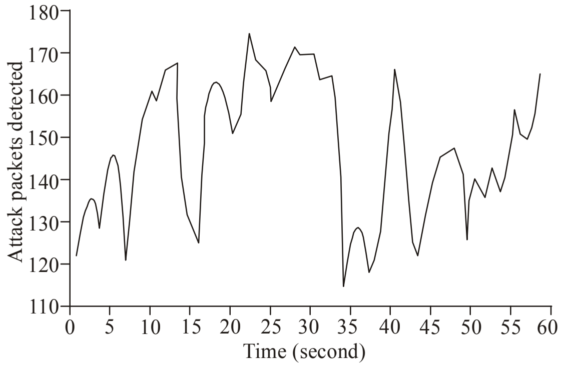

Fig. 4: Risk of teardrop attack

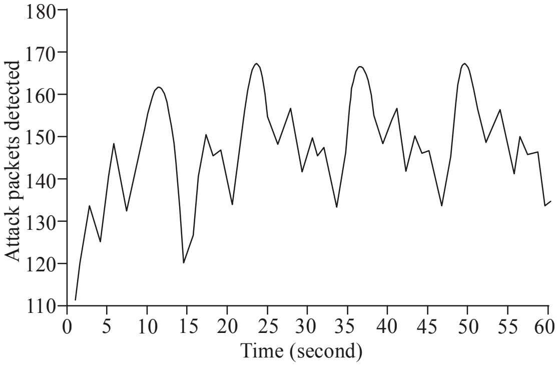

Fig. 5: Risk of smurf attack

experiment results apperceived by ENSREdm were illustrated in Fig. 3.

The teardrop attack intensity of the simulations was listed in Table 3 and the experiment results apperceived by the proposed method were illustrated in Fig. 4.

The smurf attack intensity (packets per second) of the simulations was listed in Table 4 and the experiment results apperceived by ENSREdm were illustrated in Fig. 5.

Theoretical analysis and the experimental results show that ENSREdm can aware security threats, which are caused by the network attacks, for E-government networks. Therefore, the proposed model is valid.

CONCLUSION AND RECOMMENDATIONS

This study proposes a danger model based method for E-government network security risk evaluation, which develops the concept of danger degree for network security risk evaluation, improves the formal definitions of the traditional immune detectors, describes the model architecture and gives the principles of network intrusion detection and security risk assessment. Theoretical analysis and experimental results that the proposed method is valid, it can evaluate the security risk for E-government networks, which is caused by network attacks. The higher attack frequency and intensity, the more dangerous the network faces. ENSREdm can detect what "disease" that E-government networks suffering, whether the "disease" is serious or not.

However, the current research of ENSREdm is mainly focus on network attacks frequency and intensity. In future work, the theory of ENSREdm should be perfected. Moreover, the activation threshold value (β), the matching function, encouragement factor value (η), the initial danger signal (η_0) and the damage weight (μ_i) should be tested in detailed.

ACKNOWLEDGMENT

This study was supported in part by a grant from Key Technologies R & D Program of Henan Province (No. 102102210509).

REFERENCES

Aickelin, U. and S. Cayzer, 2002. The danger theory and its application to artificial immune systems. Proceedings of the lst International Conference on Artificial Immune Systems (ICARIS), pp: 141-148.

Castro, L., N. De and J.I. Timmis, 2003. Artificial immune systems as a novel soft computing paradigm. Soft Comp., 7: 526-544.

Forrest, S., S. Hofmeyr and A. Somayaji, 1997. Computer immunology. Commun. ACM, 40: 88-96.

Kim, J., W. Wilson, U. Aickelin and J. McLeod, 2005. Coopera-tive automated worm response and detection immune algo-rithm (CARD INAL) inspired by T-cell immunity and tol-erance. Proceeding of the 3rd International Conference on Arti-ficial Immune Systems (ICARIS-2005), 3627: 168-181.

Klarreich, E., 2002. Inspired by immunity. Nature, 415: 468-470.

Li, T., 2008. Dynamic detection for computer virus based on immune system. Sci. China Series F Inform. Sci., 51: 1475-1486.

Matzinger, P., 1994. Tolerance, danger and the extended family. Ann. Rev. Immunol., 12: 991-1045.

Matzinger, P., 2001. The danger model in its historieal contex. Scandinavian J. Immunol., 54: 4-9.

Matzinger, P., 2002. The danger model: A renewed sense of self. Science, 12: 301-305.

Secker, A., A. Freitas and J. Timmis, 2005. Towards a danger theory inspired artificial immune system for Web mining. Web Mining: Applications and Techniques, pp 145-168.

Sun, F., 2010. Gene-certificate based model for user authentication and access control. WISM Proceedings of the International Conference on Web Information Systems and Mining, pp: 228-235.

Sun, F., 2011. Artificial immune danger theory based model for network security evaluation. J. Networks, 6(2): 255-272.

Sun, F. and S. Zhang, 2009. Immunity-inspired risk assessment approach for network security. Proceedings of the 2009 International Conference on Web Information Systems and Mining (WISM), pp: 515-518.

Sun, F. and F. Xu, 2009. Antibody concentration based method for network security situation awareness. Proceedings of the 3nd International Conference on Bioinformatics and Biomedical Engineering (ICBBE), 1: 1-4.

Sun, F. and Z. Wu, 2009. A new risk assessment model for e-Government network security based on antibody concentration. Proceedings of the International Conference on E-Learning, E-Business, Enterprise Information Systems and E-Government, pp: 119-121.

Sun, F., Q. Zheng and T. Li, 2008. Immunity-based dynamic anomaly detection method. Proceedings of the 2nd International Conference on Bioinformatics and Biomedical Engineering (iCBBE), 1: 644-647.

Sun, F., M. Kong and J. Wang, 2010a. An immune danger theory inspired model for network security threat awareness. Proceedings of the 2nd International Conference on Multimedia and Information Technology, 2: 93-95.

Sun, F., X. Han and J. Wang, 2010b. An immune danger theory inspired model for network security monitoring. Proceedings of the International Conference on Challenges in Environmental Science and Computer Engineering (CESCE 2010), 2: 33-35.

Timmis, J., P. Bentley and E. Hart, 2003. Improving SOSDM: inspirations from the danger theory. Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS), 2787: 194-203.

Zhang, J. and Y. Liang, 2008. A novel intrusion detection model based on danger theory. Proceeding of the IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, pp: 867-871.

Zhang, W., C. Wu and X. Liu, 2009. Construction and enumeration of boolean functions with maximum algebraic immunity. Sci. China, Series F Inform. Sci., 52: 32-40.