The Self-learning Network Defense Based on Game Theory

Wei Wang[1, a *] and Wenhong Zhao[2,b]

[1] Science and Technology on Communication Information Security Control Laboratory, Jiaxing Zhejiang 314001, China

[2] Nanhu College, Jiaxing College, Jiaxing 314001, China

[a]wwzwh@163.com, [b]whzhaonh@163.com

Keywords: Active defense; Mixed strategies equilibrium; Network security; Game theory

Abstract. At present, the active defense strategy based on game theory is based on the complete information game model. For such model cannot cope with attackers and defenders do not know each other's behavior problems, based on the cooperation, and incomplete information game theory is proposed to improve the existing strategy gains quantitative method, calculation and comprehensive analysis of the bayesian equilibrium.

Introduction

Game theory[1] has a natural close relationship with network antagonistic behavior, and can fully consider the balance between the dependence of the attacker and the defense strategy and the balance between cost and benefit. Because of this, Liang et al. [2] pointed out that the theory of game theory has played an important role in the field of online confrontation and is a promising research direction of future network security.

K. Lye et al. [3] analyzed attacker and defender game strategy, defines the required recovery time after being attacked by network as earnings game model, and analyzes the network security. Xu et al. [4] designed and analyzed the DDoS defense system based on the complete information static game theory to optimize the performance of the system. Jiang Wei et al. [5] will be the process of game between the network attacker and defender as a game, two roles established a offensive and defensive game model, and presents a zero-sum and non-cooperative zero-sum game algorithm, deficiencies in using complete information static game model, and the network scene actual close enough. Wang Chunlei et al. [6] proposed a stochastic game model and used game model to analyze network survivability. Min Yu et al. [7] analyzed the network counterfeiting attack based on the stochastic game model. The problem of Wang and Min lies in the use of the complete information game model, and the state transfer probability function is not easy to determine. Ling wang group et al. [8] introduces dynamic game model in the network active defense, through the "virtual node" network attack and defense figure into the network game tree, the existence of the problem is that based on complete information hypothesis, and did not fully consider strategy yields quantitative problem. Yu-ling liu et al. [9] apply incomplete information static game model to worm strategy performance evaluation, the existence of the problem is not considering the defenders multiple types of situation, and only the pure strategy bayesian equilibrium is analyzed. Billy Chen et al. [10] this paper presents a model based on non-zero-sum active defense strategy selection method, the actual scene abstracted as the attacker, network system and legitimate users, the game between the deficiency also is to use the complete information static game model.

At present, most of the defensive strategies based on game theory adopt the complete information game model. This kind of game model can calculate the Nash equilibrium and have the advantages of simple calculation according to the strategy income quantification. But when attackers and defenders do not know each other's behavior, the game model based on the complete information game can be very limited. The literature [11] in the wireless sensor network intrusion detection system and the interaction between the nodes is modeled as a process of static bayesian game, game result can be used to guide the defensive strategy against DoS attacks. The paper [12] designed the wireless sensor network clustering routing algorithm based on static bayesian game, and verified the effectiveness of the algorithm.

Literature [13] model the multi-node resource allocation process in wireless network into a static bayesian game process, and the bayesian equilibrium is provided with guidance for resource allocation. The paper [14] is to model the distributed power distribution process of multi-input multi-output network as the process of incomplete information game for multi-transporters, so that power distribution is more in line with actual demand. The above literature provides reference for the research of this paper.

This article contribution is as follows: (1) this paper defenders back behavior, attack the success rate of existing policy gains quantitative method is improved, making strategy income quantification is more reasonable and accurate; (2) this paper gives a test model for attackers to distinguish between normal users and intruders.

Defense Strategy Gain Quantification

The quantification of the cost-benefit of the attacker and defender in the network is the foundation of the optimal defense strategy selection of the network, and its quantification is reasonable to directly influence the selection of the network defense strategy. Jiang wei et al. [5] put forward a method of cost/income quantification on the basis of summarizing various classification of attack defense strategies. Chen yongqiang and others propose a method for quantifying strategy cost/benefit based on intention. This paper improves the quantitative methods of the above strategies and makes the quantitative results more scientific and reasonable.

Definition 1. *Dcost* (Damage cost): the cost of the loss of the system represents the degree of Damage to the target resource of a certain type of attack; *AL* (Attack Lethality): the degree of inherent harm to a type of Attack; *AC* (Attack Cost) indicates the hardware and software resources needed for an attacker to launch an Attack, etc. *Decost* (Defense cost): cost of defense is the operation cost, negative cost and residual cost of Defense strategy. It is generally possible to take the loss of the defender Dcost as the income of the attacker. See the literature [5] in detail.

Definition 2. *DR*(Defense Reward): defense reward for defense against a defensive strategy. In the literature [5] take defensive strategy against an attack, only consider the loss of network systems from without considering failure, attackers defenders to counter the defense in return. Therefore, in this paper, the defense return is divided into two situations.

attack success, even if the attacker had a successful attack, the defender will master relevant information, the attacker failed because of its defense and counterattack ability to drop, can use the discount factor μ and $DR_j^{'}$ multiply until this time back in return. At this point, the defensive return is;

when the attack fails, $DR_j^{'}$ indicates that the defender has the information of the attacker's identity and other information, and returns the attacker's backtracking and counterattack.

Definition 3. *SAR*(Success Attack Rate): the probability that an attacker will Attack a successful Attack if the attacker or defender adopts a corresponding strategy. The literature [5] did not consider the success rate of attack, and the default attackers were successful, which was obviously unreasonable. Whether an attacker can attack a successful attack has a very strong relationship with the defender's ability to detect attack and defense. Therefore, the attack success rate *SAR* can be refined as the product of the defense detection rate α and the defense success rate β. Success when attacking, likely is the defender but the test has been successful defense failed, also may be the defender test is not successful cause the failure of defense, the probability $\alpha(1-\beta)$ and $1-\alpha$, respectively, the $SAR=\alpha(1-\beta)+(1-\alpha)$. When an attacker fails, there is only one case where the test succeeds and the defense succeeds, and the success rate is equal to $\overline{SAR}=\alpha\cdot\beta$.

When the attack is successful, both sides benefit:

$$U_A(M_A,M_D,T_A)\big|_{WIN}=D\cos t-\mu\cdot DR^{'}-AC$$

$$U_D(M_A,M_D,T_D)\big|_{LOSE}=-D\cos t+\mu\cdot DR^{'}-De\cos t$$

The benefits of both parties when the attack fails:

$$U_A(M_A, M_D, T_A)\big|_{LOSE} = -DR^{'} - AC$$

$$U_D(M_A, M_D, T_D)\big|_{WIN} = DR^{'} - De\cos t$$

The success rate of the attack strategy is SAR_i, thus the expected revenue expectation of the two parties in this network scenario:

$$U_A(m_i^A, m_j^D, t_A) = SAR_i \cdot (\sum_e D\cos t_{ij}(a_e) - \mu \cdot DR_{ij}^{'} - AC_{ij}) + \overline{SAR_i} \cdot (-DR_{ij}^{'} - AC_{ij})$$

$$U_D(m_i^A, m_j^D, t_D) = SAR_i \cdot (-\sum_e D\cos t_{ij}(a_e) + \mu \cdot DR_{ij}^{'} - De\cos t_{ij}) + \overline{SAR_i} \cdot (DR_{ij}^{'} - De\cos t_{ij})$$

Here, a_e is the atomic attack contained in this attack strategy; i, j is the i-th action and j-th action for the attacker and the defender.

The sum of the proceeds of the attacker and the defender is:

$$U_A(m_i^A, m_j^D, t_A) + U_D(m_i^A, m_j^D, t_D) = (SAR_i + \overline{SAR_i}) \cdot (-De\cos t_{ij} - AC_{ij})$$

In another network game scenario, the attacker chooses not to attack, and the defender chooses the defensive action m_j^D. In this scenario, the proceeds of the attacker and the defender are:

$$U_A(not \quad attack, m_j^D, t_A) = 0$$

$$U_D(not \quad attack, m_j^D, t_D) = -(SAR_i + \overline{SAR_i}) \cdot De\cos t$$

The sum of the profits of each of the above game scenarios is:

$$U_A(not \quad attack, m_j^D, t_A) + U_D(not \quad attack, m_j^D, t_D) = -(SAR_i + \overline{SAR_i}) \cdot De\cos t$$

It is easy to know from the above derivation that the sum of the game benefit of the aggressor and the defender is not zero, and the game is non-zero sum game, whether the attacker attacks or does not attack. Attackers attack to gain valuable information from defenders, who want to defend against such attacks. In the process, both sides need to pay the price. When the attacker does not attack, the defender is defensive and the defender pays the appropriate defense.

Intrusion Detection Training Model

The purpose of the training model is to enable the scheme to have the ability to reflect the normal or invasive behavior characteristics of the network. The training process is shown in Fig. 1.

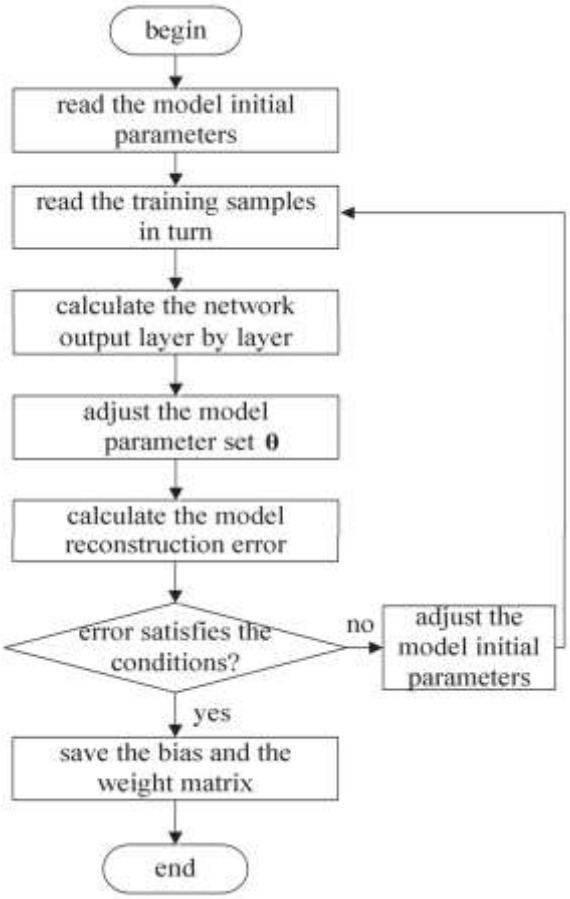

Figure 1. The flow chart of model training

Through the training of the model, the system constructs the probability characteristics of different network behaviors and is established in the form of parameters. Set a = BC to establish a network behavior profile; The intrusion detection process deviates from the normal sequence or the degree of similarity based on the observed sequence. The test process is shown in Fig. 2.

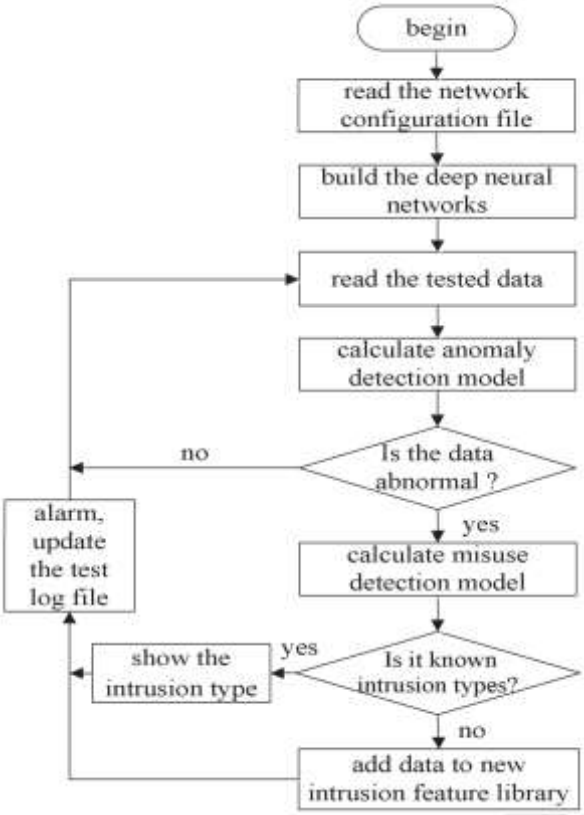

Figure 2. The flow chart of intrusion detection

Experiments and Results

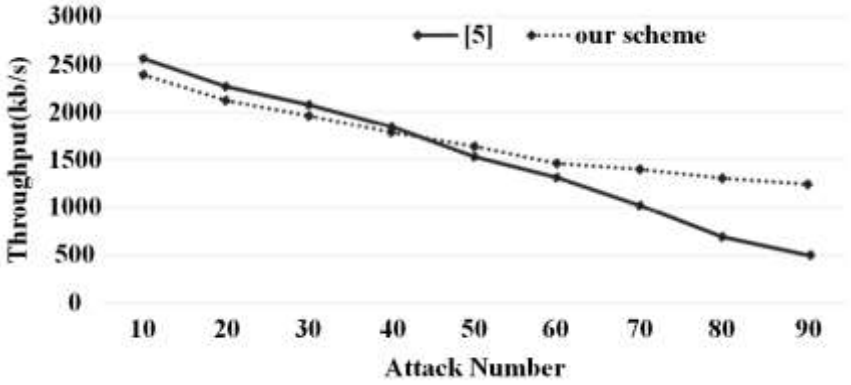

Figure 3. Attack Number VS Throughput

The experiment environment is Windows 7 operating system. The scheme is realized by VC programming. In order to verify the effectiveness of the proposed method, we also carry out simulation experiment for intrusion detection method based on BP neural network. BP neural network is a well applied and tested machine learning method in intrusion detection system. We compare the test results of two methods, and the results are shown in Fig. 3.

As can be seen from the results, the presented method is better than that of [5], and this shows that the intrusion detection method based on Self-learning method and game theory is more effective than traditional method.

Conclusion

In this paper, the equilibrium situation of the game is analyzed, and the strategy income quantification method is improved based on the counterattack return and attack success rate. Based on the analysis of

mixed strategy, this paper proposes an intrusion detection training model based on learning characteristics. Experimental analysis shows the rationality and validity of the model and method in attack prediction and detection.

References

[1] Y. Wang, Y.M. Wu, F. Li, et al. Correlation analysis and identification of unknown protocols for bitstream data. Computer application research, 2015,32(1):243-248.

[2] S A Zonouz, H Khurana, W H Sanders. RRE: A Game-Theoretic Intrusion Response and Recovery Engine. Parallel and Distributed Systems, IEEE Transactions. 2014, 25(2), 395 – 406

[3] X.N. Liang, Y. Xiao. Game Theory for Network Security. Communications Surveys & Tutorials, IEEE Volume: 15, Issue: 1. 2013, 472- 486

[4] K Lye, J Wing. Game Strategies in Network Security. International Journal of Information Security, 2005, 4(1-2):71-82

[5] J Xu, W Lee. Sustaining availability of Web services under distributed denial of service attacks. IEEE Transactions on Computers, 2003, 52(4):195-208

[6] H Larochelle, Y Bengio, J Louradour , et al. Exploring Strategies for Training Deep Neural Networks. Journal of Machine Learning Research, 2009, 10(6):1-40.

[7] C.L. Wang, Q. Miao, Y.Q. Dai. Network Survivability Analysis Based on Stochastic Game Model. Multimedia Information Networking and Security. 2012, 99 -104.

[8] Y. Min, C. Liu, X.L. Qiu, Shuang Zhao. Modelling and analysis of phishing attack using Stochastic Game Nets. Cyberspace Technology (CCT 2013). 2013, 300-305.

[9] T Wang, L Wei, J Ai. Improved BP Neural Network for Intrusion Detection Based on AFSA. 2015 International Symposium on Computers & Informatics. Atlantis Press, 2015.

[10] L. Deng, D. Yu. Deep learning for signal and information processing. Microsoft Research Monograph, 2013.

[11] M. Mohi, A. Movaghar, P.M. Zadeh. A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks. Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on Volume: 3. 2010, 639-643.

[12] G.Z. Zheng, S.Y. Liu, X.G. Qi. Clustering routing algorithm of wireless sensor networks based on Bayesian game. Systems Engineering and Electronics. 2012, 23(1), 154 -159

[13] K. Akkarajitsakul, E. Hossain, D. Niyato. Distributed resource allocation in wireless networks under uncertainty and application of Bayesian game. Communications Magazine, IEEE Volume: 49 , Issue: 8, 2011, 120-127

[14] Y. Zeng, G.W. E, Y.L. Guan. Distributed power allocation for network MIMO with a Bayesian game-theoretic approach. Information, Communications and Signal Processing (ICICS) 2011 8th International Conference on Digital Object Identifie. 2011, 1-5.