The Building of Network Security Situation Evaluation and Prediction Model based on Grey Theory

Jianfeng Dong
Campus Network Management Office, Party Propaganda Department
Zhejiang Education Institute
Hangzhou, China

***Abstract*—Network security situation evaluation and prediction is a new technology to monitor network security, and it is one of hot research domains in information security. The research situation of network security situation evaluation and prediction all over the world is analyzed. A network security situation evaluation and prediction model based on grey theory is presented. The model is divided into two stages: current network security situation evaluation modeling and future network security situation prediction modeling. The model of current network security situation evaluation using simple additive weight method is established by the threat of various services attacked. The model of future network security situation prediction adopting grey theory is built by past and current network security situation.**

***Keywords*- Network Security; Prediction Model; Grey Theory**

I. INTRODUCTION

Presently, studies of network security situation awareness model are mostly focusing on framework models, such as the multi-sensor data fusion framework model suggested by Tim Bass[1], network security situation awareness framework model based on Net flow suggested by Xiaoxin Yin et al[2], and distributed framework model for network security situation awareness suggested by Stephen G. Batsell[3]. But there hasn't a precise mathematic model. On the basis of grasping research situation and function requirements related to network security situation awareness, the paper tries to give a network security situation awareness model, which is based on simple additive weight and grey theory, to solve the measurement problem of the model.

The remainder of this paper is organized as follows. Section 2, we put forward the conceptual model of network security situation awareness, and establish the model of current network security situation evaluation and future network security situation prediction. Section 3 provides simulation test. And it end with a conclusion in section 4.

II. NETWORK SECURITY SITUATION AWARENESS MODEL

Network security situation awareness model is the research basis in network security situation awareness. Through building this model, we can measure the relationships among system components and that between the components and environments.

A. A Conceptual Model

Based on analyzing research situation related to network security situation awareness in and abroad, combining analysis of classic models of situation awareness in other domains like JDL functional model[4] and situation awareness mental model proposed by Endsley[5], we give a conceptual model of network security situation awareness. In Fig. 1, the model consists of three levels; from bottom to top are network security situation perception, situation evaluation, and situation prediction.

Level 1. Situation perception is the basis of situation awareness.. This level mainly adopts mature technologies to perceive network security situation information from mass data, translates them into understandable formats (such as XML), and prepares for situation evaluation.

Level 2. Situation evaluation is the core of situation awareness, and it is also a dynamic comprehension process of current security situation. It represents security situation of the whole network by recognizing security events, ensuring relationships among events, and generating security situation maps from threats faced.

Level 3. Situation prediction is to judge what the future security tendency is, according to the past network security situation and current network security situation. This will help decision-makers know network security situation in a higher level, and supply evidences for reasonable and precise decisions.

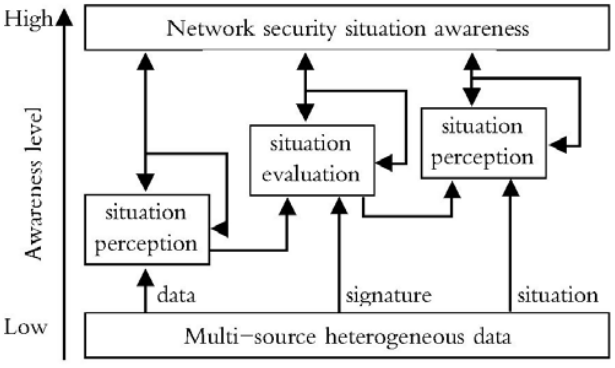

Figure 1. The conceptual model of network security situation awareness

978-0-7695-3972-0/10 $26.00 © 2010 IEEE
DOI 10.1109/CESCE.2010.271

B. Situation Evaluation Modeling

The model of situation evaluation is built according to services that network system supplies and threats that services are faced.

Assumption 1. During time t (after balancing capabilities of system processing, in order to maintain real time, *t* should be as small as possible), *S* presents n services $S_i (1 \le i \le n)$ that target network supplies. *A* presents the set how much weight the service S_i is. $\beta_i (1 \le i \le n)$ presents the weight of services S_i, and it is under control of administrators. *C* presents the number of attacks every service faced, and m kinds of attacks that services S_i faced can be presented as $C_{ij} (1 \le j \le m)$. *N* presents the attack times that a service is suffered, and then *N*. means the attack times of *C*, that S_i suffered. *T* is the set that threats equals *T*. in C_i, and its value depends on attacks.

Definition 1. According to Assumption 1, function F_{cs}(*S, A, C, N, T*) is current security situation of target network and its value equals formula (1).

$$F(S, A, C, N, T) = \sum_{i=1}^{n} \beta_i (\sum_{j=1}^{m} 10^{T_{ij}} C_{ij}) \tag{1}$$

In formula (1), $(1 \le i \le n)$, $(1 \le j \le m)$. We use $10^{T_{ij}}$ to measure the threats, because $10^{T_{ij}}$ can present threat degrees of network security situation effectively. The F_{cs}(*S, A, C, N, T*) bigger, the threats target network faced more dangerous.

C. Situation Prediction Modeling

On the basis of evaluating current security situation, aiming at the fuzzy, random and uncertainty of future situation, it is suggested to build the predicting model of network security situation based on grey theory. The theory is suitable for building the prediction model and can ensure precision of the model.

Grey theory [6] is first conducted by Deng Julong in 1982 in China, and is used to predict from small-scaled, uncertain data. The research target of the theory is the indeterminable, poor-informational system, which means the system information is partly known and partly unknown. In grey theory, the most widely used grey model is GM(1, 1) as following:

$$x^{(0)}(t) + az^{(1)}(t) = b \tag{2}$$

In formula (2), -*a* means the development coefficient, while *b* means grey input. Commonly, when $|a| < 2$, GM (1, 1) works, and the forecasting result changes with different value of a.

Assumption 2. During time t (as small as possible), an abnormal security sequence chosen from situation database, which is used as input data sequence of the prediction model of network security situation, is marked as $X^{(0)} = (x^{(0)}(1), x^{(0)}(2),..., x^{(0)}(n))$, and $x^{(0)} \ge (t)$, $t = 1,2,..., n$.

From formula (1), the whitenization equation and discrete response function of formula (2) are listed below:

$$\frac{dx^{(1)}}{dt} + ax^{(1)} = b \tag{3}$$

$$\hat{x}^{(1)}(t) = (x^{(0)}(1) - \frac{b}{a})e^{-a(t-1)} + \frac{b}{a} \tag{4}$$

$t = 1,2,..., n$. After building the model, error check should be done as follow.

The simulation value of $X^{(1)}$ that is written as $\hat{X}^{(1)}$ can be computed according to formula (4). And then the simulation value of original data that is written as $\hat{X}^{(0)}$ can be computed according to formula (5).

$$\hat{x}^{(0)}(t) = \hat{x}^{(1)}(t) - \hat{x}^{(1)}(t-1) \tag{5}$$

And residual value $\varepsilon(t)$ can be computed according to formula (6).

$$\varepsilon(t) = x^{(0)}(t) - \hat{x}^{(0)}(t) \tag{6}$$

So, the relative error Δ_t, and the average relative error Δ can be got from formula (7) and (8), and be listed.

$$\Delta_t = \frac{|\varepsilon(t)|}{x^{(0)}(t)} \times 100\% \tag{7}$$

$$\Delta = \frac{1}{n-1} \sum_{i=2}^{n} \Delta_t \times 100\% \tag{8}$$

From analysis of grey theory above, it is known that the steps to build the prediction model of network security situation awareness are:

1. Get $X^{(1)}$ from original input data from Assumption 2.It is easy to do this from 1-AGO; 2. Get $Z^{(1)}$, the mean generation of consecutive neighbors sequence, from $X^{(l)}$; 3. On the basis of first two steps, get development coefficient -a and grey input b from Theorem 1; 4. Put a and b into formula (3) and (4), then the network security situation prediction model is built; 5. According to formula (5) to (8), the network security situation prediction model performs error check.

III. SIMULATION TEST

The model is tested under the platform of Redhat Linux 9.0/P4 3.0/1024M/160G. This platform is equipped with Huawei 5000 multilayer route switch, IDS, Firewall and 6 PCs. And configurations of every PC are Redhat Linux 9.0/P4 3.0/512M/80G, with IG Ethernet.

Table. Shows services status during 14pm and 19pm in May 15th, 2006. The whole time is divided into 5 time sectors, T_1, T_2, T_3, T_4, T_5, and each equals 1 hour.

TABLE I. THE STATUS OF SERVICES RUNNING

Time	Table Column Head	j	n
T_1	{FTP,RPC,SCOKET}	{0.335,0.375,0.29}	3
T_2	{FTP,RPC,DNS,SCOKET,HTTP}	{0.265,0.282,0.103,0.295,0.155}	5
T_3	{FTP,RPC,SCOKET,TELNET}	{0.192,0.391,0.306,0.111}	4
T_4	{FTP,RPC}	{0.564,0.436}	2
T_5	{FTP,RPC,SCOKET,HTTP}	{0.079,0.295,0.237,0.389}	4

TABLE II. THE TIMES AND THREAT OF SERVICES ATTACK

Service / Time	FTP	RPC	DNS	SOCKET	HTTP	TELNET
T_1	{1(2) }	{1(3) }	—	{1(5)}	—	—
T_2	{1(1) }	{2(2) }	{2(2)}	1(1)	0	—
T_3	{2(2),1(2) }	{1(1) }	—	{2(1)}	—	{2(2)}
T_4	{2(1),1(6) }	{1(1) }	—	—	—	—
T_5	{3(1),1(3) }	{1(4) }	—	0	{1(2 }	—

A. *Maintaining the Integrity of the Specifications*

T_{ij} in formula (1) commonly has five kinds, which is Discovery, Scan, Escalation, Denial-of-Service and Stealth. Here we references user's handbook of Snort [7] and defines kinds of attacks with its threat degrees (3 means high, 2 means medium and 1 means low). It is shown in Table.2.

TABLE III. THREAT DEGREE AND ATTACK SORT

Threat Degree	Kinds of attacks
High (3)	Shellcode-detect
	Attempted-admin
Medium (2)	RPC-portmap-decode
	Attempted-Dos
Low (1)	Network-scan
	Misc-activity

During sectors of every T. (i=1,2,3,4,5) , some hacker tools such as DNS zone transfer, Buffer Overflow and Synflood are used for testing. According to the statistics of IDS and Firewall, comparing with Table 2, threat degrees of every sector are listed in Table.3. Symbol " " means that this service is out of running. "0" means that the corresponding service is out of attacks. While {Threat degree (Times of attacks)} means the times of different attacks.

The status of network security situation awareness of T_1, T_2, T_3, T_4 and T_5 is computed with formula (1) and shown in Table.4.

TABLE IV. SECURITY SITUATION IN T_i

T_1	T_2	T_3	T_4	T_5
32.45	83.2	98.95	94.6	100.95

Supposed that it takes network security situation information in T_1, T_2, T_3, T_4 and T_5 as original input data of the prediction model, the whitenization equation and discrete response function are easy to be got with formula (3) and (4).

$$\frac{dt^{(1)}}{dt} - 0.0508x^{(1)} = 83.5026$$

$$\hat{x}^{(1)}(t+1) = 16.77.5792e^{0.0508t} - 1645.1292$$

And from the above model, the value of network security situation in T6 can be computed as 107.0105.

Table.5 shows the error check, including original data of network security situation $x^{(0)}(t)$, simulation value of network security situation $\hat{x}^{(0)}(t)$, residual value ε_t and relative value Δ_t in T_i (i=2,3,4,5)

The average relative error that can be computed according to formula (8) is 3.7675%. Namely, the prediction precision of network security situation awareness model is higher than 96%.

TABLE V. ERROR CHECK

Time	T_2	T_3	T_4	T_5
T_1	83.2	87.3477	-4.1477	4.985%
T_2	98.95	91.8957	7.0543	7.129%
T_3	94.6	96.6805	-2.0805	2.199%
T_4	100.95	101.7145	-0.7645	0.757%

IV. CONCLUSIONS

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

REFERENCES

[1] T. Bass, Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness, Communications of the ACM, 2000, 43(4), pp.99-105.

[2] Xiaoxin Yin, William Yurcik, and Adam Slagell, The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness, The third IEEE International Workshop on Information Assurance (IWIA), 2005, pp.141-153.

[3] Stephen G.Batsell, Nageswara S.Rao, and Mallikarjun Shankar, Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security, http://www.ioc.oml.gov/projects/ documents /containment.pdf, 2005.

[4] AN Steinberg, CL Bowman, and FE White, Revisions to the JDL Data Fusion Model, Proceedings of SPIE AeroSense, Orlando, Florida, USA. 1999, pp.430-441.

[5] Mica R.Endsley, Toward a theory of situation awareness in dynamic systems, Human Factors, 1995, 37(1), pp.32-64.

[6] DENG Ju-long, Grey Forecast and Grey Decision, Wuhan:Huazhong University of Science and Technology Press,2002.

[7] Martin Roesch, Chris Green, Snort Users Manual, http://www.snort.org/docs/ snortmanja.pdf,2006.