Network Security Situation Awareness Based on the Optimized Dynamic Wavelet Neural Network

Huang Cong[1] and Wang Chao[2]
(Corresponding author: Wang Chao)

China Tobacco Guangxi Industry Co., Ltd, China[1]
No. 28 Research Institute, China Electronics Technology Group Corporation, China[2]
No. 1, Alfalfa East Street, Qinhuai District, Nanjing 210007, China
(Email: diguatongxue@163.com)
(Received Mar. 28, 2017; revised and accepted June 26, 2017)

Abstract

In order to analyze the evolvement trend of the network threat and to explore the self-perception and control problem of the security situation, the dynamic wavelet neural network model is integrated into the model design, and a kind of network security situation awareness based on the optimized dynamic wavelet neural network is put forward, so as to enhance the interaction and cognitive ability between the layers of the network security system. On the basis of the analysis of the model components and their functions, the dynamic wavelet neural network algorithm is applied to obtain the accurate decision of the heterogeneous sensors for the network security events. Combined with the deduction of the relationship between the threat grade and threat genes, the shortcoming of the necessity to handle the complicated relationships among network components during the process to obtain the threat genes is overcome, and the hierarchical situation awareness method including the service level and network level is proposed to improve the expressiveness for the network threats. The simulation results show that: The network security situation awareness and method based on the optimized dynamic wavelet neural network can integrate the heterogeneous security data with dynamic perception on the evolution trend of the threat, and have the ability of self-regulation and control to certain extent, which has achieved the goal of situation awareness, and provided new methods and means for the supervision and management of network.

Keywords: Awareness; Multi-source Fusion; Network Security Situation; Wavelet Neural Network

1 Introduction

Nowadays, the role of the network and information technology is becoming more and more important in the field of economy, society and national defense. As a result, it has risen to the height of the interests of the state and all the people. It has gradually become an important factor in the economic development and national strategic deployment. However, the heterogeneous heterogeneity and complexity of the current network system, the continuous deterioration of the utilization environment, the continuous expansion of the scale and the emergence of a variety of emerging applications, the traditional "lugging holes, building high walls and anti attack" security model is lack of self-adaptability, unified scheduling and effective coordination, resulting in the widespread network intrusion and sabotage, which has led to major economic losses, adverse social impact, and even major fatal crash and casualty accident due to serious dereliction of duty.

Network security situation awareness (NSSA) is considered as a new approach to solve the problems in the field of network security [15, 21]. It can fuse the security events detected by network components and real-time perceive the network security situation and the risks faced, and has become a hot research field with the cutting-edge international and cross-disciplinary nature. In 1999, Bass *et al.* [1] proposed a multi-sensor fusion based on the situation awareness model, and the fusion model became representative at this stage of research, including the three level model composed of element extraction, state perception and situation prediction proposed by Tadda *et al.* [20], and the network situation fusion perception and risk awareness model proposed by Shen *et al.* [17]. At the same time, the visualization technology is also an significant branch of the initial phase of NSSA research.

Lawrence Berkeley National Laboratory, the National Center for Advanced Security Systems Research of the United States and other foreign military departments and research centers have developed "Spinning Cube Potential Doom" [18], NVisionIP [25] and other visual situation awareness software, and even until now, the trend of visualization for situation is still a major research direction [19]. In the period of NSSA research, the framework model and the visualization tools are developed. How-

ever, the methods and mechanisms involved in the NSSA are still validated. In the large-scale network, the visualization of network traffic and connectivity is also important. It is difficult to accurately obtain network security situation. In 2006, Chen *et al.* [3] proposed a hierarchical awareness method of network security threat situation quantification. Although the threat weight in this work still depended on the expert experience and fusion perception, the proposed hierarchical threat awareness concept had important impetus influence on the research of situation awareness.

At this stage, there was vigorous development in the research direction of the analytic hierarchy process (AHP) according to Hu *et al.* [13]. However, some problems, including the incomplete knowledge of situation knowledge, large subjective dependence of situation threat genes, and difficulties in obtaining such methods are still existed. Since 2008, fusion perception has become a hot topic in NSSA research field, and fusion algorithm is one of the core contents of the research process. Due to the randomness and suddenness of network security events, it is difficult to obtain the prior and conditional probabilities, moreover, it is hard to deal with the uncertainties in the fusion process.

D-S evidence theory meets the demand of multi-source fusion, and the demand of data traffic is small. The reasoning process has low requirement to prior probabilities and good adaptabilities in dealing with uncertainty. The fusion-perception method based on D-S linear weighting is introduced into D-S evidence by Wei *et al.* [23], while Zhang *et al.* [26] adopted the average method to improve D-S merge rule to deal with NSSA fusion perception problem. Research on NSSA fusion perception confirms the feasibility of fusion perception. But, there are still some problems such as the non-normalization and fusion conflict in the process of D-S evidence fusion.

Since 2010, the cognitive ability and feedback control of situation awareness have received a great attraction from network security researchers, and there have been many representative research results. For example, according to [5], author thought cognitive perception is an important challenge in the field of information fusion, and has discussed the formal theory basis of cognitive situation awareness (like dependency theory and extended constructive function). Gong *et al.* [11] emphasized the feedback control structure of NSSA research in the proposed framework of network situation, and argued that extended control cycle model (OODA) provided a data fusion mechanism to deal with multiple concurrency and latent interaction. Zhang *et al.* [24] constructed an NSSA model based on Markov game. Although the core of the research was to build a tripartite game model by using risk communication networks, the concept of security system reinforcement emphasized not only the realization of threat situation, but also the control of system state.

Neural network is considered to be a new mechanism to solve the problem in NSSA. In the literature, there are several researches on cognitivering, cross-layer structure and self-adaptability taking into account. Thomas *et al.* [8] agreed that neural networks should employ designs similar to those of the OODA ring, enhancing the cognitive ability of the system. Cross-layer design is another research hotspot of neural network, and also a widely accepted structural form in academia. Clark *et al.* [4] and Shakkottai *et al.* [16] considered that the cross-layer structure was the basis of neural networks and could overcome the shortcomings of the traditional network level information interaction difficulties, which had been initially applied and tested in the wireless network channel management [7], self-interference [6], path selection [2] and other studies. unfortunately there were still the shortcoming only for the specific network level, overlap optimization and other issues.

The autonomic and dynamic configuration ability of neural networks are also considered as a feasible way to realize adaptive system. Gomez *et al.* [10] proposed a neural network framework abstraction layer and operating environment (ALOE), which can provide dynamic configuration, resource awareness and operation control for the real-time system platform. Gupta *et al.* [12] and Ogiela *et al.* [14] thought that neural networks have the ability to reason and perceive autonomously, and can simulate cognitive functions,including learning, memory, reasoning and perception.

Furthermore, they can be applied to security, information system decision-making and many other fields. The above mentioned studies have provided feasible theoretical basis for the realization of intelligent systems with autonomous characteristics, perception and learning ability via using neural networks, while foreign military and research institutions start their own research program from the dynamic configuration of neural network capacity, for example, National Natural Science Foundation of the United States, DARPA and NASA funded the BNA (bio-networking architecture project) [9], Tbatou [22] and other research, also, the European Union launched the seventh Framework Program (FP7).

Such research programs have validated that neural networks can build adaptive systems in a systematic and empirical manner and can provide a new approach to self-management. According to the development of NSSA, NSSA has transitioned from perception network to perception control network. In this paper, based on the existing research results, the wavelet neural network is integrated into the research of the security situation awareness, and a model of network security situation awareness is proposed. The research is applicable to the dynamic wavelet neural network algorithm in the heterogeneous sensor environment, and the dynamic awareness is achieved for the perception of external environmental information, controlling of internal operating state, and the establishment of the bridge between the discrete control and continuous control, so as to achieve the purpose of situation awareness.

2 Dynamic Wavelet Neural Network Security Situation Awareness

Through the cross-layer optimization and integration of CPSO-DS, the data accuracy, consistency and other issues have been solved. And the situation awareness is the dynamic evolution view of the network system generated on the basis of the fusion results, with the situation factor extraction and hierarchical threat awareness as the key issue.

2.1 Situation Elements Extraction

For a successful NSSA system, effective perception depends on accurate factor extraction. The composition of the situation elements should include all the key factors in the network that can cause changes in the situation, such as the attack threat gene (threat level), attack intensity (event frequency), asset importance, and so on. Among them, the importance of assets and attack strength are attributes that are easy to be obtained, but the threat gene generation is the current difficult content in the study. From the current research status, empirical recursive and AHP analytic methods are the most successful research methods in threat gene research. However, the experience recursive method is more dependent on expert experience, subjectivity is strong and difficult to obtain. AHP method needs to make a complex deduction to the influence of the problem component and subordinate relationship.

In this work, the wavelet neural network is introduced into NSSA and its fitting with NSSA is studied. Assuming that there are n targets in the network environment, it is required assign the threat genes. The decision-making target can obtain m threat genes for n different types of events. Each threat gene is treated as a random variable x_i with value taken as 1 and -1, respectively. The purpose is to make the random variable satisfy a distribution with the mean 0. Let $X_n = \sum_{i=1}^{n} x_i$, $Y = \frac{X_n}{\sqrt{n}}$ (X, n), when $n \to \infty$, Y obeys a normal distribution, then X_n gradually obeys the normal distribution $N(0, n)$, and then the horizontal ordinate of the normal distribution curve is the importance of the decision-making target (the size of the threat gene), and the vertical ordinate is the number of decision targets (sorted by the threat level from highest to lowest). According to the characteristics of the normal distribution, the threat gene pattern can be described as follows: The greater the impact on the network security situation, the threat gene of the event closer to the first quadrant of the first position; the other hand, the threat gene in the second quadrant more left Position, as shown in Figure 1. The following will simplify the acquisition of the threat gene by reasoning, so that the threat gene can be easily calculated only at the known threat level.

Perform equidistant partition on the normal distribution curve vertical axis with as the scale factor, as presented in Figure 2, making transformation on the curve in the second quadrant with line $f(x) = A$ as the axis of symmetry, and moving the vertical axis to the left by 3σ.

$$y = \begin{cases} 3\sigma + \sqrt{-2\sigma^2 \ln[\sigma\sqrt{2\pi}x]}, 0 < x < \frac{1}{\sqrt{2x}} \\ 3\sigma, x = \frac{1}{\sqrt{2\pi}} \\ 3\sigma - \sqrt{-2\sigma^2 \ln[\sigma\sqrt{2\pi}(\frac{2}{\sigma\sqrt{2\pi}} - x)]}, \frac{1}{\sigma\sqrt{2\pi}} < x < \frac{2}{\sigma\sqrt{2\pi}} \end{cases} \quad (1)$$

From Equation (1), it can see that the target range is $(0, \frac{2}{\sigma\sqrt{2\pi}})$. Divide it into n equal parts $(x_i = \frac{i}{n} \times \frac{2}{\sigma\sqrt{2\pi}}$, $1 \le i \le n)$, and introduce into Equation (1), then y_i corresponding to x is the threat gene of the queue level i. The maximum threat gene is $ny_{max} \approx 6\sigma$, then the i-th threat gene (G_i) can be quantified as

$$G_i = \frac{y_i}{y_{max}} \begin{cases} \frac{1}{2} + \frac{\sqrt{-2\ln\frac{2i}{n}}}{6}, 1 \le i < \frac{n}{2} \\ \frac{1}{2}, i = \frac{n}{2} \\ \frac{1}{2} - \frac{\sqrt{-2\ln[2-\frac{2i}{n}]}}{6}, \frac{n}{2} < i < n. \end{cases} \quad (2)$$

At this point, the threat gene can be obtained only by knowing the different threat types (n), and ranking the threat degree of each type of threat to the network (i), to obtain the threat gene of the i-th level event. When NSSA is applied to networks with different attack susceptibilities, it is only necessary to rearrange the rank of the threat type. This method can greatly reduce the complexity of the acquisition of threat gene and improve the current status of the acquisition of threat genes with strong subjectivity, high complexity, and dependence on the expert experience.

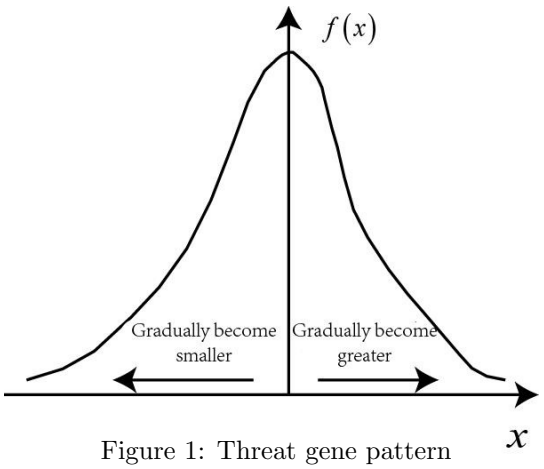

Figure 1: Threat gene pattern

2.2 Threat Quantitative Awareness

In this paper, the network security situation is divided into two different levels, including service-level and network-level. The core idea is: At two different levels, the security situation values are both based on the sensitivity of the network system for the type of attack, with the situation elements as the central point of view to achieve the hierarchical awareness.

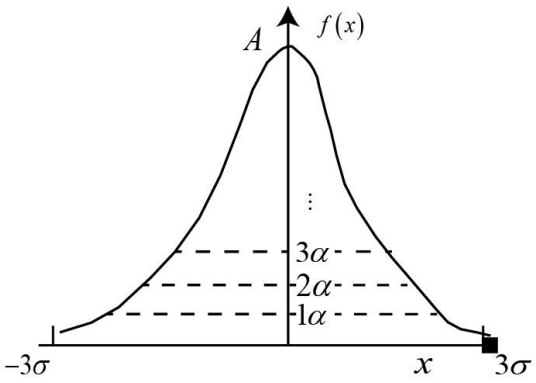

Figure 2: Threat equal interval separation

2.2.1 Service Security Situation

Definition 1. *(Threat Gene). In the time window tw, the service $s_i(0 \le i \le u)$ is subjected to n different types of attacks $a_{ij}(0 \le j \le n)$. According to the degree of threat to the service s_i, n attacks can be divided into $g(1 \le g \le n)$ different threat levels (a variety of different types of attacks can fall under the same threat level), then the threat gene of grade k is*

$$l_k = \begin{cases} \frac{1}{2} + \frac{\sqrt{-2\ln\frac{2k}{n}}}{6}, 1 \le k < \frac{n}{2} \\ \frac{1}{2}, i = \frac{n}{2} \\ \frac{1}{2} - \frac{\sqrt{-2\ln[2-\frac{2k}{n}]}}{6}, \frac{n}{2} < k < n. \end{cases} \quad (3)$$

According to the different types of attacks, from the Definition 1 the degree of threat to attack the service quantization weight can be determined. Additionally, the service security situation is also related to the attack strength, and Definition 2 can be obtained accordingly.

Definition 2. *(Service Security Situation). Under the premise of Definition 1, the threat gene quantization weight of g different attacks is $l_k(1 \le k \le g)$; service s is subject to a total N_i number of various types of attacks, in which, the number of type $j(0 \le j \le g)$ attack is denoted as N_{ij}, known as the attack strength, and $N_i = \sum_{j=0}^{s} N_{ij}$ is satisfied. Then the security situation of service $s_i(0 \le i \le u)$ is $N_i = \sum_{j=0}^{g} N_{ij}$.*

In which, u is the number of the services. The purpose of Equation (4) using 10^{l_k} is to emphasize the importance of the threat genes, and weaken the impact of attack strength on the service security situation.

$$V_{S_i} = \sum_{k=1}^{g} N_{ik} 10^{l_k} \quad (4)$$

2.2.2 Network Security Situation

Network security situation is composed of the host security situation within the time window *tw* and the number of host and so on.

Definition 3. *(Network Security Situation). In the time window tw, there are v hosts in the network system NS, where in the importance degree of the host $H_i(1 \le i \le v)$ is $g_{H_i}(1 \le i \le v)$, then the network security situation is*

$$V_{NS} = \sum_{i=1}^{v} (V_{H_i} g_{H_i}) \quad (5)$$

In which, the host weight is determined by the number of the key services running on the host, the asset value, and whether there is the presence or confidential data as $(t_{H1}, t_{H2}, \cdots, t_{Hv})$, on conduct normalization to obtain the host weighting:

$$g_{H_i} = \frac{t_{H_i}}{\sum_{j=1}^{v} t_{H_j}} \quad (6)$$

In the network system, the greater the value of VNS is, it indicates that the more serious threat that network system is facing; on the other hand, the network system is relatively safe. In contrast to intrusion detection, security situation awareness techniques map discrete alarm events into continuous security situation evolution curves, and visually express the threats and evolving trends of current network systems. Combined with the visualization technology, it can generate hierarchical, multi-dimensional dynamic evolution view, intuitive perceptual service, host and network and so on, which have provided new methods and means for the monitoring and management of the network, and can also be applied to construct the multi-dimensional dynamic evolution view, as well as provide the reference for safety control.

3 Simulation Experiment and Analysis

3.1 Fusion Ability

According to the research demand, the network topologies are designed.The three kinds of sensors, including Netflow, Snort and Snmp, are deployed to detecting data at different levels. The cross-layer heterogeneous sensor data transmission and formatting are realized by XML technology. Furthermore, the relationship between the three sensors and cross-layer perception ring components, as well as the structure of the Snmp sensor design are shown in Figure 3.

The training set and test set select 20% and 9% of the 10% data set of DARPA 99 intrusion detection data (See Table 1). The data selection process is based on the proportion of traffic in the real network and Netpoke, so as to achieve the greatest degree of simulation Internet. Adopting the results of three kinds of sensors to conduct several rounds of training on the CPSO-DS fusion engine with the population size of 55, and search the optimization weights in [0, 1]. The influence of noise on the weight optimization is reduced by the combination of the offline

optimization and on-line adjustment. And the expected variance and Netflow port change rate and flow access ratio is adopted to obtain the heterogeneous sensor BPA, as listed in Table 1.

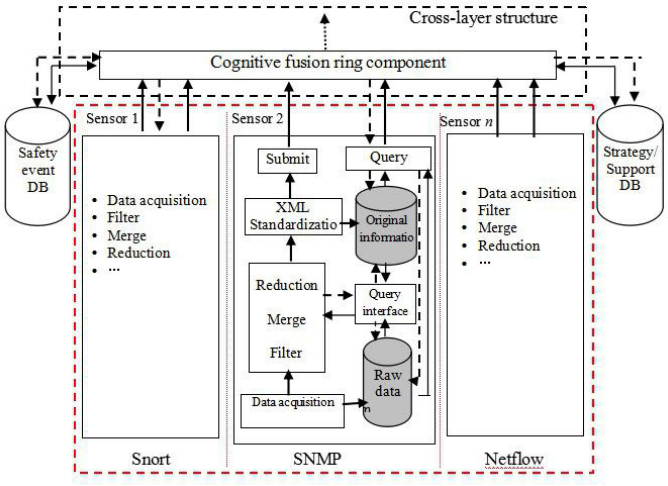

Figure 3: Relations between sensors and cognitive circle components

According to the network topology, the CPSO-DS is applied to fuse the alarms generated by the replay test set and fuse with the un-weighted traditional DS and the empirical weight DS. The PSO-DS of the two data sources fusion is compared at the detection rate (DR) and false discovery rate (FDR) aspects, as shown in Table 2.

The experimental results show that CPSO-DS multi-source fusion is superior to the other methods in detection rate and false alarm rate. In addition, compared with the two sensor research in literature [9], the increase of sensor number can improve the detection rate and reduce false alarm rate. During the experiment, from the point of view of U2R and R2L, it is more difficult to improve the detection efficiency simply by increasing the number of sensors. More host-based sensors should be designed to improve their detection capability. Besides, from the two data sources and three data sources on the performance comparison, an increasing of the data source can improve the accuracy, but sometimes can not significantly enhance the accuracy of fusion, in other words, for multi-source integration, it is not necessary better if there are greater number of sources, and the accuracy of the fusion is closely related to the detection performance and characteristics of the added sensor itself.

3.2 Hierarchical Awareness

3.2.1 Service Security Situation

On the basis of the output of the CPSO-DS fusion engine, the threat awareness can be performed according to the steps of factor extraction, feature quantization and layer awareness. The attack method needs to quantify the attack strength, attack type and threat gene, etc. The attack strength can be determined statistically in the time window through the output of the CPSO-DS fusion engine. Attack types and their threat levels are listed in Table 1, and the threat genes (n = 5, g = 4) are calculated according to Equation (3). The simulation network runs for a total of one week (From June 10, 2013 to June 16, 2013), the attacker consists of two terminals, which autonomously arrange the attack time, the defense side has no knowledge of the hacking simulation behavior, the test set attack data is selectively replayed to the local area network and the dynamic evolution curve of the security situation of a certain service is obtained according to Equation (4). Figure 4 shows the evolution of security situation for the running three services of Email, Http and Snmp on host H1. The abscissa is time, the length is 7 days, time window is 2 hours; and vertical ordinate is the service security situation value, which expresses the threat level of the attack to the service.

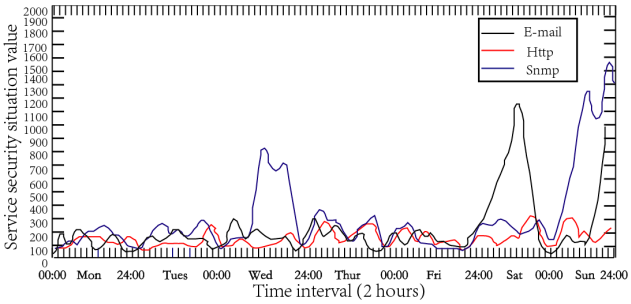

Figure 4: Service security situation after self-adapting

As can be seen in Figure 4, both Http and Snmp services are heavily attacked on Sunday, on Wednesday afternoon and at night, Http's security situation should also be concerned, and Snmp is threatened late Saturday night; email service is stable during the whole monitoring period. According to the service security wavelet network curve, the network analyst should strengthen the supervision of the managed service in the time of severe threat and make further inspection on the vulnerability and configuration, etc. From the service security situation view can also be seen in a certain period of time, security threats there is a gradual and serious regularity, the administrator should be based on service security trends and trends in advance to take appropriate measures. Owing to the space limitation, this work only shows the E-mail, Http and Snmp security situation on host H1, and will not elaborate the host H2 and H3 service security situation evolution view.

3.2.2 Network Security Situation

The perception of network security situation requires to determine the weight of the importance of the host, but the determination of the host weight is more complicated than the service weight, which is related to the host asset value (V_h), service criticality (C_s), access frequency level (A_f) and confidentiality (D_c) and other factors, the im-

Table 1: Basic experiment data

Type	Train. Set	Experi. Set	$BPA_{Netflow}$	BPA_{Snort}	BPA_{Snmp}	$w_{Netflow}$	w_{Snort}	w_{Snmp}	Threat Grade	Threat Gene
R2L	226	98	0.098	0.194	0.347	0.26	0.71	0.67	1	0.726
U2R	31	11	0.146	0.203	0.261	0.23	0.91	0.69	1	0.726
DoS	78291	33665	0.283	0.189	0.167	0.93	0.34	0.22	2	0.611
Probe	822	354	0.367	0.288	0.188	0.88	0.60	0.41	3	0.389
New	*	*	0.106	0.126	0.037	0.58	0.71	0.43	0	1

Table 2: Fusion ability

Parameter	Traditional D-S(%)	Empirical Weighted D-S(%)	PSO-DS (Two Data Sources) (%)	CPSO-DS (Three Data Sources) (%)
DR	73.33	82.60	86.67	88.11
FDR	9.86	5.80	5.63	5.06

portance level is shown in Table 3, in which, the host complex importance $t_{H1} = k_V V_{hi} + k_C C_{si} + k_A A_{fi} + k_D D_{ci}$, $k_V = 0.2$, $k_C = 0.3$, $k_A = k_D = 0.25$. Based on the host security situation, we can obtain the composite importance weight of the host using Table 3, and use Equation (5) to generate the security situation evolution view of the whole network system, as depicted in Figure 5.

Table 3: Host weight grade

Host	V_{hi}	C_{si}	A_{fi}	D_{ci}
H_1	High	Medium	Medium	High
H_2	Medium	Low	Medium	Medium
H_3	High	Low	Low	Low

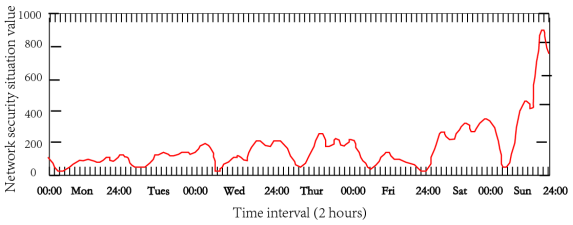

Figure 5: Network security situation

The evolution of the entire network's security situation over the course of a week can be seen from Figure 5 that On Wednesday, Thursday, and Saturday, there was a concern that have been caused by a hacker attempting to attack the network, although the need for individual hosts and services for security maintenance, but still did not have a huge impact on the entire network. Network system in June 16, 2013 appeared very serious attack situation, requiring administrators to focus on monitoring and taking appropriate action, so as to avoid the entire network system inefficient and even the collapse of the situation.

In addition to dynamically assessing the threat situation of services, hosts and networks, the hierarchical awareness method proposed in this paper has good environmental adaptability and shows certain cognitive ability. In this article, based on the weight coefficient of the threat gene acquisition method, the situation awareness system is applied to the new network, and the administrator only needs to re-sort the grades of the attacks that the network is sensitive to. Assuming a new network environment, the sensitivity of the attack on the services in order of unknown attacks, DoS, U2R and R2L and Probe, the threat genes in Table 1 in accordance with the Equation (3) can be adjusted, as shown in Table 4, and according to Table 1, Table 4, Equation (4) and (5), the security wavelet network curve at service and network levels can be generated, and it is not required to make complicated association analysis on components and elements of composition situation. Under the same attack, as plotted in Figure 4, the security situation evolution of E-mail, Http, and Snmp on the host H1 after the adaptation of the threat genes is shown in Figure 6. Similarly the security situation of the monitored service can also be perceived and shows a trend similar to the situation evolvement trend as Figure 4, but the same attack data on different networks will usually show different degree of threat.

Table 4: New threat gene

Attack Type	Threat Grade	Threat Gene
R2L	2	0.611
U2R	2	0.611
DoS	1	0.726
Probe	3	0.389
New	0	1

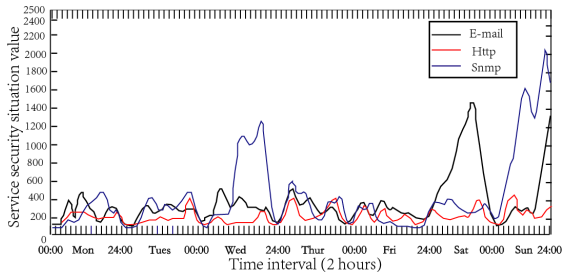

Figure 6: Service security situation after self-adapting

4 Conclusions

In this paper, existing models, fusion algorithms and perceptual methods of the network security awareness have been analyzed. Also, a network security situational awareness and control fusion model is put forward and discussed. Under the guidance of the model, CPSO-DS dynamic wavelet neural network algorithm that is applicable to the heterogeneous network is discussed, on the basis of the acquisition of the threat genes, comprehensive analysis on the two different levels of services and network security situation awareness methods are conducted, and the situation gradient is applied to achieve the self-regulation of the network security situation. Simulation results reveal that the network security situation awareness and control model based on the optimized dynamic wavelet neural network and its method can accurately identify the network security events and dynamically perceive the threat evolution trend at different levels.

References

[1] T. Bass, "Multi-Sensor data fusion for next generation distributed intrusion detection systems," in *Proceeding of the IRIS National Symposium on Sensor and Data Fusion*, vol. 4, pp. 24-27, 1999.

[2] J. S. Chen, C. Y. Yang and M. S. Hwang, "The Capacity Analysis in the Secure Cooperative Communication System," *International Journal of Network Security*, vol. 19, No. 6, pp. 863-869, 2017.

[3] Y. Chen and J. Chou, "On the privacy of user efficient recoverable off-line e-cash scheme with fast anonymity revoking," *International Journal of Network Security*, vol. 17, no. 6, pp. 708-711, 2015.

[4] D. D. Clark, C. Partridge and J. C. Ramming, "A knowledge plane for the internet," in *Proceeding of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03)*, pp. 3-10, 2003.

[5] R. Dapoigny and P. Barlatier, "Formal foundations for situation awareness based on dependent type theory," *Information Fusion*, vol. 14, no. 1, pp. 87-107, 2013.

[6] A. R. Emilio, W. Stefan, L. V. Roberto, R. Taneli and W. Risto, "Wideband full-duplex MIMO relays with blind adaptive self-interference cancellation," *Signal Processing*, vol. 130, pp. 74-85, 2016.

[7] M. Erdelj, M. Krl and E. Natalizio, "Wireless Sensor Networks and Multi-UAV systems for natural disaster management," *Computer Networks*, vol. 124, pp. 72-86, 2017.

[8] C. Fortuna and M. Mohorcic, "Trends in the development of communication networks: Cognitive networks," *Computer Networks*, vol. 53, no. 9, pp. 1354-1376, 2009.

[9] P. Gandotra, R. K. Jha and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *Journal of Network and Computer Applications*, vol. 78, pp. 9-29, 2017.

[10] I. Gomez, V. Marojevic and A. Gelonch, "ALOE: An open-source SDR execution environment with cognitive computing resource management capabilities," *IEEE Communications Magazine*, vol. 49, no. 9, pp. 76-83, 2011.

[11] Z. H. Gong and Y. Zhuo, "Research on cyberspace situational awareness," *Journal of Software*, vol. 21, no. 7, pp. 1605-1619, 2010.

[12] M. Gupta, "On fuzzy logic and cognitive computing: some perspectives," *Scientia Iranica*, vol. 18, no. 3, pp. 590-592, 2011.

[13] W. Hu, J. Li and X. Jiang, "A hierarchical algorithm for cyberspace situational awareness based on analytic hierarchy process," *High Technology Letters*, vol. 13, no. 3, pp. 291-296, 2007.

[14] M. R. Ogiela and I. You, "Cognitive and secure computing in information management," *International Journal of Information Management*, vol. 33, no. 2, pp. 243-244, 2013.

[15] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[16] S. Shakkottai, T. Rappaport and P. Karlsson, "Cross-Layer design for wireless networks," *IEEE Communications Magazine*, vol. 41, no. 10, pp. 74-80, 2003.

[17] D. Shen, G. Chen, J. B. Cruz, J. L. Haynes, M. Kruger and E. Blasch, "A Markov game theoretic approach for cyber situational awareness," in *Proceeding of the Multi-Sensor, Multi-Source Information Fusion: Architectures, Algorithms, and Applications*, LNCS 6571, pp. 1-11, Springer, 2007.

[18] Y. Shi, R. Li, Y. Zhang and X. Peng, "An immunity-based time series prediction approach and its application for network security situation," *Intelligent Service Robotics*, vol. 8, no. 1, pp. 1-22, 2015.

[19] H. Shiravi, A. Shiravi and A. A. Ghorbani, "A survey of visualization systems for network security," *IEEE Transactions on Visualization andComputer Graphics*, vol. 18, no. 8, pp. 1313-1329, 2012.

[20] G. Tadda, J. J. Salerno, D. Boulware, M. Hinman and S. Gorton, "Realizing situation awareness within

a cyber environment," in *Proceeding of the Multi-Sensor, Multi-Source Information Fusion: Architecture, Algorithms, and Applications*, LNCS 6242, pp. 1-6, Springer, 2006.

[21] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.

[22] Z. Tbatou, A. Asimi, Y. Asimi, Y. Sadqi and A. Guezzaz, "A New Mutuel Kerberos Authentication Protocol for Distributed Systems," *International Journal of Network Security*, vol. 19, no. 6, pp. 889-898, 2017.

[23] Y. Wei, Y. F. Lian and D. G. Feng, "A network security situational awareness model based on information fusion," *Journal of Computer Research and Development*, vol. 46, no. 3, pp. 353-362, 2009.

[24] Y. Zhang, X. B. Tan, X. L. Cui and H. S. Xi, "Network security situation awareness approach based on Markov game model," *Journal of Software*, vol. 22, no. 3, pp. 495-508, 2011.

[25] Y. Zhao, P. C. Fan, H. T. Cai, Z. G. Qin and H. Xiong, "Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare," *International Journal of Network Security*, vol. 19, no. 6, pp. 1044-1052, 2017.

[26] Y. Zhang, S. G. Huang, S. Z. Guo and J. M. Zhu, "Multi-Sensor data fusion for cyber security situation awareness," *Procedia Environmental Sciences*, vol. 10, pp. 1029-1034, 2011.

Biography

Huang Cong was born in the Jiangxi of Guangxi in 1974, the Master of Business School, Guangxi University. Now he is the Engineer of China Tobacco Guangxi Industry Co., Ltd. His main research direction is the computer network security.

Wang Chao was born in Nanjing in 1989, who is the Doctor of Nanjing University of Science and Technology, and his main research direction is the computer network security. Now, he is working in No. 28 Research Institute, China Electronics Technology Group Corporation, Nanjing, China.