Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 1
AIEA 2023

Current Situation and Prospect of Game Theory based Network Security Methods

Wei Zhang [1, a, *], He Yang [2, b], Tengteng Zhao [1, c], Tingting Wang [1, d], Weili Ban [2, e], Zongliang Shen [3, f]

[1] Beijing Institute of Control and Electronics Technology, Beijing, China

[2] China Academy of Aerospace Science and industry, Beijing, China

[3] Beijing University of Posts and Telecommunications, Beijing, China

[a, *] ychcqshan@163.com, [b] 2439642332@qq.com, [c] 728777331@qq.com, [d] 1363257037@qq.com, [e] 1151312337@qq.com, [f] shenzongliang@bupt.edu.cn

* Corresponding Author: Wei Zhang

Abstract. The attack and defense model of network security based on game theory has developed into an effective network security model. It is a hot topic in the field of network and information security to use the idea of game theory to attack and defend the network security. This paper analyzes the general model of game theory in the field of security. This paper also analyzes the general model of network security attack and defense game. This paper also analyzes the game theory model of cryptographic protocol. This paper studies the existing network security methods based on game theory, reviews the development and evolution process and technical core of network security based on game theory, and compares the specificity of network security models based on game theory. Finally, the paper discusses the problems in the field of network security based on game theory, and tries to forecast its future development trend.

Keywords: Game Theory; Network Security; Offensive and Defensive Model.

1. Introduction

In recent years, network security theory and technology has developed rapidly, from the traditional research on encryption and decryption, anti-virus software, firewall, intrusion detection to intrusion tolerance, survivability, trusted computing, network security, from the focus on network confidentiality development to focus on network availability and service sustainability. From focusing on the solution of a single security problem to the study of the overall security status of the network and the trend of change. The field of network security has entered the information security guarantee era with three-dimensional defense and in-depth defense as the core ideas, forming the whole life cycle security management with early warning, attack protection, response and recovery as the main characteristics, and many new research contents such as large-scale network attack and protection, Internet security supervision and so on. Network security management has also developed from information security product assessment to overall risk assessment and level protection of large-scale information systems [4].

For network security, network security technology is undoubtedly the most important. Many even believe that the network security problem can be solved with good enough access control mechanisms, formalized cryptographic protocols, effective firewalls, and better detection of intrusions and malicious code [1]. As a matter of fact, any technology is a "double-edged sword", which can be used for both defense and attack. One day a security hole is fixed, the next day an attacker finds a new one. , on the other hand, an ideal defense system should be on all the weaknesses or attack protection, but from the organization's resources limit the consideration of the actual situation such "at all costs" defense is obviously unreasonable, must be considered "safe" moderately, or consider investing in

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

the information security risk and seek a balance between, Limited resources should be used to make the most reasonable decision [15].

While significant advances in information technology and infrastructure have provided new opportunities, cyberspace is still far from completely secure. In many cases, the security solutions adopted are AD hoc and lack a quantitative decision-making framework. While they are effective at solving the specific problems they are designed for, they generally do not respond well in dynamically changing scenarios. Therefore, while attaching importance to the development of network security technology, more and more scholars pay attention to the strategic perspective and try to use economic methods to solve the problem of information security [12]. Game theory, as one of the important methods, has attracted more and more scholars' attention in the application of cyberspace security. This paper tries to review the application of game theory in network security attack and defense, cryptography and security technology configuration, and shows the basic status quo of using game theory tools to study the security problems in cyberspace and the main content of information security economics.

2. Technical Overview

2.1. Security Game Theory

Game theory is to study the behavior of decision-making body direct interaction occurs in the decision-making and the balance of this decision-making problem, is the study of competition participants to gain maximum benefit should be how to make a decision of mathematical method, is the study of decision-making behavior between more balance, and their interactions with a countermeasure to maximize profit or utility theory[18]. Game theory is a process of strategy and decision making. Security game process refers to the process of strategy deployment and decision making in the face of threats in order to maintain the soundness of social, enterprise and individual resources.

In the process of human production, safety is to control the operation of the whole project may cause potential damage to human life, property and environment. Safety problems widely exist in traffic safety, food safety, electrical safety, fire safety, information safety and other fields, is closely related to our life. With the rapid development of economy, science and technology, engineering construction and other aspects, many industries have appeared safety problems, by management practitioners and scholars attach great importance to. At the same time, also constantly put forward higher, newer, more stringent requirements for safety management personnel. Protecting critical public infrastructure and targets is a very challenging task for security agencies in modern societies. For example, security agencies need to protect public transport networks and passengers from terrorist attacks and other sabotage; And to stop the illegal flow of drugs, weapons, and money between countries; There is also a need to protect rare animals and natural resources from illegal hunting, fishing and deforestation. With the development of the network society, security departments need to detect and contain network attacks in time to maintain the security of network system resources[19]. The system based on security game theory has been successfully applied in many network security fields, such as network resource allocation, network attack and defense scheduling, network administrator scheduling, information resource permission optimization, etc.

The classic Stackelberg game is a two-player game consisting of a leader and a follower [14]. The following, we give a general definition of Stackelberg game. The leader (protector/security department) is denoted by θ, the follower (attacker) is denoted by ψ. Each player has a pure strategy set, The leader's pure policy set is represented by $\sum \theta = \{\theta 1, \ldots, \theta_{\sum \theta}\}$, The pure policy set of the follower is represented by $\sum \psi = \{\psi 1, \ldots, \psi_{\sum \psi}\}$. A mixed strategy is a probability distribution defined on a set of pure strategies for the participants, $\mathrm{x} \in \mathrm{X}$ is the leader's mixed strategy, $\mathrm{q} \in \mathrm{Q}$ represents the follower's mixed strategy. Here, $\mathrm{x}_i \in [0, 1]$ is the probability that the leader uses pure strategy $\theta_i \in \sum \theta$, A similar, $\mathrm{q}_i \in [0, 1]$ is the follower's probability of using pure strategy $\psi_i \in$

$\sum \psi$. We use Sθ to represent the index set of the leader pure strategy, and SΨ to represent the index set of the follower pure strategy. For all possible pure strategy combinations, the returns of leaders and followers are defined as:

$$\Omega\Theta : \sum \theta \times \sum \psi \rightarrow \mathrm{R} \tag{1}$$

$$\Omega\psi : \sum \Psi \times \sum \Theta \rightarrow \mathrm{R} \tag{2}$$

Given the leader's mixed strategy $x \in X$ and the follower's mixed strategy $q \in Q$, the return function of the above pure strategy can be extended to the form of mixed strategy, which can be defined as:

$$\Omega_{\theta}(x,q) = \sum_{i\in S_{\theta}} \sum_{j\in S_{\psi}} \Omega_{\theta}(\theta_i,\psi_j) \cdot x_i \cdot q_j \tag{3}$$

$$\Omega_{\psi}(x,q) = \sum_{i\in S_{\theta}} \sum_{j\in S_{\psi}} \Omega_{\psi}(\theta_i,\psi_j) \cdot x_i \cdot q_j \tag{4}$$

2.2. Game Theory of Network Security

The game theory of network security is an application classification of the game theory in network security. The game theory has been applied in many network security scenarios such as attack defense interaction and network data encryption [20].

Research on the offensive and defensive game of network users usually requires the assumption that users are selfish. Attackers exploit security vulnerabilities and harm the interests of other users to improve their own utility. These attackers may be motivated by financial gain, peer recognition or to satisfy their curiosity. An attacker may choose to attack the entire network or a few terminal nodes. In short, users cannot trust other network participants. Generally speaking, the network security offense and defense game can be expressed in a form similar to (S, A^1, A^2, Q,R^1,R^2,β) [9]. Where, S is the state set, A^1 and A^2 are the action sets of the attacker and the defender respectively, Q is the state transfer function, R^1 and R^2 are the payment of the attacker and the defender respectively, and β is the discount rate of payment [22]. At present, the use of game theory to depict the network security attack and defense interaction has been paid attention to by many scholars.

Game theory analysis of cryptographic protocols is also an important part of network security game theory. Traditional cryptographic protocols assume that participants are either honest or malicious. The honest participants always abide by the agreement in the communication process, while the evil participants always use various means to cheat other participants and violate the agreement. The idea of game theory is that all players are rational, maximizing their own interests[23]. In contrast, cryptography does not exclude irrational behavior. The application of game theory in cryptographic protocols is mainly embodied in secret sharing and secure multi-party computing[24]. The typical secret sharing problem is that secret shares are distributed to participants and only a certain number of participants can reconstruct the secret[25]. In the secure multi-party computing problem, participants can only accept their own private input and cannot obtain any additional information from others' input.

3. Research Status of Network Security Game Theory

In 2004, A. Patcha et al. proposed A game theory method for modeling intrusion detection in mobile AD hoc networks [10]. This method is a game theory method to analyze intrusion detection in mobile AD hoc networks. The method uses game theory to simulate the interaction between nodes in an AD hoc network. We regard the interaction between the attacker and a single node as a two-person non-cooperative game, and construct a model for this game [11].

In 2012, Bursztein et al. [3] proposed a model to assess the likelihood of a successful attack on a given network with interdependent files and services. This work provides a logical model that takes into account the time required to attack, crash, or patch a network system. Instead of providing a game theory model, the work uses given times and topological constraints to determine whether an attack or defense will succeed. The provided example describes a highly available Web server configuration with interdependent elements and considers the strategic actions of both attackers and defenders.

In 2013, Quanyan Zhu et al. [10] made a structured and comprehensive overview of security and privacy research in computer and communication networks using game theory from six levels of investigation: security at physical layer and MAC layer, security of self-organizing network, intrusion detection system, anonymity and privacy, network security economics and cryptography. The survey could also help researchers from a variety of fields develop game theory solutions to current and emerging security problems in computer networks. Branislav Bosansky et al. [2] studied an iterative algorithm for calculating accurate Nash equilibrium in two-person zero-sum extended form games with imperfect information. The method uses the sequential form representation of extended form game and the double predictor algorithm framework. The main idea is to limit the game by allowing the player to play only a few available action sequences, then iteratively solve the restricted game, and add additional sequences to the restricted game for the next iteration using a fast best response algorithm.

In 2015, Christopher Kiekintveld[6] modeled the strategic use of deception and information manipulation. They described several game models that addressed honeypot deployment strategies, including a basic honeypot selection game, and ended up with a version that used attack graphs to represent attacker strategies. They also discuss the strengths and limitations of game theory in the context of cybersecurity.

In 2016, Wang Yong [16] studied a network security situation prediction model based on Markov game theory. Firstly, a network security situation prediction model is constructed based on coarse granularity processing. Secondly, the network security situation prediction model based on Markov game theory is established, and the basic flow of network security situation prediction is established. Finally, the simulation of network security situation based on Markov game shows that Markov game theory is an effective method to predict network security situation.

In 2017, Quanyan Zhu et al. [5] strategically approached the attacker by using cyber deception techniques and influenced his behavior by creating and enhancing his view of the computer system. They applied cyber spoofing techniques to the field of cyber security and studied the effect of deception on the attacker's beliefs using a quantitative framework of game theory.

Table 1. Research Timeline

Year	Method	Features
2004	Game theory model	Modeling intrusion detection in mobile AD hoc networks
2012	Game theory model	The model takes into account the time required to attack, crash or patch a network system.
2013	Game theory iterative algorithms	The method uses the sequential form representation of extended form game and the double predictor algorithm framework.
2015	Game theory model	Model the strategic use of deception and information manipulation.
2016	Game theory model	A network security situation prediction model based on Markov game theory.
2017	A quantitative framework for game theory	Network spoofing technology is applied to network security
2019	Game theory model	Game theory solves common problems in blockchain networks
2020	Combining cryptography with game theory	Solve the security problem of wireless sensor network
2021	Game theory model	Effectively generate the optimal attack and defense strategy

In 2019, Ziyao Liu et al. [17] proposed a game model for common problems in blockchain networks, such as selfish mining, majority attacks, and denial of service (DoS) attacks, issues related to mining management, such as computing power allocation, reward allocation, and mining pool selection, as well as issues related to blockchain economics and energy transactions.

In 2020, Hanane Saidi et al. [8] studied the application of game theory in solving security problems in wireless sensor networks. They propose three techniques to protect WSN from malicious nodes, cryptography, trust-based approaches, and game theory. Finally, they suggest a combination of cryptography and game theory for greater privacy and security.

In 2021, Fei Liu et al. [7] analyzed the establishment of game model and strategy selection in the process of offense-defense confrontation in network security. They set up a new network attack and defense game model; The components of the model are analyzed. Finally, the optimal defense strategy is obtained by solving the Nash equilibrium of the mixed strategy. Their simulation results show that the method can find the optimal offense-defense strategy {a3, d4} in complex mixed strategies. The calculation of income verifies the correctness of the strategy. The experimental results show that the application of attack-defense antagonism in the field of network security is feasible, and it can effectively generate the optimal attack-defense strategy to achieve network security.

4. Further Direction

In network security game theory, the fusion mode of multiple technologies has become the mainstream, as one of the most important branches: network attack and defense game model, which is based on the combination of network attack technology and network defense technology. Attack modeling is also one of the most important aspects, which is often used in conjunction with network defense technologies. Therefore, we can improve the combination of network attack technology and network defense technology. For example, simulated attack drills are used to improve the security of the defense model, and attack behaviors can be automatically identified and responded to. Therefore, it is the future trend to use attack and defense simulation to improve network security game, and constantly update new attack means and coping strategies in the model, especially in the network system with the increase of network resource content.

In addition, the application of offensive and defensive game to new fields, such as blockchain system, Internet of vehicles system, is also a development direction. Develop specific game models for attack and defense to deal with specific scenarios.

Network security game has been studied a lot and has a lot of development potential. However, it must be admitted that network security game technology is facing many shortcomings and challenges.

First of all, in many cases, the network security game is still not comprehensive. For example, for some large network systems, the attack and defense game model still cannot make correct decisions on all network attacks, and network security incidents still occur from time to time.

Second, the cybersecurity game is expensive. Network security game model needs to consume a lot of computing resources for attack behavior identification or attack log analysis.

To sum up, its development direction can be divided into three categories: improving the combination of network attack technology and network defense technology; Improve the efficiency of network attack and defense game or reduce the cost of resources; Apply the network attack and defense game to a new field.

5. Conclusion

Since the network security technology based on game theory was put forward, it has experienced many developments. First, the technology has been formally proposed for widespread use in the field of network system security. Many network attack and defense game models have been put forward and network security technology based on game theory has been widely used in various network environments. A large number of researchers began to pay attention to this kind of research. Network security technology based on game theory has become one of the most important branches of game theory. With the development of network technology, network security technology based on game theory will also have a lasting development.

References

[1] R. Anderson. Why information security is hard - an economic perspective. Seventeenth Annual Computer Security Applications Conference, pages 358–365, 2001.

[2] Branislav Bosansky, Christopher Kiekintveld, Viliam Lisy, Jiri Cermak, and Michal Pechoucek. Double-oracle algorithm for computing an exact nash equilibrium in zero-sum extensive-form games. International Conference on Autonomous Agents and Multi-agent Systems, 2013.

[3] E. Bursztein and J. Goubault-Larrecq. A logical framework for evaluating network resilience against faults and attacks. Annual Asian Computing Science Conference, 2007.

[4] Deng-Guo Feng, Min Zhang, Yan Zhang, and Zhen Xu. Study on cloud computing security. Journal of Software, 22:71–83, 01 2011.

[5] K Horák, Q. Zhu, and Branislav Boansk. Manipulating adversary's belief: A dynamic game approach to deception by design for proactive network security. International Conference on Decision and Game Theory for Security, 2017.

[6] C. Kiekintveld, Viliam Lis, and R Píbil. Game-theoretic foundations for the strategic use of honeypots in network security. Springer International Publishing, 2015.

[7] Fei Liu, Hongyan Gao, and Zegang Wei. Research on the game of network security attack-defense confrontation through the optimal defense strategy. Security and Privacy, 2021.

[8] H. Saidi, D. Gretete, and A. Addaim. Game Theory for Wireless Sensor Network Security. Fourth International Congress on Information and Communication Technology, 2020.

[9] K. W. Lye and J. M. Wing. Game strategies in network security. International Journal of Information Security, 4(1-2):71–86, 2005.

[10] M. H. Manshaei and Q Zhu. Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 2013.

[11] Patcha and J. M. Park. A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. Information Assurance Workshop, 2005. 1

[12] S. Shiva, Sankardas Roy, and Dipankar Dasgupta. Game theory for cyber security. 04 2010.

[13] Jason Tsai, Shyamsunder Rathi, Christopher Kiekintveld, Fernando Ordóñez, and Milind Tambe. Iris – a tool for strategic security allocation in transportation networks, 2009.

[14] von Stackelberg. Marktform und gleichgewicht. New York:Springer, 1934.

[15] Jiang Wei, Fang Binxing, Tian Zhihong, and Zhang Hongli. Network security evaluation and optimal active defense based on offense and defense game model. chinese computer science, 32(004):817–827, 2009.

[16] W. Yong. Research on network security situation prediction based on markov game theory. International Journal of Security and Its Applications, 10(9):301–308, 2016.

[17] Nguyen Cong Luong Ziyao Liu. A survey on applications of game theory in blockchain. 2019.

[18] EC Amadi, G Eheduru, F Ezea, and C Ikerionwu. Game theory application in cyber security. IEEE 3rd international conference on electrotechnology for national development (NIGERCON), 2017.

[19] Dipak V Bhosale, Prajakta K Mitkal, and Yogesh S Lonkar. Cybersecurity using game theory. International Journal of Innovative Science, Engineering & Technology, 3(1):505–509, 2016.

[20] Robert Gibbons et al. A primer in game theory. 1992.

[21] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 45(3):1–39, 2013.

[22] Roger B Myerson. Game theory. Harvard university press, 2013.

[23] Steven Tadelis. Game theory: an introduction. Princeton university press, 2013.

[24] Lin Wangqun, Wang Hui, Liu Jiahong, Deng Lei, Li Aiping, Wu Quanyuan, and Jia Yan. Research on active defense technology in network security based on non-cooperative dynamic game theory. Journal of computer research and development, 48(2):306, 2011.

[25] Quanyan Zhu and Stefan Rass. Game theory meets network security: A tutorial. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 2163–2165, 2018.