Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (16): 3285-3289, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.3285.3289

Research on the Network Security Situation Awareness Model for the Electric Power Industry Internal and Boundary Network

Guo Xiaoli and Wang Hui
Department of Information Engineering, North East Dianli University (NEDU), 132012, China

Abstract: Due to the most majority of communication network of electric power industry used Strong logic isolation to ensure network security, so the network security has its own particularity. This study proposed an object-oriented vulnerability model, which using the D-S evidence theory to complete information fusion and in the view of vulnerability-service-host-network to build up network security situation assessment based on the analysis characteristics of the Intranet and boundary network. The method matches the private network special features to the hilt compared with other methods. Experimental results show that the method provids good support for the electric power network security situation assessment and improve the accuracy of the evaluation effectively.

Key words: Electric power industry, information fusion, nssa, internal and boundary network

INTRODUCTION

In recent years, electric power industry informatization construction progress is rapid with the construction of smart grid. Whether, it is a power generation enterprise or the grid company, enterprise internal network and various types of information application system construction has been gradually improved, however with the increasing demand of users, the electric power system information network application is more and more widely, its scale is more and more huge, its structure is more and more complex, the safety problem is becoming more and more serious. Hu *et al*. (2009) especially the combined attack, distributed attack and attack from intranet put forward a serious challenge for network security management within the electricity. Many security tools meet some security requirements, such as IDS, Firewall, Honey pot and so on but there are still some problems, such as network security deployment repeated, Protection loopholes and a lack of coordination solve the problem of composite attack ability, etc. The traditional single defense and detection equipment has been unable to meet the demand of electric power information network security (Jiang *et al*., 2010; Kong and Li, 2008; Li *et al*., 2010; Liu *et al*., 2008).

Network Security Situation Awareness (NSSA) can consider all sides of safety factors, reflect the dynamic status of network security as a whole, provide the base data to forecast the development trend of network security situation, provide reliable reference to enhance network security. Therefore, the research of security situation evaluate mode for the power industry intranet and boundary network is a significant element in the construction of smart grid (Liu *et al*., 2012). In recent years, researchers domestic and overseas, depending on different kinds of technical ideas, designs and implements a large number of computer network security situation evaluate methods.

The project group SIFT developed NVisionIP and VisFlow Connect two visual tools. NVisionIP can display a class B network status and to provide a precision of 3 different view; VisFlow Connect can dynamically display the connection status of the network and network traffic and has the ability of data filtering but the tool only reflects the network connection status, evaluation index is relatively single and meanwhile the administrator need very high level of experience (Liu *et al*., 2008).

Bass T proposed Distributed intrusion detection system based on sensor data fusion to evaluate computer network security situation, it use data fusion and data mining methods to assess the security of the computer network but absence of specific prototype system.

Gorodetsky proposed a security situation assessment method based on asynchronous data flow network, multi agent network data stream anomaly detection and analysis, to obtain the security situation but this method only consider the attack information while ignoring the characteristics of Internet itself.

Zhang Haixia and others proposed a network security analysis model based on the increasing attack ability, using the attack ability to grow an attacker's ultimate goal makes the attack graph more accurate, this study analyzed

Corresponding Author: Guo Xiaoli, Department of Information Engineering, North East Dianli University (NEDU), 132012, China

the attack path and also conducted the network safety analysis (Zhang *et al*., 2012). Due to the problems existing in the existing research this study puts forward the electric power industry internal and boundary network security situation awareness model based on information fusion, fusion different safety partition information of electric power industry internal and boundary network using D-S evidence theory, the model has better precision compared to the general network security situation evaluate method, can effectively improve the level of safety management in electric power industry intranet. avoid omissions and misstatements greatly.

NETWORK SECURITY SITUATION AWARENESS

Model based on information fusion: Compared with other enterprises, the security problem of electric power industry is mainly due to the vulnerability of the services provided by the servers, hosts or network. According to the characteristic feature of electric power industry internal and boundary network, this study uses vulnerability as evaluation object, sets up a hierarchical network security situation awareness model as Fig. 1. This model divides NSSA into three levels, to be named as data level, evaluation level and presentation level. The previous two complete acquisition data, information fusion, situation evaluate, respectively (Liu *et al*., 2009; Wei and Lian, 2009). The presentation level from the view of Vulnerability-Services-Host-Network to evaluate network situation for visual display.

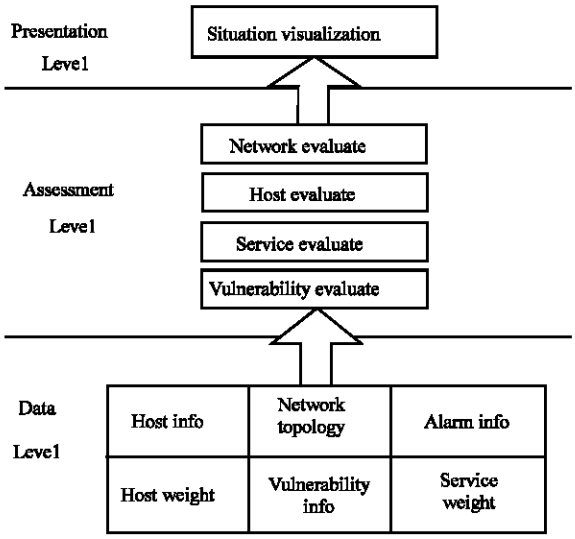

Fig. 1: Electric power industry security situation awareness model

The first level is the data level. Data is the basic of information fusion and situation evaluate, its quality different partition network information.

The second level is the evaluate level. At first using D-S evidence theory to complete the fusion of network directly affects the accuracy of evaluation. Because of electric power industry network structure scale, partitioning isolation and the important data distributed storage, its data acquisition is more difficult (Zhang and Yun, 2012). Thus in data level, using different access methods, such as special agent interface, obtain information processing, get the vulnerability evaluate results. Secondly, considering the host services and its corresponding vulnerabilities, to obtain service evaluation result by summation method. Then considering the services in this host and its weights, using weighted method to get the host evaluate results. Finally considering all host's weight, using weighted sum method to get the network security evaluate results.

The third level is the presentation level. According to the history of the results of situation awareness, using graphics and image technology, to show the network security situation analysis results by statistical graphs, reports, network attack topology and other means in the form of visual presentation to the users, to enhancing the practicability of the system.

SECURITY SITUATION EVALUATE ALGORITHM BASED ON INFORMATION FUSION

Basic concept of d-s evidence theory: D-S evidence theory was first proposed by Dempster in 1967 and developed by his student Shafer in 1976, it's an inexact reasoning theory mainly used for dealing with uncertainty problems, also been known as the Dempster-Shafer Evidence Theory. In D-S evidence theory, the most basic concept is to create a frame of discernment. Let U be the set domains of all values of X and all elements in U are mutually incompatible, U is called the frame of discernment of X.

Defined function m: $2^U \rightarrow [0, 1]$ to be Basic Probability Assignment Function (BPAF) and if it meets conditions as flow:

$$\begin{cases} m(\varnothing) = 0 \\ 0 \le m(A) \le 1 \\ \sum_{A \subset U} m(A) = 1 \end{cases} \quad (1)$$

Regard m (A) as the BPAF of A.

Defined function $2^U \rightarrow [0, 1]$ to be the basic probability assignment on U.

Defined function Bel: $2^U \rightarrow [0, 1]$ as:

$$Bel(A) = \sum_{B \subset A} m(B)(\forall A \subset U)$$

and call this function the belief functions of U.

Fusion rules of D-S evidence theory: Let Bel_1 and Bel_2 to be the belief functions in the same frame of discernment in U, m_1 and m_2 are the basic probability assignment function, focal element is respectively A_1, A_2, L, A_k and B_1, B_2, L, B_r. Let:

$$K = \sum_{\substack{i,j \\ A_i \cap B_j = C}} m_1(A_i) m_2(B_j) < 1$$

Then:

$$m(C) = \begin{cases} \dfrac{\sum_{\substack{i,j \\ A_i \cap B_j = C}} m_1(A_i) m_2(B_j)}{1 - K}, \forall C \subset U, C \neq \varnothing \\ 0, C \neq \varnothing \end{cases} \quad (2)$$

In the above formula, if $K \neq 1$, then m determines a basic probability assignment. If K = 1, that m_1 and m_2 contradiction, can not fusion the basic probability assignment. The above fusion rules for Information between the two only in the face of multiple sensor fusion improvements are as follows:

$$m(C) = \begin{cases} \dfrac{\sum_{\cap A_i = C} \prod_{n=1} m_n(A_i)}{1 - \sum_{\cap A_i = \varnothing} \prod_{n=1} m_n(A_i)}, \forall C \subset U, C \neq \varnothing \\ 0, C \neq \varnothing \end{cases} \quad (3)$$

Security situation evaluate algorithm: This study uses vulnerabilities score announced by CNVD and IDS alarm statistics as evidence, from the view of Vulnerability-Services-Host-Network evaluate the entire network security situation. Using the D-S evidence theory to fusion network vulnerability information to gain the vulnerability situation value, then considering the host existing services and service weight to gain service security and host security situation value, according to the host security situation value and weight gain network security situation value. Algorithm flow as Fig. 2 below.

Security situation evaluate algorithm flow: The network existences host H_n (1 = n = host number in network), H_i existences vulnerability L_i, normalized vulnerability

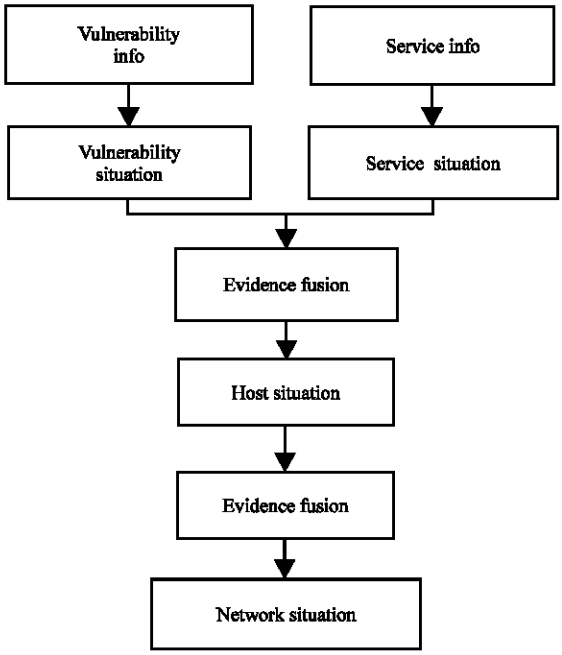

Fig. 2: Scheme of security situation evaluate algorithm

information of H_i. Find the vulnerability severity score from vulnerability database, using the Eq. 4 to get the vulnerabilities of evidence:

$$E_{L_i} = \frac{EE_i}{180} \times 100\% \quad (4)$$

where, E_L (0 = E_L = 1) stands for the vulnerabilities of evidence, EE_i (1 = EE_i = 180) stands for vulnerability severity score.

Get alarm statistics evidence from statistical information in the database and named as A_{li}. NA_i is defned as the number of alarm produced by L_i on H_i in unit time.NA_a stands for in unit time all alarm number in H_i.

Defining the identification frame $\theta = \{h, \bar{h}\}$, h stands for computer safe in L_i, stands for computer unsafe in L_i. In this study, using the improved D-S evidence theory method to synthesize the multiple correlation detection equipment related network data, get the corresponding basic probability assignment function as follows:

$$\begin{cases} m_1(h) = 1 - A_{L_i} \\ m_1(\bar{h}) = A_{L_i} \\ m_2(h) = 1 - E_{L_i} \\ m_2(\bar{h}) = E_{L_i} \end{cases} \quad (5)$$

After the evidence synthesis, m (α) calculation equation:

$$m(\bar{h}) = \frac{\alpha}{1+2\alpha-\gamma} \quad (6)$$

In the equation of α and γ, respectively, $(A_{Li} \bullet E_{Li})$ and $(A_{Li} + E_{li})$. It was evident that the larger m $(\bar{h})$ values, the less system secure, vulnerability E_{Vi} situation value should be higher. The situation value of vulnerability L_i can directly use m $(\bar{h})$ to obtain:

$$S_{L_i} = m(\bar{h}) \times 100\% \quad (7)$$

For any service Ser_i in the host H_i, can obtain the security situation value S_{seri}:

$$S_{Ser_i} = \sum_{L_i \in Ser_i} S_{L_i} \quad (8)$$

$L_i \in Ser_i$ stands for vulnerability in service Ser_i.

Utilize security situation value of services Ser_i can get H_i security situation value:

$$S_{H_i} = \sum_{Ser_i \in H_i} w_{Ser_i} S_{Ser_i} \quad (9)$$

$Ser_i \in H_i$ stands for service in H_i, w_{Seri} stands for weights of service Ser_i.

Eventually can get network security situation value S:

$$S = \sum_{H_i \in N} w_{H_i} S_{H_i} \quad (10)$$

$H_i \in N$stands for the host in network, w_{Hi} stands for weight of host H_i.

According to the weight information of the host node service information and service, can use Eq. 11 calculation the host node weight:

$$w_{H_i} = \sum_{i=1}^{m} w_{Ser_i} \quad (11)$$

where, m stands for the service number provided by the host nodes, w_{Seri} stands for weight of each service .The result of all the service weights addition is 1, if there a re several host to provide the same service, so the service weights will be evenly distributed to the host, the result of host node weights addition is also 1.

Simulation experiment: In order to verify the model and the algorithm applicability, we select a electric power company internal network operation data in the year 2011 as the experimental data.

Table 1: Network vulnerability information in network

Vulnerability information	Host 1	Host 2	Host 3	Host 4	Host 5	Host 6
ICMP Incorrectly configured	2	1	1	3	1	2
SunRPC incorrectly	0	1	2	0	0	0
Sadmind buffer overflow	2	0	1	0	0	0
RCP Incorrectly configured	3	1	1	3	0	0
Host Info query Incorrectly configured	1	4	0	0	0	0

Table 2: Network service information in network

Service information	Host 1	Host 2	Host 3	Host 4	Host 5	Host 6
HTTP	×	√	√	×	√	√
FTP TEL	√	√	√	×	×	×
NET	√	√	√	×	×	×
DNS	√	×	×	×	×	×
SMTP	×	×	×	√	×	×
POP3	×	×	×	√	×	×

Table 3: Host weights

Host	1	2	3	4	5	6
Weight	0.21	0.21	0.27	0.22	0.04	0.05

Table 4: Service weight

Service	Weight
HTTP	0.3
FTP	0.2
TELNET	0.2
DNS	0.1
SMTP	0.1
POP3	0.1

The data mainly is network vulnerability data gained through the network vulnerability scanner and deployment event collectors in the major equipment such as server, terminal host. In the experimental data chooses 10 consecutive time slot (each time slot 30 seconds) as the evaluation data, analysis to get vulnerability information of each host, as shown in Table 1. Service information list in Table 2.

The weight of hosts and services has been respectively obtained, as shown in Table 3 and 4.

According to the vulnerabilities reports reported by CNVD, assignment value for each vulnerability severity, through the situation evaluate algorithm described by the second section, obtained each time slot the host security situation as shown in Table 5:

Finally calculating to obtain the network security situation curve, as shown in Fig. 3. The horizontal axis is the time slot, for a period of time, the longitudinal axis is the network security situation value. The higher the situation value indicates that the network security situation is more serious.

Table 5: Host security situation

Time slot	Host 1	Host 2	Host 3	Host 4	Host 5	Host 6	Security security situation
1	0.0367	0.04	0.0367	0.04	00	0.0343	
2	0.0459	0.05	0.0459	0.00	0	0	0.0329
3	0.5	0.5	0.50	00.00	0.35		
4	0.20.175	0.18340	0	0.00	0.1325		
5	0.4	0.35	0.3668	0.00	0	0.4	0.2850
6	0.0734	0	0	0.00	0	0	0.0249
7	0.5	0	0	0.00	0	0	0.1700
8	0.2	0	0	0.00	0	0	0.0680
9	0	0	0.6125	0.00	0	0	0.1155
10	0.4	0	0.3668	0.00	0	0.4	0.2220

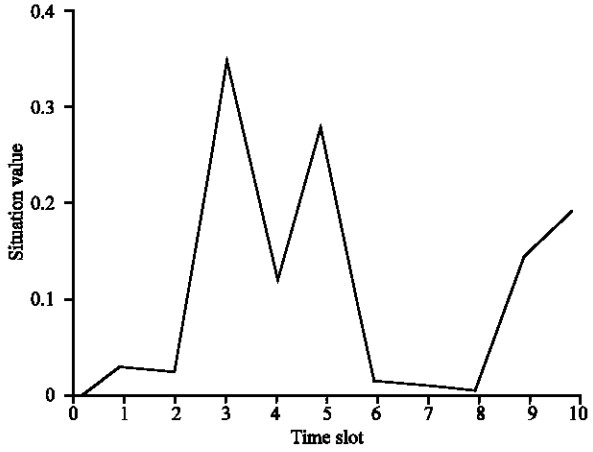

Fig. 3: Curve of network security situation

CONCLUSION

Based on the analysis of problem the present situation of electric power network security management faced, this study proposes a electric power industry intranet security situation evaluate model based on information fusion, this model synthetically considers multiple security divisions information, using D-S evidence theory to obtain the network security situation evaluate results, evaluation from the view of Vulnerability-Services-Host-Network. Simulation experimental results show that compared with the traditional single sensor network security situation assessment, this method has higher accuracy and credibility. However, the power network security situation evaluate model and quantitative evaluation method still need to study and improve, the attack information and the vulnerability information still need to find more visually.

REFERENCES

Hu, W., J.H. Li, X.Z. Chen and X.H. Jiang, 2009. Improved design of the scalable network security situation model. J. Univ. Electr. Sci. Technol. China, 38: 113-116.

Jiang, W., A. Zhang and Y. Deng, 2010. A novel information fusion method based on our evidence conflict representation. J. Northwestern Polytechn. Univ., 28: 27-32.

Kong, J. and W. Li, 2008. Evidence theory information fusion method based on fuzzy set. Comput. Eng. Appl., 44: 152-154.

Li, S., X. Dai and Y. Zhou, 2010. Research progress of network security situation awareness. Appl. Res. Comput., 27: 3227-3232.

Liu, X., H. Wang, J. Yu and B. Cao, 2012. Network security situation awareness model based on multi-source fusion. J. PLA Univ. Sci. Technol., 13: 403-407.

Liu, X., H. Wang, Y. Liang and J. Lai, 2008. Network security situation awareness model based on heterogeneous multi-sensor fusion. Comput. Sci., 35: 69-73.

Liu, X., J. Yu and M.L. Wang, 2009. Network security situation generation and evaluation based on heterogeneous sensor fusion. Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, September, 24-26, 2009, Beijing, China, pp: 4173-4867.

Wei, Y. and Y. Lian, 2009. A network security situational awareness model based on log audit and performance correction. Chin. J. Comput., 32: 763-772.

Zhang, X., B. Wang and X. Cheng, 2012. A hierarchical network security situational awareness model based on information fusion. Network Secur. Technol. Appl., 9: 72-74.

Zhang, Y.Z. and X.C. Yun, 2012. Network operation security index classification model with multidimensional attributes. Chin. J. Comput., 35: 1666-1674.