Network Security Model Based on Active and Passive Defense Hybrid Strategy

Zhaofang Du
Henan Industry and Trade Vocational College,Zhengzhou, Henan, China
**Corresponding Author.*

Abstract

This paper studies a new network information security system and its evaluation method based on the security threat situation network security model. This paper expounds the application of active defense system and passive defense system in network security, and uses advanced technical support platform and network security model. In this paper, the active defense system and the passive defense system are organically combined to form a new model of computer network security with characteristics. At the same time, based on the idea of security threat situation evaluation, this paper extends the traditional PDRR security model and proposes a network active defense security model and defense in depth security strategy. On this basis, a hybrid architecture of active and passive defense is proposed. The architecture integrates some new network active defense technologies, and constructs a comprehensive and deep network defense system together with network passive defense means. The experimental results show that the proposed defense model improves the security defense efficiency and effective defense rate of the traditional PDRR security model.

Keywords*: Security threat situation, network security, active defense, passive defense.*

I. Introduction

The core idea of cognitive networks is to be able to perceive changes in the internal and external environment, adjust the configuration of network systems in real time, dynamically and intelligently adapt to the environment, and guide future autonomous decision-making [1-2]. It should enhance environmental adaptability and cognitive abilities by introducing autonomous strategies at the network level, such as spectrum management of cognitive radio networks [3]. At present, there is little discussion on the application of cognitive networks in wireless network security [4]. With the large-scale deployment and application of wireless networks [5], networks are not only limited by energy, means of communication and external devices, but also face more complex security threats [6]. For example, military network, emergency and disaster relief network and field animal tracking network, their application environment is complex and changeable, data packets pass through many different areas, and are limited by equipment and maintenance conditions. Managers can not make timely and effective response to environmental changes in the network operation, resulting in network performance degradation and even the termination of network services.Using passive defense, network managers predict the security threats that will occur in the network, and then design security defense strategies. This method requires network managers to be familiar with the network environment and network performance, and to master the security threats that network operation is facing.Obviously, when the network environment changes and new security threats occur, this policy will not be sufficient to solve new security threats. Even if managers can predict new security threats, due to environmental constraints, they may not be able to deploy to the running network in time.Therefore, a different method from traditional passive defense is needed, that is, network security management can actively adapt to the changes of network environment, dynamically select security policies and manage network security, and establish a bridge between external environment and internal security requirements. Therefore, an active security strategy for cognitive networks is proposed, which enables the establishment of security mechanisms to fully consider network performance and capabilities.Choose a reasonable security strategy to cope with complex and changing network environment, ensure that the network can make timely adjustments without the intervention of network

ISSN: 0010-8189

administrators, improve the initiative, security and flexibility of network security management, and have the nature of self-protection.

II. Situation awareness based on HMM model

Hidden Markov model is a kind of model with double random process developed on the basis of Markov chain. The output of Markov chain with limited hidden state is unobservable state sequence, and it also has the random process of producing observable sequence [7-10]. The stochastic process is associated with each state of Markov chain through a set of probability distributions. Because the state is invisible, the existence and properties of the state can only be perceived by observing the sequence, so it is called hidden Markov model. HMM can be used to estimate the probability of states hidden behind surface events. The composition of HMM is shown in Figure 1.

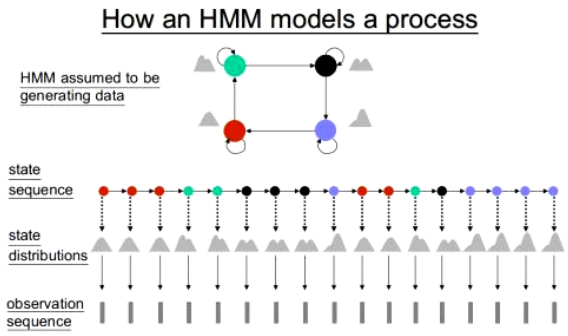

Fig 1: Schematic diagram of HMM composition

Due to the complexity of the network structure and the differences within the network, if we build a HMM model for the whole network to conduct situation assessment, it will not only increase the complexity of the assessment, but also a model can not adapt to the needs of different networks. Therefore, this paper establishes a HMM model for each service on the asset, obtains the observation sequence according to the threat type and vulnerability information, and evaluates the security situation of the service. HMM model can be represented by a five tuple λ: λ = {S, V, II, A, B}.

State space S: hidden Markov chain in hmm. S={S_1, S_2,...,S_N}, which indicates the set of service states. The model has four States, namely Safe, Ignorable, Danger and Disastrous. The success probability of network threats is different in different states. Transitions between states form a Markov chain, and each state can be directly transferred to another state. Yes! At the moment, the service status is q_t, q_t ∈ (Safe, Ignorable, Attacked, Dancer).

Safe: indicates that it is in a safe state and the success probability of network threat is low.

Ignorable: it means that the security is reduced and the success probability of network threats is slightly improved.

Danger: in a dangerous state, the success probability of network threats is greatly increased.

Disastrous: it means that it has been invaded by people, the success probability of network threat is close to 1, the confidentiality, integrity and availability are damaged, and it is in a disastrous state.

III. Model structure

In the aspect of network security situation assessment, the paper proposes a bottom-up quantitative model. However, this method only considers one asset of the host, and only calculates the threat index according to the alarm log, and the threat index only reflects the security situation in a period of time, so the real-time performance is not strong. In this paper, the hierarchical structure model is improved, and the hierarchical network system security threat situation quantitative assessment model as shown in Figure 2 is proposed.

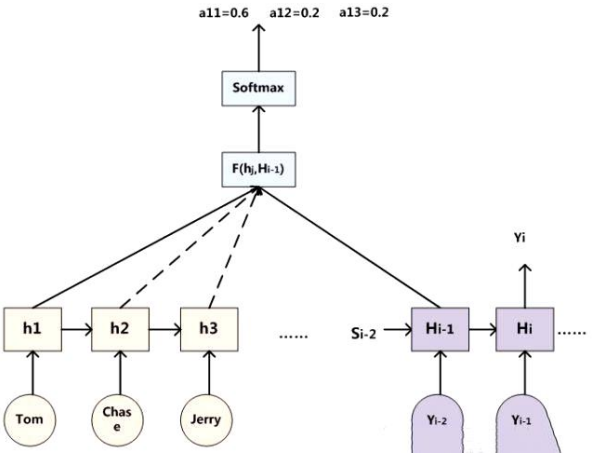

Fig 2: Hierarchical network system security threat situation assessment model

The network system can be divided into three levels: network, asset and service. Assets are valuable resources in the system, including hosts, servers, routers, gateways and firewalls. Asset weight is determined by asset type, performance and network location, which indicates the importance of assets in the network. For each service on the asset, it can be divided into three levels according to the importance of the asset, value = {1,2,3}, and the weight of the service in the asset can be obtained according to the level.

Aiming at the weakness of the original model, the improved model can generate a threat record for each threat detected. If no threat is detected in a time unit, a normal record is generated. According to each record to calculate the security situation value, as the smallest unit of situation change, it has strong real-time. Network threats generally appear continuously in a period of time. The threats that appear in the previous moment not only affect the security situation at that moment, but also affect the security situation at the following moment. In order to highlight the characteristics of network threat persistence, the time vector $\dot{t}$ is defined as the weighting factor of 10 records before time t. The closer to the time t, the greater the weighting factor. The weighting factor of the last record is 1.

Definition 1: Service threat index ST: the loss of a service under network threat. According to the configuration of each service, the vulnerability information of the service is recorded. When the service is threatened by the network, it matches with the vulnerability information. If the required vulnerability exists, the threat is likely to succeed; if the required vulnerability does not exist, the threat is unlikely to succeed. Considering the security state of the service at that time, the success probability P of the threat can be obtained. Combined with service importance level and success probability, the service threat index of the record can be calculated:

$$T = value \cdot P \quad (1)$$

Define the index vector (the index of the last 10 records $T = (T_1, T_2, ..., T_{10})$, where T_{10} is the index of the last record. The service threat index at time t is:

$$ST(t) = \dot{T} \cdot \dot{t} \quad (2)$$

Compared with the service threat index in the literature, the index reflects the threat and vulnerability information comprehensively, and every threat will change the index. Therefore, it has strong real-time performance.

Definition 2: asset threat index PT: the sum of asset security losses when threatened at a certain time. When multiple services are attacked, various threats interact with each other, which will increase the threat degree of assets. The weighting factor $\theta = (\theta_1, \theta_2, ..., \theta_m)$ is defined, which can be obtained according to the combination and weight of different services, avoiding the calculation of asset threat index by accumulating the threat degree of several services.

$$PT_j = \theta \sum_{i=1}^{n} (\omega s_i \cdot ST_i) \quad (3)$$

Definition 3: network system threat index LT: the total loss of the overall network security at a certain time. Weighted by each asset threat index, it can be concluded that:

$$LT = \sum_{i=1}^{m} (\omega t_i \cdot PT_i) \quad (4)$$

Where: PT_i is the threat index of the ith asset; n is the number of services; wt_i is the weight of the ith asset, and $\sum_{i=1}^{n} \omega t_i = 1$.

IV. Simulation experiment

In order to verify the rationality of the model, this paper demonstrates the specific implementation process of the model based on KDD CUP99 data set. The experimental environment is LAN, which has eight different assets, including host, router, firewall, etc. The network structure is shown in Figure 3.

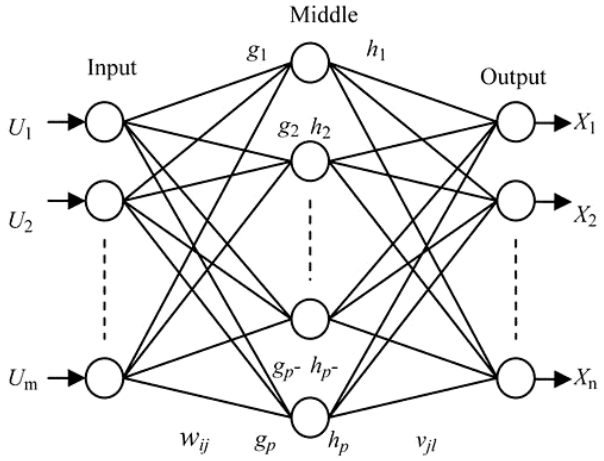

Fig 3:Topology diagram of network structure

Each asset has different weight in the network according to its type, location and configuration. Services in each asset have different weights. The assets in the system, the weight of the assets, the services contained in the assets and their weights are shown in Table 1.

Through the training of training set in data set, II, A and B in λ can be initialized as: II = (0.5,0.2,0.2,0.1).

$$A=\begin{bmatrix} 0.7 & 0.2 & 0.06 & 0.04 \\ 0.2 & 0.7 & 0.05 & 0.05 \\ 0.1 & 0.1 & 0.6 & 0.2 \\ 0.05 & 0.05 & 0.1 & 0.8 \end{bmatrix},$$

$$B=\begin{bmatrix} 0.05 & 0.025 & 0.2 & 0.15 & 0.15 & 0.075 & 0.075 & 0.1 & 0.15 & 0.025 \\ 0.2 & 0.1 & 0.1 & 0.05 & 0.15 & 0.075 & 0.075 & 0.15 & 0.05 & 0.15 \\ 0.075 & 0.075 & 0.15 & 0.15 & 0.1 & 0.075 & 0.15 & 0.075 & 0.2 & 0.5 \\ 0.2 & 0.15 & 0.15 & 0.1 & 0.1 & 0.075 & 0.075 & 0.075 & 0.05 & 0.025 \end{bmatrix}$$

Table 1: Assets, services and their weights in the system

Assets	Asset weight (wt)	Servicescontainedinassets(server)	Serviceimportancelevel(value)	Serviceweight(ws)
1	0.161	http,domain_u,pop3,private	(3,1,2,3)	(0.4,0.1,0.2,0.3)
2	0.121	http,domain_u,smtp	(3,3,3)	(0.4.0.2,0.4)
3	0.121	domain_u,ftp,private,telnet	(1,3,3,3)	(0.1,0.35,0.25,0.3)
4	0.129	ftp,pop3,private,eco_i	(3,2,3,1)	(0.4,0.2,0.3,0.1)
5	0.078	http,telnet,pop3	(3,3,2)	(0.4,0.4,0.2)
6	0.141	http,ftp,smtp	(3,1,3)	(0.3,0.4,0.3)
7	0.132	ftp,pop3,domain_u,private	(3,2,1,3)	(0.4,0.2,0.1,0.3)
8	0.140	domain_u,ftp	(1,3)	(0.25,0.75)

V. Results and discussion

Figure 4 is the service threat index calculated according to the threat records of 40 times of HTTP service on asset 2 in a certain period of time. The weight of HTTP is 3, and the greater the threat index is, the more dangerous the service is. The hierarchical evaluation method without adding time vector can be selected to compare with the method in this paper.

In Figure 4, the first four times are normal records. At this time, the service is in safe state, and the threat index is 0. The seventh threat makes the service state become ignorable. The 18th threat makes the service state become danger. The 22nd attack makes the service state become disastrous. With the change of state, the success probability increases and the threat index increases faster. The network administrator adjusts the security policy in the 28th threat to eliminate the vulnerability of the service. At this time, although the attack is still continuing, it cannot succeed, and the success probability becomes zero.

ISSN: 0010-8189

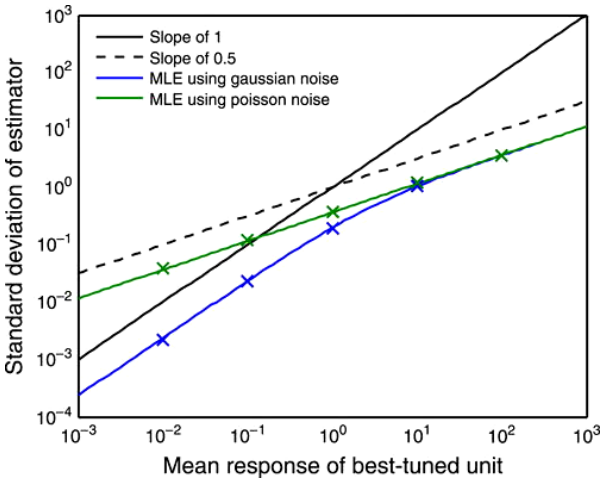

Fig 4:Value of service threat index in a certain period of time

Figure 5 shows the threat situation of asset 2. In about 110 minutes, the assets are attacked by HTTP and SMTP. The threat index calculated by this method is significantly higher than that calculated by hierarchical method, which better reflects the security situation information of assets.

Figure 6 shows the threat situation of the whole network system. Through Figure 6, the network administrator can intuitively understand the network security situation and timely adjust the security strategy.

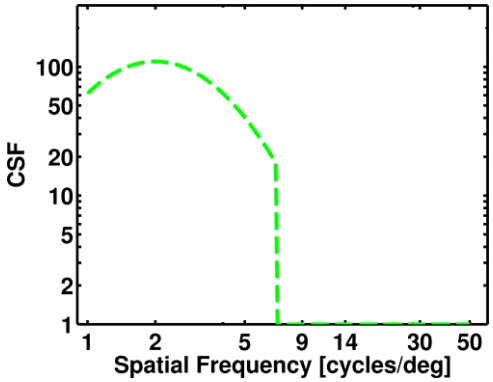

Fig 5:Threat index of asset 2

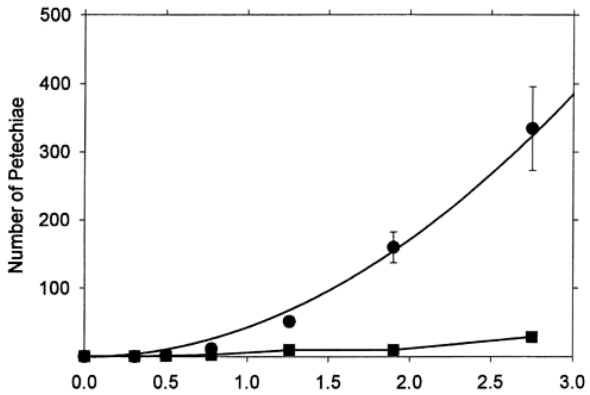

Fig 6:Schematic diagram of overall network threat index

ISSN: 0010-8189

Because the hierarchical method does not use the time vector, the security situation value of the previous time does not affect the subsequent value, and the threat index of the hierarchical method is lower than that of the proposed method. Therefore, compared with hierarchical method, this method is more sensitive to threats and can provide more accurate network security situation information for network administrators.

VI. Conclusion

The current network security situation assessment method is not mature enough. In this paper, considering the network attack and network attributes, we use HMM to calculate the security situation quantitatively, which provides a new idea for the evaluation of network security situation. The follow-up work is to optimize the training method of transfer matrix in the model and study the network situation prediction.

References

[1] Yang Yi, Bian Yuan, Zhang Tianqiao. Network Security Situation Awareness Based on Machine Learning. Computer Science and Application, 2020, 10 (12): 8
[2] Li Zhiyong. Hierarchical Network Security Threat Situation Quantitative Assessment Method. Communication World, 2016, 23: 70-70
[3] Hu Wenji, Xu Mingwei. Analysis of Secure Routing Protocols for Wireless Sensor Networks. Journal of Beijing University of Posts and Telecommunications, 2006, 29 (s1): 107-111
[4] Wei Yonglian, Yi Feng, Feng Dengguo, Yong W, Yifeng L. Network Security Situation Assessment Model Based on Information Fusion. Computer Research and Development, 2009, 46 (3): 353-362
[5] Xu Guoguang, Li Tao, Wang Yifeng. A Network Security Real-time Risk Detection Method Based on Artificial Immune. Computer Engineering, 2005,31 (12): 945-949
[6] Jiang Wei, Fang Binxing, Tian Zhihong. Network Security Evaluation and Optimal Active Defense Based on Attack Defense Game Model. Acta Computer Sinica, 2009, 32 (004): 817-827
[7] Miao Yongqing. Stochastic Model Method and Evaluation Technology of Network Security. China Science and Technology Investment, 2017, 4: 314
[8] Yi Hua Zhou, Wei Min Shi, Wei Ma. Research on Computer Network Security Teaching Mode for Postgraduates Under the Background of New Engineering. Innovation and Practice of Teaching Methods, 2020, 3 (14): 169
[9] Bao Xiuguo, Hu Mingzeng, Zhang Hongli. Two Quantitative Analysis Methods for Survivability of Network Security Management Systems. Acta Communication Sinica, 2004, 25 (9): 34-41
[10] Li Weiming, Lei Jie, Dong Jing. an Optimized Real-time Network Security Risk Quantification Method. Acta Computa Sinica, 2009 (04): 793-804