A Improved Network Security Situation Awareness Model

Fangwei Li
Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
lifw@cqupt.edu.cn
Jiang Zhu
Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
zhujiang@cqupt.edu.cn
Xinyue Zhang
Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
zhangxinyue159@163.com
Yan Wang
Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing, China
wangyan2250@sina.com

ABSTRACT
In order to reflect the situation of network security assessment performance fully and accurately, a new network security situation awareness model based on information fusion was proposed. Network security situation is the result of fusion three aspects evaluation. In terms of attack, to improve the accuracy of evaluation, a situation assessment method of DDoS attack based on the information of data packet was proposed. In terms of vulnerability, a improved Common Vulnerability Scoring System (CVSS) was raised and maked the assessment more comprehensive. In terms of node weights, the method of calculating the combined weights and optimizing the result by Sequence Quadratic Program (SQP) algorithm which reduced the uncertainty of fusion was raised. To verify the validity and necessity of the method, a testing platform was built and used to test through evaluating 2000 DAPRA data sets. Experiments show that the method can improve the accuracy of evaluation results.

Categories and Subject Descriptors
D.4.6 [Operating Systems]: Security and Protection; C.2.3 [Computer-Communication Networks]: Network Operations-Network monitoring

General Terms
Security

Keywords
DDoS evaluation, improved CVSS, combined weights, SQP, DAPRA2000.

1. INTRODUCTION
The current security technology is to consider network security from a single aspect and lack of awareness of the overall network situation, such as firewall, intrusion detection and vulnerability scanning. In this context, network security situation awareness is proposed and attracted much attention from researchers [1].

Network security situation awareness can access information in many aspects through related technology, obtain the whole network situation through quantification analysis, and forecast the future development trends based on the previous analysis. The concept of network security situation awareness was proposed, but the assessment framework was not realized [2]. In order to realize the framework, some methods were raised. The method of using multi agent anomaly detection and data flow analysis ignored the characteristics of the network itself [3]. The network security situation could be got when bayesian network was introduced to the evaluation, but the method cost high computational complexity and need huge training sample [4-5]. Analytic hierarchy process needs to set the relative weights which was subjective and relied on conventional wisdom and common sense [6-8]. The previous studies considered only the threat caused by attacks, ignored the situation changes caused by the network's own defects, reduced the accuracy of the whole situation assessment.

In order to reflect the situation of network security assessment performance fully and accurately, a new network security situation awareness model based on information fusion was proposed. This model has the following advantages. Firstly, the error evaluation of DDoS attacks is reduced. Secondly, the degree of accuracy is improved by increasing the assessment of vulnerability. Thirdly, the node weight of single one-sided is avoided through combining subjective weight and objective weight.

2. NETWORK SECURITY SITUATION AWARENESS MODEL BASED ON INFORMATION FUSION

2.1 The assessment framework
The following are three basic definitions in the model.

Definition 1. Threat($T(t)$): The extent of the damage caused by the different attacks on different nodes, mainly to explain the influence of external attacks on nodes' situation.

Definition 2. Vulnerability($V(t)$): The degree of vulnerability of host nodes, mainly to explain the effect of internal vulnerability on the nodes' situation.

Definition 3. Combined Weights(W): The weights have the advantage of objective weight and subjective weight, mainly to explain the nodes' important degree.

This model fuse the information of external attack threats, internal vulnerability and the nodes' important degree and obtain current network security situation.

MOBIMEDIA 2015, May 25-27, Chengdu, People's Republic of China

DOI 10.4108/icst.mobimedia.2015.259032

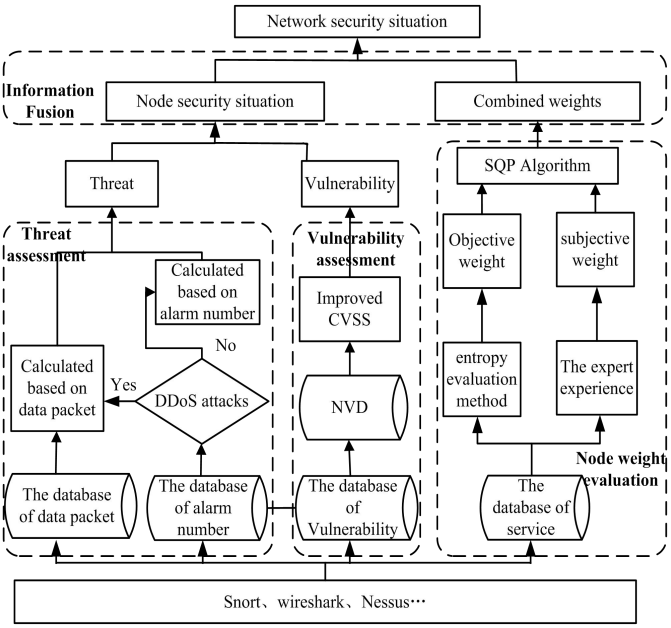

Figure 1: The model framework based on fusion information

2.2 The assessment of attacks

The original method relied on the alarm of IDS. The expression of the threat of attacks is given by [9] :

$$T_i(t) = f(c_i(t), d_i(t)) = c_i(t) \cdot 10^{d_i(t)} \tag{1}$$

where $c_i(t)$ is the amount of attacks, $d_i(t)$ is the threat level of attacks, $T_i(t)$ is the threat of attacks.

Most attacks can be evaluated by the above formula with the exception of DDoS attack. Firstly, the alarm number is very different based on different rule bases of IDS. Besides, DDoS attack is a repeated attack in a short period of time. There are so many same alarm at the same time that it is hard to differentiate between the same alarm and the repeated alarm.

The original method is irrelevant because of the above two reasons. Aiming at solving the problem, a new method of the assessment of DDoS attacks is proposed based on the characteristics of DDoS attacks and the information of data packet. The threat of DDoS attack is expressed as follows:

$$T_i(t) = f(p_i(t), a_i(t), \Delta t) = p_i(t) \cdot 10^{a_i(t)} \cdot \Delta t \tag{2}$$

where $p_i(t)$ is the range of attacks, it is the occupation ratio of attacked ports. $n_i(t)$ is the amount of attacked ports. The total of ports is 65536. The occupation ratio of attacked ports is defined as: $p_i(t) = n_i(t)/65536$.

where $a_i(t)$ is the strength of attacks, it is the average amount of data packet each attacked port. $b_i(t)$ is the total of data packet. The strength of attacks is defined as: $a_i(t) = b_i(t)/n_i(t)$.

where Δt is the duration of DDoS attack, it is the attack time from beginning to end.

2.3 The assessment of Vulnerability

The existing methods ignored the vulnerability of the node itself and got the situation only based on external attacks. The previous studies considered only the threat caused by attacks, ignored the situation changes caused by the Vulnerability, so the assessment of vulnerability is increased in this model. In order to reflect the fully and accurately, CVSS is adopted [10].

Firstly, the vulnerabilities are discovered by vulnerability scanners like Nessus. Next, The vulnerabilities are related to National Vulnerability Database and quantified form six aspects which are attack avenue, attack complexity, authentication, confidentiality, availability and integrity. In order to emphasize vulnerabilities that are exploited, the activating factor is identified and added to CVSS and reflects the different vulnerability in different period of time. The assessment of vulnerability is given by:

$$\begin{aligned} V_{ik}(t) &= \delta_{ik}(t) \times (0.6 \times M_k + 0.4 \times BE_k - 1.5) \times f(M_k) \times \beta_{ik}(t) \\ \text{where} \quad M_k &= 10.41 \times (1 - (1 - C_k) \times (1 - I_k) \times (1 - A_k)) \\ BE_k &= 20 \times AV_k \times AC_k \times Au_k \\ f(M_k) &= \begin{cases} 0, & M_k = 0 \\ 1.176, & M_k \neq 0 \end{cases} \end{aligned} \tag{3}$$

where $\delta_{ik}(t)$ is equal to 1 if the node i contains the vulnerability k , otherwise 0.

where $\beta_{ik}(t)$ is equal to 1 if the vulnerability k of the node i is exploited, otherwise 0.7. The value can be adjusted based on specific condition of the network and the administrator's needs.

where M_k is the value that the vulnerability k affects security situation. C_k、I_k、A_k are the value of confidentiality, integrity and availability.

where BE_k is the value of the vulnerability k 's the utilizability. AV_k、AC_k、Au_k are the value of attack avenue, attack complexity, authentication.

2.4 The assessment of nodes' weight

The weight reflects the importance of the node, the larger the weight is, the more effect security situation has. If the weight is unreasonable, the whole assessment of security situation will be meaningless.

The current method of determining weight are subjective weighting and objective weighting. The subjective weighting can reflect the people's intention, but the weight is more subjective. The objective weighting is determined based on objective data, but the weight has no participation of people and the weight and the importance of node may be opposite. In order to obtain the reasonable weight, this paper combines the two weights and the combined weight represents the importance of node.

2.4.1 The object weight

The object weight is determined based on the improved entropy evaluation method [10]. In information theory, entropy reflects the degree of disorder information and is a measure of uncertainty. The smaller entropy means the bigger certainty and the more information and more importance of the index. The process of the improved entropy evaluation method is:

a) Establish judgment matrix based on service

$$R = (r_{ij})_{n \times m}, (i = 1, 2, \ldots, n; j = 1, 2, \ldots, m) \tag{4}$$

where r_{ij} is the value of the service, if the node i has the service j , the value is 1, otherwise 0. n is the total of the

node, m is the total of the service.

b) Calculate the entropy of the service j

$$H_j = -(\sum_{i=1}^{n} f_{ij} \ln f_{ij}) / \ln n \tag{5}$$

where f_{ij} is the service j 's weight of the node i and $f_{ij} = r_{ij} / \sum_{i=1}^{n} r_{ij}$. If the value of f_{ij} is 0, $\ln f_{ij}$ is meaningless. f_{ij} is redefined as:

$$f_{ij} = (1 + r_{ij}) / \sum_{i=1}^{n} (1 + r_{ij}) \tag{6}$$

c) Calculate the variation coefficients of the service j

$$g_j = 1 - H_j / m - E_e$$
$$where \quad E_e = \sum_{j=1}^{m} H_j, 0 \le g_i \le 1, \sum_{j=1}^{m} g_i = 1 \tag{7}$$

where g_j is the variation coefficients of the service j , the larger the value is , the more effect the node has.

d) Calculate the object weight

$$w_{1i} = \sum_{j=1}^{m} (g_j \Big/ \sum_{j=1}^{m} g_j) \cdot f_{ij} \tag{8}$$

2.4.2 The subject weight

The subject weight is determined based on the experts' experience [8]. The weight depends on the number and the importance of the service. The subject weight is given by:

$$w_{2i} = \sum_{j=1}^{m} v_{ij} \Big/ \sum_{i=1}^{n} \sum_{j=1}^{m} v_{ij} \tag{9}$$

where w_{2i} is the subject weight , v_{ij} is the importance of the node i 's the service j .

2.4.3 The combined weight

In order to make the weight more reasonable, the object weight and the subject weight are fused. The combined weight can not only reflect the intention of people but also be more objective.

In order to consider the advantages of the subject weight and the object weight, the concept of weighted euclidean distance is proposed. The weight is optimal when the sum of euclidean distance is the minimum. Firstly, the different nodes' euclidean distance of the subject weight and the object weight is calculated. Then, in order to avoid the preference, this paper uses the combined weight itself instead of the constant weight. The method makes the weight adaptive. The formula of the combined weight is defined as:

$$\min F = \sum_{i=1}^{n} w_i \sqrt{(w_i - w_{i1})^2 + (w_i - w_{i2})^2} \tag{10}$$

The solution of the formula(10) can be described as the solution of the nonlinear quadratic programming. The nonlinear quadratic programming is described as:

$$\begin{cases} \min \quad \sum_{i=1}^{n} w_i \sqrt{(w_i - w_{i1})^2 + (w_i - w_{i2})^2} \\ s.t. \quad \sum_{i=1}^{n} w_i = 1 \\ \qquad \min(w_{1i}, w_{2i}) \le w_i \le \max(w_{1i}, w_{2i}) \end{cases} \tag{11}$$

The optimal solution can be got based on the SQP. The SQP is one of the best algorithm that solves the nonlinear quadratic programming. The SQP can guarantee the global convergence that is superlinear convergence. Figure 2 is the flowchart of SQP.

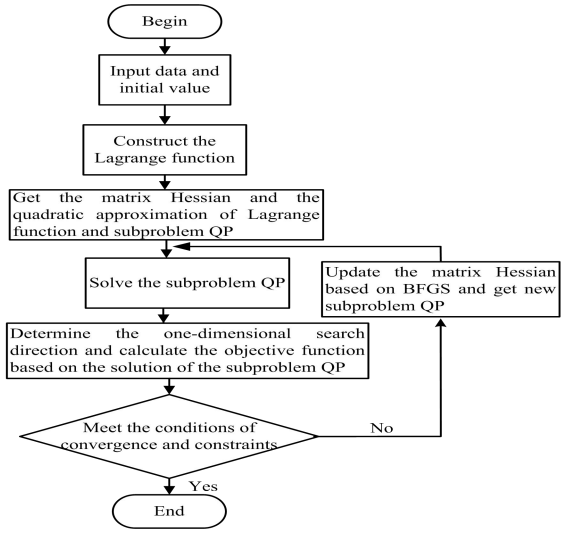

Figure 2: The flowchart of SQP

2.5 The information fusion

The node and network security situation are calculated by fusing the threat, the vulnerability and the weight.

Definition 4. The node security situation: The extent of the influence caused by the external attacks and the internal vulnerability on the nodes' situation. The node security situation is expressed as follows:

$$NA_i(t) = f(T_i(t), V_{ik}(t)) = \sum_{k=1}^{l} T_i(t) \cdot log_2 V_{ik}(t) \tag{12}$$

where $T_i(t)$ and $V_{ik}(t)$ represent the threat and the vulnerability. l is the total of the node's vulnerability. $NA_i(t)$ is the value of the node security situation.

Definition 5. The network security situation: The extent of the influence caused by the whole nodes' security situation based on the weight. The network security situation is defined as:

$$SA(t) = f(NA_i(t), w_i) = \sum_{i=1}^{n} w_i \cdot NA_i(t) \tag{13}$$

3. EXPERIMENT RESULTS ANALYSIS A-ND COMPARISON

This experiment selected the scenario one of the data sets DARPA 2000 from MIT Lincoln Laboratory[12]. The scenario has five steps of attack. Figure 3 is the network topology.

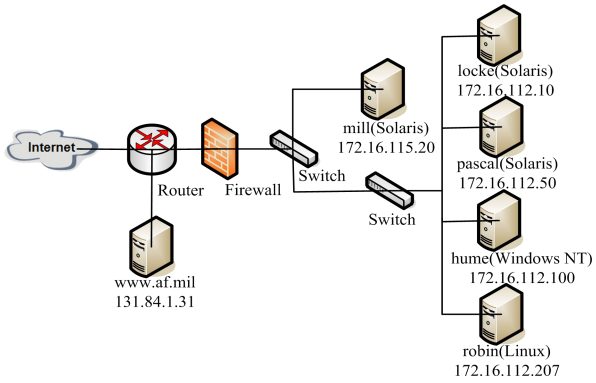

Figure 3: the network topology

3.1 The experiment 1

In order to prove the unstability of the assessment of DDoS attack based on the attack alarm, this experiment was designed. Firstly, the intrusion detection system was constructed. Secondly, the data packet was detected by the different rule database. Lastly, the result was imported into the MySQL. Table 1 is the statistical result.

Table 1: the number of alarm based on different rule in different period

the number of alarm / the period / rule	1	2	3	4	5
Rule database 1	40	79	42	8	266
Rule database 2	40	77	50	8	4
Rule database 3	40	72	35	11	1404

Table 1 shows that the number of alarm caused by the attack which is not DDoS is approximately equal. The original method is still valid except DDoS. In the fifth period, the number of alarm caused by DDoS is completely different. The original method no longer applies to DDoS.

3.2 The experiment 2

3.2.1 The threat of DDoS

This method is proposed based on the characteristics of DDoS and the analysis of data packet by wireshark. The threat of DDoS is calculated by the formula (2).

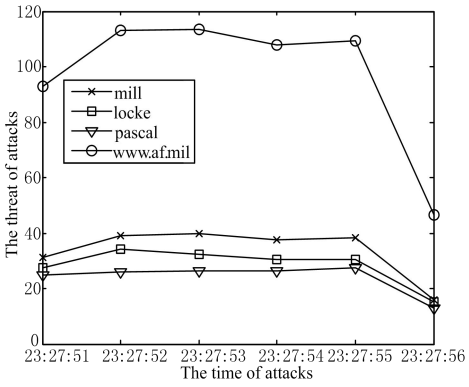

Figure 4: the threat of the different host in fifth period

Figure 4 shows that the value of the server www.af.mil's threat is largest. The server www.af.mil is attacked and the host mill, locke and pascal are controlled remotely. The obtained results were consistent with actual condition. Figure 5 indicates the threat is completely different because of different rules. The proposed method based on data packet is stable and effective and reflects the threat of DDoS objectively.

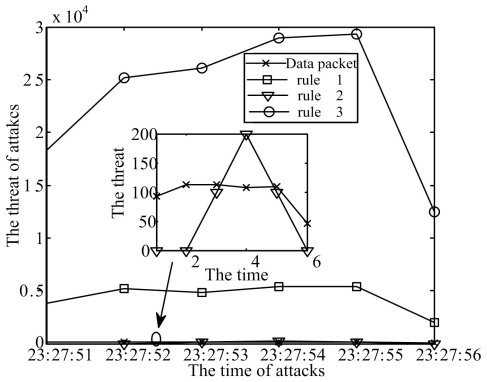

Figure 5: the network threat based on different source

3.2.2 The network security situation

The threat is calculated by the formula (1) and (2). The threat level of attacks are divided into three degrees. The value of the high, middle and low levels of attacks are 1, 2 and 3.

Figure 6 shows that the threat of mill, pascal, locke are biggest in the third period because these hosts' permissions of root are obtained by hackers and controlled remotely. The threat of the server www.af.mil increases rapidly because of the attack of DDoS. When the permission of root is obtained, the administrator should be as soon as possible to repair in order to avoid more damage.

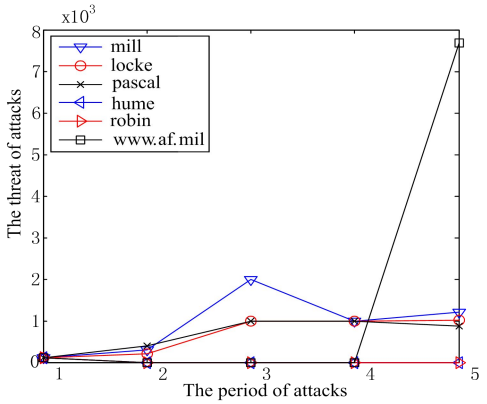

Figure 6: The threat of hosts in different period

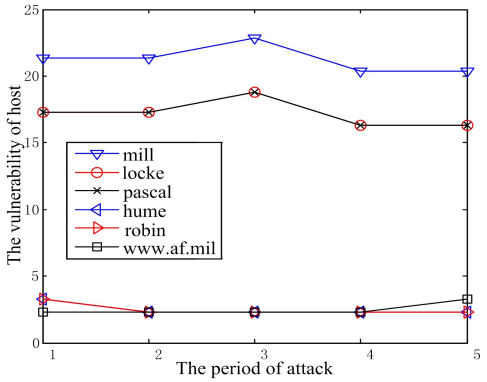

Figure 7: The vulnerability of hosts in different period

According to the score of vulnerability by NVD, Figure 7 is the vulnerability of hosts based on the improved CVSS. As can be seen from the figure, the vulnerability of the host mill is largest, followed by locke and pascal. The vulnerability of these host are large and the vulnerability are exploited by attacks. The administrator should be as soon as possible to patch the code.

According to the information of services, the nodes' importance is evaluated by the entropy evaluation and the expert experience. The combined weight is optimized based on SQP algorithm.

Table 2: the process of the optimization

iterations	function($x10^{-2}$)	iterations	function($x10^{-2}$)
0	5.814086	6	5.302910
1	5.444816	7	5.302879
2	5.431330	8	5.302878
3	5.416835	9	5.302877
4	5.371880	10	5.302877
5	5.329074	11	5.302877

Table 2 shows that the value of the objective function is steady and minimum after the ninth iteration. The optimal weight is [0.2240 0.2147 0.2147 0.1469 0.0999 0.0999].The combined weight takes advantage of the subject weight and object weight. The sum of weighted euclidean distance is minimum.

The threat, vulnerability and combined weight are fused based on the formula (14) and (15). Figure 8 is the result of the fusion.

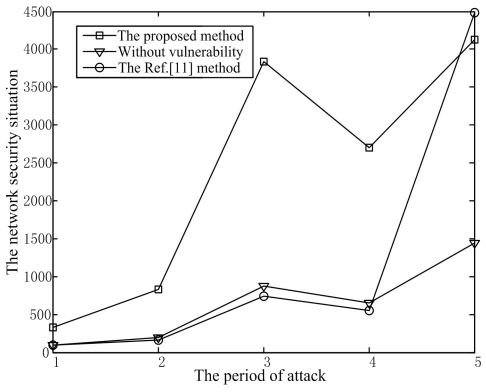

Figure 8: Comparison of the network security situation

As can be seen from the Figure 8, the value of the network security situation is low caused by network-scan attack in the first and second period. In the third period, the value increased rapidly because these hosts' permissions of root are obtained by hackers and controlled remotely. The network is in danger and a lot of attacks will follow. The administrator should be as soon as possible to repair and patch the code in order to avoid more damage. The value is generally low and can't reflect the potential danger without the assessment of vulnerability. In fifth period, the value of situation caused by DDoS is too high and exaggerates the threat of DDoS based on the method [10]. Because it is difficult to distinguish the repeat alarm and the real alarm.

Experimental results show that the proposed model and quantization is reasonable and necessary. The assessment of DDoS is more accurate because it is independent of alarm. The result of the assessment is more comprehensive with vulnerability. The combined weight is more reasonable and takes advantage of the subject and the object.

4. CONCLUSION

The threat of attacks, the vulnerability and the importance of nodes are evaluated effectively by the proposed model. The network security situation is obtained reasonably by the fusion of the above three aspects. The change of the situation can be observed visually. The administrator can know the dynamic of the network security situation and the caused could be established and corrected. In future work, the more comprehensive index and quantitative method will be researched. And in this basis, we will study how to forecast the network security situation.

5. ACKNOWLEDGEMENT

This research was supported by the National Nature Science Foundation of China (NO.61271260, No.61301122) and the Scien ce and Technology Research Project of Chongqing Education Co mmission (No.KJ120530).

6. REFERENCES

[1] X.ZHENHUA. Demand-oriented traffic measuring method for network security situation assessment. Journal of Networks, 9(4), 221-224, 2014.

[2] B.Tim. Intrusion systems and multi-sensor data fusion: creating cyberspace situational awareness. Communications of the ACM, 43(4):99-105, 2000.

[3] V.Gorodetsky, O.Karsaev, V.Samoilov. On-line update of situation assessment based on asynchronous data streams. Knowledge-Based Intelligent Information and Engineering Systems. Berlin/Heidelberg: Springer, pages 1136-1142, 2004.

[4] M.Frigault, L.Y.Wang, A.Singhal, S.Jajodia. Measuring network security using dynamic Bayesian network. In Proceedings of the 4th ACM workshop on Quality of protection, pages 23-30, 2008.

[5] L.J.Wang, B.Wang, Y.J.Peng. Research the information security risk assessment technique based on Bayesian network. The 3rd International Conference on Advanced Computer Theory and Engineering, vol 3, pages 600-604, 2010.

[6] X.H.Ji, C.Pattinson. AHP implemented security assessment and security weight verification. IEEE International Conference on Social Computing, pages 1026-1031, 2010.

[7] X.Z.Chen, Q.H.Zheng, X.H.Guan. Quantitative hierarchical threat evaluation model for network security. Journal of Software, 17(4):885-897, 2006

[8] Q.X.Liu, C.B.Zhang, Y.Q.Zhang. Research on key technology of vulnerability threat classification. Journal on Communications ,33(Z1):79-86, 2012.

[9] Y.Fu, X.P.Wu, Q.Ye. Approach for information systems security situation evaluation using improved FAHP and Bayesian network. Journal on Communications, 30(9):135-140, 2009.

[10] W.Hu J.H.Li. Improved Design of the Scalable Network Security Situation Model. Journal of University of Electronic Science and Technology of China, 38(1):113-116, 2008.

[11] C.Li, B.J.Zhao. X.L.Shen. Network security situational awareness method of multi-period assessment. Journal of Computer Applications,33(12):3506-3510, 2013.

[12] MIT Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific data sets. [2014-12-20]. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/2000data.html