Overview on MTD technology based on game theory

Yan Sun*, Weifeng Ji, Jiang Weng and Beiying Zhao

Air Force Engineering University, Xi 'an, Shanxi Province, China

Keywords: Network space security, MTD, Signal game, Markov game, Differential game, Evolutionary game, Network defense decision.

Abstract. Mobile target defense (MTD) is a research hotspot in the field of network security. The decision method of network defense based on game theory is an important technique to guide MTD to make the optimal defense behavior in different network environments (GT-MTD). A lot of related work has been put forward in this field. In this paper, we focus on the scope and field of GT-MTD, systematically introduce the application scenarios of MTD in combination with four different game theory models of classical games (static games, signal games), Markov games, differential games or evolutionary games, and put forward the future development direction. There are some new views and explanations on the research of GT-MTD.

1 Introduction

In recent years, the number of global cybersecurity incidents has increased year by year, and the impact has become increasingly serious. In 2011, RSA data breach and CSDN password breach; In June 2013, Snowden revealed the "prism" program, revealing that the United States used its technical advantages to conduct large-scale Internet surveillance. In December 2015, Ukrainian electronics company equipment was hacked, resulting in a massive power outage and causing great public panic.

Researchers have carried out a lot of research in the field of traditional network defense and improved network defense by establishing firewalls, intrusion detection, identity authentication, anti-virus software, vulnerability repair, and other measures. However, the existing system is difficult to effectively deal with the constantly developing network attack means, which are shown as follows:

Static defense is difficult to deal with high-intensity network attack;

Passive security strategy is difficult to deal with new network attack methods;

Software and hardware design vulnerabilities cannot be avoided.

cyberspace confrontation for a long time, forming an asymmetric situation of "small attack, big defense, and one attack, global defense"[1]. The national science and technology council of the United States (NITRD) issued "trusted networks: federal strategic planning for

* Corresponding author: 1776797737@qq.com

cybersecurity research and development"[2], proposing the development of a series of "game-changing" revolutionary cybersecurity defense technologies. MTD aims to change the situation of extreme asymmetry between attack and defense, build a dynamic, random and polymorphic active defense mechanism, limit the exposure of network vulnerability, improve the complexity and cost of a network attack, and thus reduce the success rate of attack.

In MTD technology, using game theory to guide MTD decision-making can maximize the effect of MTD and minimize the cost. The paper is organized as follows. In the second part, background knowledge about GT-MTD is discussed. In the third part, the representative progress of the latest GT-MTD is introduced from the classical game model, Markov game model, differential game model, and evolutionary game model. The fourth part sorts out the whole text and puts forward the prospect of the future direction and conclude.

2 Background

Given MTD technology, the traditional network defense decision-making method is seriously deficient in science and accuracy. Game theory[3] is a theory that studies how to make decisions when the behaviors of decision-making subjects interact directly with each other. Among them, MTD game refers to the process in which network defenders have different defense strategies and network attackers have different attack strategies. Attackers attack the information system by selecting corresponding attack measures. The defender takes a series of defensive actions against the attack on the network system to minimize the possible loss of the attacker. The process of network attack and defense confrontation has the following characteristics: Object opposition; Strategic dependence; Relationships are not cooperative

According to the above analysis, game theory and MTD have very similar characteristics. Therefore, the exploration of network security analysis methods and defense technology systems based on game theory has important practical significance and has become the focus of research in recent years.

3 Taxonomy of MTD technology based on game theory and overview of typical studies

According to the existing literature on game theory that has contributed to MTD, we divide it into four categories according to different game theory models: classical game model (static game, signal game), Markov game model, differential game model and evolutionary game model.

3.1 Classical game model

Liu et al.[4] studied the existence of Bayesian Nash equilibrium by using Bayesian game theory to analyze the intrusion detection of mobile ad-hoc network. Otrok et al.[5] also proposed a cooperative game model to analyze the interaction behavior of inspectors and reduce the false alarm rate for the intrusion detection failure of mobile ad-hoc network nodes. Taking worm design and data transmission as examples, Gueye et al.[6] introduced the game relationship between worm designer, data tamper and defender in detail. Sallhammar et al.[7] used game theory to model and calculate attack probability when quantifying security stochastic model. Shi J et al.[8] proposed a DIRBGT model of dynamic intrusion response based on game theory, which effectively improved the accuracy and effect of alarm response.

LIN et al.[9] introduced a dynamic game model and transformed the network attack and defense graph into a network game tree through "virtual node", which was used to study

strategy selection in active defense. BURKE D et al.[10] used incomplete information repetition game to model the behavior of participants in information war. LIU Y L[11] applied the static game model with incomplete information to the performance evaluation of worm attack and defense strategies. GAO X et al. [12] used the signal game model to analyze the defense mechanism of DDoS attack and give the principles of defense strategy selection. According to information confidentiality, LIN J Q et al.[13] used signal game model to model attack and defense scenarios, analyzed factors that affect the benefits of attack and defense parties, and gave defense Suggestions. ZHANG H W et al. [14] studied offensive and defensive behaviors from the perspective of dynamic confrontation and limited information. Based on the signal game equilibrium analysis, the optimal defense strategy selection algorithm is designed. Such as JIANG L[15] from the Angle of attack surface conversion and detection surface extension defined defense strategy, for the limited information in the process of dynamic defense enhance efficiency provides the model of moving targets defense. ZHANG [16] put forward a signaling game model in the APT attacks, APT to attack and defense both sides in the behavior of the antagonism between the abstract for the incomplete information and dynamic game process, there is information transmission.

3.2 Markov game model

Chowdhary A et al.[17], considering the heterogeneity of interactive network devices and applications in the cloud network, proposed A zero sum Markov game, which provided an intelligent strategy to place the detection mechanism to maximize the detection of vulnerabilities while considering the impact on the performance of the cloud network. Zhou Y et al.[18] used multi-target Markov decision process to model the interaction between attacker and defender, and designed an effective DDoS attack defense scheme based on moving target transformation. Maleki et al.[19] proposed an MTD game model based on Markov decision process. Markov game model is used to compare the single - target IP jump and multi - target IP jump. The results show that multi-element selection can effectively improve the efficiency of jump defense.

Zhang et al.[20] analyzed the influence of vulnerability relationship and player strategy on network system security based on Markov game model. It improves the defense efficiency by searching the node or path with the greatest threat in the target network. Lei et al.[21] proposed an optimal strategy selection method based on the complete Markov game model. The exploitation of network vulnerability is abstracted as the change of attack surface and detection surface to ensure the universality of the model. Lei et al proposed an incomplete information Markov game theory method IIMG-MTD[22] on the basis of reference [21]. Markov decision process was used to describe the transition between network states in the realization process of MTD, and the development of network resources was transformed into mobile attack surface and mobile detection surface.

3.3 Differential game model

HUANG, et al.[23] through analyzing the process of continuous time of network attack and defense, in order to meet the needs threat warning, put forward the network attack and defense of qualitative differential game model, construct defense grid partition capture area and avoid area, the introduction of multidimensional space Euclidean distance evaluation threat level, determine the safety status of threat warning level and put forward pertinence suggestion according to the warning level of network defense. ZHANG et al.[24] analyzed and studied the network attack and defense behavior in the continuous process, constructed the differential game model of attack and defense, and on this basis, proposed the solution method

of saddle point strategy and the selection algorithm of optimal defense strategy. On the basis of reference [23] and reference [24], ZHANG et al.[25], for the first time, based on the differential game theory and Markov decision-making method, transformed the network attack-defense confrontation in a certain period of time into a multi-stage continuous attack-defense process with short duration in each stage, and constructed the Markov attack-defense differential game model for research. Guo R et al.[26] advocate that defenders should take active actions to prevent DDoS attacks. A new model based on differential game theory is proposed. These include four main roles: attacker, defender, victim, and botnet. The model indicates the minimum number of Bots that should blocked by Defender. A Differential Games model is used to determine how a Defender combats an Attacker and protect the servers.

Yang L X et al.[27] discussed the problem of APT repair, that is, how to reasonably allocate available repair resources to potentially insecure hosts to mitigate potential losses of the organization. Based on a new expected state evolution model, APT response problem is modeled as a differential Nash game problem (APT repair game). This paper proposes an algorithm for searching APT and repairing potential Nash equilibrium of game. Li et al.[28] discussed how to find an effective dynamic recovery (DR) strategy to mitigate the total loss of cloud defenders in APT campaigns, which we call the dynamic cloud storage recovery (DCSR) problem. Based on the expected state evolution model, the net gain of APT attackers and the total loss of cloud defenders are measured.

3.4 Evolutionary game

Sun wei et al.[29] applied evolutionary game theory to network information security, established an information security attack and defense game model based on evolutionary game, and studied the dynamic evolution process of network attack and defense confrontation by adopting replication dynamics. Zhu jianming et al.[30] built a network information security evaluation model based on game theory and studied the optimal configuration of information security. In addition, reference [31] combined with the actual situation of network attack and defense, the evolutionary game model of network attack and defense with learning mechanism was proposed, and the system dynamics was used to establish the evolutionary game model for simulation analysis.

D. Cheng[32] applied evolutionary game theory to the study of offensive and defensive costs, and analyzed the replication dynamics and evolutionary stability strategies of both offensive and defensive parties. Steven Tadelis[33] proposed the optimal control method of network performance based on evolutionary game, which can help network agents change their behaviors according to strategy information and strategy benefits, so as to achieve the goal of optimal overall network performance. WANG et al.[34] proposed a system and method to evaluate network group behavior and random evolution process. SHEN[35] analyzed the evolution trend of trust relationship between network nodes by applying the principle of replication dynamics.

Lye Kong wei[36] combined the randomness of state change in offensive and defensive system with Markov decision-making process to form a Markov stochastic evolution game model of multi-state and multi-agent. ZHANG et al.[37] analyzed the influence of various random interference factors on the selection and evolution of attack and defense strategies by establishing a game model of random attack and defense evolution based on Ito stochastic differential equation with reference to the concept of gaussian white noise. On the basis of reference [37], HUANG et al.[38] improved the traditional replication dynamic equation by introducing the incentive coefficient, indicating that strategies between consenting groups are interdependent and can promote or inhibit the convergence speed of game evolution. Alabdel

et al.[39] used evolutionary game to capture the long-term continuous behavior of APT on cloud storage devices and studied the dynamic stability of defense and attack strategy pairs according to the Dynamics criterion of replicator, so as to characterize the equilibrium strategy of local asymptotic stability. Qiu Y et al.[40] proposed a wireless sensor network active defense model with limited learning ability of node evolution based on evolutionary game theory. The node can adjust the defense strategy actively and dynamically according to the different strategies of the attacker to achieve the most effective defense.

3.5 Conclusion

In the above analysis, how to choose an appropriate strategy is a problem. The classical game model is suitable for the simple offensive and defensive process and short duration. Markov game is suitable for attack and defense with repetition, which needs to consider the influence of past behavior on present and future. Differential game is suitable for attack and defense with high frequency and real-time behavior. Evolutionary game is suitable for the situation where both sides of attack and defense do not have absolute rationality and search for the optimal behavior through trial and error.

4 Summary

Mobile target defense based on game theory has always been a hot topic in the field of cyberspace security. So far, the techniques known in game theory as cyber defense strategies have been developing rapidly, but some of them are too complex to be used on a large scale in real life. Therefore, it is necessary to improve the defense performance while simplifying the burden of the algorithm on the hardware and software, and meet the normal performance requirements of users with full group of security.

We provide an overview in this article. First, we discuss the background of MTD and GT-MTD. Then we systematically introduce the recent progress in the field of GT-MTD including four aspects: classical game model, Markov game model, differential game model and evolutionary game model. Finally, the research direction of this field is pointed out. We hope that this review will contribute to the further research on defense in the field of mobile target networks.

This research was financially supported by the National Science Foundation.

References

1. YANG l, YU Q. Dynamically-enabled Cyber Defense[M]. Beijing: The People's Posts and Telecommunications Publishing House, 2018:34-35
2. Baker S. Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program[R].
3. https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf, 2011.
4. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. W. Q. Wu. A survey of game theory as applied to network security[C]. in Proc. 2017 43rd Hawaii Int. Conf. Syst. Sci., 2017, pp. 1–10.
5. Y. Liu, C. Comaniciu, and H. Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. ACM International Conference Proceeding Series. 2006, 99

6. H. Otrok, N.Mohammed, L. Wang, M.Debbabi, P. Bhattacharya. A game-theoretic intrusion detection model for mobile ad hoc networks Computer Communications, 2008, 31(4),708~721
7. AssaneGueye, Jean C. Walrand. Security in Networks: A Game-Theoretic Approach. Proceedings of the 47th IEEE Conference on Decision and Control Cancun, Mexico. 2008, 829~834
8. Karin Sallhammar, Bjarne E. Helvik, Svein J. Knapskog. On stochastic modeling for integrated security and dependability evaluation. Journal of Networks, 2006, 1(5)
9. SHI J, LU Y, XIE L. Dynamic Intrusion Response Based on Game Theory. Journal of Computer Research and Development. 2008, 45 (5): 747~757.
10. LIN W Q, WANG H, LIU J H. Research on active defense technology in network security based on non-cooperative dynamic game theory [J]. Journal of Computer Research and Development, 2013, 48(2): 306-316.
11. BURKE D. Towards a game theory model of information warfare [D]. Montgomery: Air University, 2013.
12. LIU Y L, FENG D G, WU L H. Performance evaluation of worm attack and defense strategies based on static Bayesian game [J]. Journal of Software, 2013, 23(3): 712-723.
13. GAO X, ZHU Y F. DDoS defense menchanism analysis based on signaling game model[C]//The 5th International Conference on the Computer Security Institute. San Francisco, c2013: 414-417.
14. LIN J Q, LIU P, JING J W. Using signaling games to model the multi-step attack-defense scenarios on confidentiality[J]. Security Lecture Notes in Computer Science, 2014, 39(6): 118-137.
15. ZHANG H W, YU D K, HAN J H et al. Defense policies selection method based on attack-defense signaling game model [J]. Journal on Communications,2016(5):51-61.
16. JIANG L, ZHANG H W,WANG J D. Optimal strategy selection method for moving target defense based on signaling game[J]. Journal on Communications, 2019(6).
17. ZHANG H W, YANG H P. Defense Decision-Marking Method for Anti-apt Attack Based on Attack-Defense Signaling Game[J]. Computer Engineering and Design, 2019, 40(01):67-72.
18. Chowdhary A , Sengupta S , Huang D , et al. Markov Game Modeling of Moving Target Defense for Strategic Detection of Threats in Cloud Networks[J]. 2018.
19. Zhou Y, Guang C. A cost-effective shuffling method against DDoS attacks using Moving Target Defense[J]. 2019.
20. H. Maleki, S.Valizadeh,W.Koch, A. Bestavros, and M. van Dijk, ``Markov modeling of moving target defense games," Proc . ACMWorkshop Moving Target Defense (MTD), Oct. 2016, pp. 81_92
21. Z. Yong, T. Xiaobin, C. Xiaolin, et al., Network security situation awareness approach based on Markov game model, J. Softw. 22 (3) (2011) 495–508.
22. C. Lei, D.H. Ma, H.Q. Zhang, Optimal strategy selection for moving target defense based on Markov game, IEEE Access 1 (2017) 367–382.
23. Lei C , Zhang H Q , Wang L M , et al. Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense[J]. Computer Communications, 2018, 116:184-199.
24. HUANG S R, ZHANG H W, WANG J D, et al. Network security threat warning method based on qualitative differential game[J]. Journal on Communications, 2018(8):29-36.

25. ZHANG H W, LI T, HUANG S R. Network Defense Decision-Making Method Based on Attack-Defense Differential Game[J]. Acta Electronica Sinica, 2018, v.46;No.424(06):151-158.
26. ZHANG H W, HUANG S R. Markov Differential Game Model and Its Application in Network Security[J]. Acta Electronica Sinica, 2019, 47(3):606-612.
27. Guo R, Chang G, Qin Y, et al. Research on active defense strategy of counter DDoS attacks based on Differential Games Model[C]// International Workshop on Knowledge Discovery & Data Mining. 2008.
28. Yang L X , Li P , Zhang Y , et al. Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7):1713-1728.
29. LI P D,YANG, X F. On Dynamic Recovery of Cloud Storage System Under Advanced Persistent Threats. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2932020.
30. SUN W. Research on Attack and Deference in Information Security Based on Evolutionary Game [J]. Information Science, 2015, 23(9): 1408-1412.
31. ZHU J M. Evaluation Model of Information Security Technologies Based on Game Theoretic [J]. Chinese Journal of Computers, 2015, 5(4): 828-834.
32. ZHU J M, SONG B, HUANG Q F. Evolution game model of offense-defense for network security based on system dynamics [J]. Journal on Communications, 2014, 35(1): 54-61.
33. D. Cheng, F. He, H. Qi, and T. Xu, Modeling, nalysis and control of networked evolutionary games, IEEE Transactions on Automatic Control. 2015, 99(3): 41–49.
34. Steven Tadelis. Game Theory: An Introduction[M]. Princeton: Princeton University Press, 2014.
35. WANG Y Z, YU J Y, QIU W. et.al. Evolutionary Game Model and Analysis Methods for Network Group Behavior [J]. Chinese Journal of Computers. 2015, 38(2): 282-300.
36. Shigen Shen, Changyuan Jiang, Hua Jiang, et al. Evolutionary Game Based Dynamics of Trust Decision in WSNs[C]. 2016 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2016, 49–56.
37. Lye K W, Jeannette W. Markov Game strategies in network security [J]. International Journal of Information Security, 2008, 4(1): 71-86.
38. HUANG J M, ZHANG H W, WANG H J, et al. A Method for Selecting Defense Strategies Based on Stochastic Evolutionary Game Model[J]. Acta Electronica Sinica.
39. HUANG J M, ZHANG H W. Improving replicator dynamic evolutionary game model for selecting optimal defense strategies[J]. Journal on Communications,2018.
40. Alabdel Abass A A, Xiao L, Mandayam N B, et al. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage[J]. IEEE Access, 2017, 5:8482-8491.
41. Qiu Y , Chen Z , Xu L . Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory[C]// International Conference on Wireless Communications Networking & Mobile Computing. IEEE, 2010.