ISSN 2959-6122

Adversarial Models and Game Theoretic Logic Related to Online Security

Yuexiao Chen[1, *]

[1]Shenzhen Foreign Language School, 2005 Hongli Road, Futian District, Shenzhen, Guangdong Province, China
*Corresponding author: Dawangbi02@gmail.com

Abstract:

As the percentage of online activities in people's daily lives increases, the importance of protecting users' information from online attackers is getting more concerned. This article is going to explore the possibility of the approach that game theory is used as a framework of adversarial models by analyzing and contrasting the mechanism of three different types of adversarial, designing game theory models to simulate those adversaries, and thinking about the challenges and limitation of the approach the article is talking about. With those steps being carried out, it is feasible to apply game theory to simulate the actions of adversaries and security keepers. However, game theory is still limited in some fields, including simulating a passive adversary's usual behaviors that lack interaction and simulating counteraction, including a large number of participants. To summarize, by testing and analyzing the game theory model that simulates adversaries, it can improve or design protocols to ensure online security.

Keywords: Adversarial Model; Game Theoretic Logic; Online Security.

1. Introduction

Cryptography is constructing and analyzing protocols that prevent third parties or the public from reading private messages [1]. A protocol (or scheme) specifies each party‘s algorithm. It gives some guarantees to each party that follows its algorithm — even if the other parties do not fully follow their instructions. A party is honest if it follows the protocol instructions. Therefore, Cryptography is a game between adversaries and challengers, the two crucial participants who follow the rules and use strategies to win. In such a game, the adversary intends to break the cryptosystem, which means defeating any information protection.

There is not only one type of adversarial model: a formalization of an attacker in a computer or networked system. Depending on how complete this formalization is, the adversary may be an algorithm or simply be a series of statements regarding capabilities and goals. Adversaries can be passive, active, or adaptive. Underlying the models of those adversaries, the logic is similar to the logic of game theory, which is formally a branch of mathematics developed for conflict of interest situations in social science. In a game theory model, participants act with their own goals and use strategies to make decisions while maintaining the game‘s equilibrium. Game theory emerged as a unique field when John von Neumann published On the Theory of Games of Strategy in 1928 [2]. When game theorists use the word "game," they are referring to any social situation involving two or more actors(players) in which the interests of the players are interconnected or interdependent [3]. This leads to the serious consideration of players‘ strategies and decision-making. Throughout the centuries, game theory has had applications in many social science fields, and it has been used extensively in economics, logic, systems science, and computer science [4].

Recently, Game theory has become increasingly important in logic and computer science, which are related to the topic of this article. Several logical theories have a basis in game semantics. In addition, computer scientists have used games to model interactive computations. It is important to note that some cryptographic models involving adversaries were constructed using game theory.

Nowadays, most people‘s daily lives and the digital world are inseparable. For example, online payments, during which users‘ sensitive financial information like credit card numbers and account details are protected from those „cryptosystem breakers“. Safeties of online activities like signing digital signatures and using VPNs are also closely relevant to preventing adversaries‘ attacks. In that case, understanding how adversaries work is crucial for figuring out how to keep civilians‘ privacy safe. To achieve this, the article will mainly discuss the game-theoretical logic underlying the several types of adversarial models

in cryptography. In addition, it will explore how game theory secures secrets in different ways while facing the challenge of adversaries.

2. Types of Adversarial Models

2.1 Passive Models

The passive adversarial model is the weakest among all the adversarial models, where the adversary is a legitimate entity and follows the specified protocol but can read all the transmitting information between the corrupted entities [5]. Simply put, a passive adversary is like an eavesdropper who quietly listens to the conversation between two parties. Game theory is useful in demonstrating this kind of adversary‘s strategies. The following setup of a passive model illustrates why it is.

First and foremost, game theory is used to make the regulation the „game.“ A secret keeper(sender) encrypts the information into ciphertext and sends it to a server. Then, a passive adversary tries to decrypt the information without being detected. After understanding the rule, two participants need to learn the evaluation of their game. In game theory models, outcomes are assigned values. In this passive adversarial model, when the secret keeper protects the information from being read, he gets a higher score. If the adversary successfully decrypts the information, he gets a higher score. To win the game, the two participants start to use strategies. The secret keeper will choose a proper encryption, and the adversary will decide when to eavesdrop. Daily, people frequently send and receive emails that include very important messages, such as personal and work information. Designing a competence protocol to protect email content from passive adversaries is quite crucial. A very important use of game theory is that the secret keeper can anticipate the adversary‘s move. Therefore, the secret keeper can adjust the playing methods by analyzing collected information of the adversary model built into game theory to make it more difficult for the opponent to succeed. In that case, game theory may be applied to design or improve cryptographic protocols to defend against passive adversaries‘ attacks in reality.

2.2 Active Models

Unlike passive adversarial models, the active model, known as the Byzantine adversary model, is the strongest among all the adversarial models, where the adversary hides in the network and reads all the transmitting information between the entities by making them corrupt and ultimately not following the defined protocol. These corrupted entities behave maliciously by sending falsified messages, eventually leading to false results in the protocol [5]. To be short, the difference between a passive attacker and an active attacker is that the latter interferes with the communication between the two parties.

Again, game theory can be used to build an active adversary model, in which there is a secret keeper who protects the information by encrypting it and an adversary who uses different methods such us Netscan, Cobalt Strike, and Remote Desktop Protocol to interrupt the system. The adversary Therefore, for an active adversary, winning the game means successfully controlling the system. For the secret keeper, to win a game means to use several highly credible approaches to defend the attacker. In real life, people have a large potential to meet this kind of adversary. For example, an active adversary attempts to steal or obtain a user‘s credentials online. They often trick the user into logging in on a fake website or page to steal the username and password. Protocols like two-factor authentication add an extra layer of security by requiring further verification, such as a code sent to the user‘s phone. With game theoretic logic, two participants can create a dynamic interaction between them, which means they can anticipate, counteract, and change strategies by learning from the previous games. This can be useful while facing an active adversary because the secret keeper will be more sophisticated after analyzing the attacker‘s tactics.

2.3 Adaptive Models

A very different characteristic of an adaptive adversary from a passive or active adversary is that it changes strategies in response to an opponent. This kind of adversary can be built into an adaptive model, a self-learning predictive model that uses machine learning to calculate propensity scores [5].

By using game theory, an adaptive model contains a secret keeper and an adversary who is sort of intelligent. In this game, the secret keeper is similar to his colleagues who appeared in the last two sections. He uses the key to encrypt the message to keep the truth from the adversary and may adjust his approaches based on the adversary‘s action. The adversary meant to decrypt the message by using strategies. Similarly, he can change how he uses it by looking at and analyzing the counteraction of the secret keeper. In that case, the stronger the encryption is, the more advantage the secret keeper has.

In contrast, if the adversary is more adaptive to the protocol, he has more advantage. In the last example of an active adversarial model, if an adaptive adversary tries to gain the user‘s credentials, it may attempt to use large sets of usernames and passwords that he used in the past. It can adjust the logging frequency to reduce the speculation from protocols and make it more challenging to find. The significance of game theory in an active model is that it allows two participants to modify their strategies by inter-

acting. The secret keeper will improve in his defense by analyzing the attacker‘s tactics and being good at dealing with unfriendly counteracting.

3. Challenges and Limitations

Game theory models can simulate adversarial models correspondingly. By analyzing the behaviors of the constructed adversary in the game and changing the strategies of the secret attacker, it is easier to design or improve protocols against real adversaries online. However, there are still some unsolved tricky problems and drawbacks of the approach that uses game theoretic logic as the framework of a specific adversarial model.

Those features are shown in 3.1, which talks about passive adversaries. In a classical passive model, the adversary barely interrupts the conversation between two parties. Nevertheless, a game theory model emphasizes the interaction of strategies and decision-making more. Therefore, a game theory model may not describe the behavior of a passive adversary well. To consider the challenges while dealing with passive adversaries, it is necessary to point out that this type of attacker seldom actively disrupts the system but silently steals and collects information. This leads to the problem of limited strategy options. With an active or adaptive model, the effective or new strategies will be more quickly figured out by gathering, learning, and analyzing the data of their attacks. But there is a little information about a strange passive adversary. If there is a lack of understanding about the opponent, the probability of winning is also subtle.

Another apparent limitation of the game-theoretic model is the limitation of players‘ participation, usually in a one-to-one or small group setting. In a real-world scenario of adversaries attacking, the interaction may not only be between one adversary and one user. For example, phishers try to trick users from being identified by online security measures [6]. Those phishers interact with the users whose personal information is sought by the phishers and service producers who help users filter useless or harmful information with potential security threats. Sometimes, the phishers also have to interact with security researchers who give suggestions on online security to organizations and individuals to protect themselves from phishing attacks. Therefore, to fully apply the game theory model to cryptography, more efforts should be made to improve the traditional game theory.

4. Conclusion

As the importance and urgency of keeping the security of online information is getting more attention these days, the study of how to prevent online attacks is getting diversified. Game theoretic logic is considered an approach to simulate various adversarial models, including the passive, active, and adaptive models. With different forms and mechanisms, the three adversarial models need different ways for the game theory model to be applied and perhaps give inspiration to improve protocols or to design a better one. A passive adversary lurks under the communication between two parties and seldom interrupts it. Game theory can model how the adversary decrypts messages using a certain strategy.

In contrast, an active adversary tries to disturb the communication. It may change the context of messages or deceive the users. Game theory can model the adversary by allowing it to create dynamic counteractions with a secret keeper. An adaptive adversary can learn and adapt to opponents’ behaviors. It is easy to use game theory to model these actions and analyze the playing of the adversary and the secret keeper.

Nevertheless, while constructing those models, some problems were revealed. It is shown that a traditional game theory model is not suitable for simulated action between a passive adversary and a secret keeper because the exchange of behaviors and strategies is not obvious in real attacks of a passive adversary. In addition, in many real examples, the number of attackers and types of defenders are varied. Traditional game theory models always contain one participant on each side or a small group of players with the same function. Therefore, it is tricky for a game theory model to simulate a complex scenario with multiple players.

References

[1]Bellare, Mihir; Rogaway, Phillip, “Introduction”. Introduction to Modern Cryptography. 2005 p. 10.

[2]Von Neumann, John Zur Theorie der Gesellschaftsspiele” [On the Theory of Games of Strategy]. Mathematische Annalen [Mathematical Annals] (in German). 1928, 100 (1): 295–320.

[3]Frank C. Zagare, Game Theory: Concepts and Applications, SAGE, 1984.

[4]Shapley, Lloyd S.; Shubik, Martin “Chapter 1, Introduction, The Use of Models”. Game Theory in Economics. Archived from the original on 23 April 2023. Retrieved 23 April 2023.

[5]Bhawna Narwal and Amar Kumar Mohapatra, “A Survey on Security and Authentication in Wireless Body Area Networks,” Journal of Systems Architecture, 2021, 113: 101883, https://doi.org/10.1016/j.sysarc.2020.101883.

[6]