International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 12987-12990

Applications of Game Theory for Cyber Security System: A Survey

Annapurna P Patil[1], Bharath S[2], Nagashree M Annigeri[3]

[1]Department of Computer Science and Engineering,
Ramaiah Institute of Technology, Bengaluru, Karnataka-560054, India.

Abstract

Cyber Security is a process designed to prevent the attacks on Computers connected to internet and the sensitive data present in it by unauthorized users. Cyber risks are evolving at quick rate along with the growth of cyber infrastructure. Traditional cyber security technologies focus only on well-known threats and are not well suitable for infrastructure with more network traffic. Game Theory helps to deal with the cyber security concerns in a better way than traditional approaches.

Keywords: Cyber security, cyber physical systems, game theory, cyber-attacks.

INTRODUCTION

Cyber security is the term used to collectively denote the technologies, processes and controls that are intended to protect systems, networks and data from cyber attackers. Cyber security is different from information security though in concepts there is a substantial overlap between both. The significant way in which cyber security differs from information security conceptually is that in cyber security denotes the security of other assets in addition to information security. This includes human factors such as humans as targets of cyber-attacks [1].

Game theory is a branch of applied mathematics which uses mathematical models that use the perception of rational decision makers (players) to find the best strategy that each player can adopt to win the game. There can be several numbers of players in the game whose decisions are not fixed. Decision of each player can affect the decision of others thereby affecting the outcome. Game theory studies the optimal decision making of independent players, whose interests may be similar, opposite or mixed.

Cyber security problems that require rational decision making can be solved in a better way using game theory. But game theory has a limitation if the defender is provided only with limited information on the opponent's strategy and decisions. Game theory enhances the ability to anticipate the actions of the hackers. To make game theory a practicable approach to solve cyber security issues strategies of hackers should be a finite and predictive set. Ideally it is very difficult to predict the strategies for both attacker and defender in real time.

In the recent times there has been more number of cyber-attacks. Game theory for Cyber Security is a promising research area. In this survey paper, an attempt is made to analyze the methods of game theory to anticipate the actions of the hackers based on different game models and security issues.

LITERATURE REVIEW

Internet has benefitted the life of people by its application in several areas such as business, entertainment, health care, education, e-commerce, banking etc. But it also has a drawback of very serious security issue due to cyber-attacks.

As we experienced there were few serious attacks in recent times where hackers invaded the sensitive data from the systems which are connected to the internet and demanded for Bitcoins to ensure the security and integrity of the invaded data. This is just an example of serious cyber security issues. Once the data has been invaded by the hackers they will complete control over the data. They can threaten the availability and confidentiality of the invaded data, which results in a compromise on the stored information [2].

For a small system which doesn't have any sensitive data it may not be a serious concern. But for the big organizations the sensitive data is a very serious concern. If the data is leaked to any other organization in this competitive world they may lose their business. Hence cyber security plays a massive role in defending the security threats.

Cyber security technologies which are dependent on Firewall, Intrusion detection and Antivirus software are called as traditional cyber security technologies. They are effective but can be applied only for specific type of attacks [2].There are few drawbacks in these traditional approaches, they lack in quantitative analysis and decision making. At the same time Hackers are becoming more intelligent and they use various intelligent approaches to invade the data.

The most important skill which is acknowledged by most of the researchers is "Adversarial Thinking" which is also defined as "think like a hacker". This can be used to avoid security threats to the system connected to internet. This skill is widely acknowledged because now a day's cyber security is dependent on guessing or analyzing the attacker's strategies [3].

Game theory and Cyber security share similar concerns in various aspects of their application. In which payoff with respect to players is not only contingent of the decision he made but it also depends upon the opponent's behavior. Based on this resemblance, we can use Game theory as a mathematical tool to deal with cyber security problems based on multi agent behaviors. Game theory in the field of cyber security is booming and many researchers are working on implementing the combination of Game theory and Cyber security for real time issues [3].

A. Aspects of Game Theory [4]:

Game theory is a tool which is used to study the situations such as competition and cooperation between the players involved in the game based on rational decision making. Whatever may be the situation and whatever may be the game, there exit a strategy to win a game for one particular player. These strategies are sometimes based on the decision of the opponent. Logical decision making can be harvested to its best by applying the concept of game theory.

If there are several players involved in the game then analyzing the strategies of each player and finding the best strategy for each player to win the game can be explained using game theory.

B. Components of Game Theory:

The components of game theory are players, strategies, actions and payoff functions [4].

Players: The individuals or entities, which make their own decisions with respect to game, are called as players. Each individuals or entities have their own goals and preferences. Entities may be humans, organizations or institutions; main aim of players is to select proper choice of action which results in maximizing his utility.

Actions: The decisions made by each player are called as actions. Decision is made in each move of the player. Game theory reckons that each player discerns the actions of all other players participating in the game.

Payoffs: It is defined as the amount of satisfaction each player gains from an advent. Based on the decisions made player gets the payoff, it may be positive or negative. Payoff of each player is known at the end of the game.

Strategies: With respect to past and expected actions of the opponent there will set of actions defined to each player to win the game. These set of actions are known as Strategies.

C. Classification of games:

Games can be classified into different categories based on perspectives. Below table shows the classification of games and the security concerns which are related to each classification [2].

TABLE I. GAME THEORETIC METHODS FOR CYBER SECURITY

Game Models			Application and Security Issues
Cooperative game models	Static game models		mobile ad hoc networks security
Non cooperative game models	Static game models		intrusion detection
			security investment optimization
	Dynamic game models	Complete information game models	security investment optimization
			security incentive mechanism
		Incomplete information game models	cyber attack-defence analysis

Co-operative games: The game in which all the players enforce cooperative behavior. These kind of games aren't between two individuals it is between coalitions of players.

Non Co-operative games: The game in which all the players exhibit selfish behavior. A player doesn't take the opponents into account. Main aim of all the players is to increase their payoffs.

Static Games: All the players involved in the game make one time decision at the beginning of the game. No player has any information about the behavior of the other player.

Dynamic Games: In contrast to Static Games each player in dynamic games will have some information about the behavior of other players and game is conducted in many stages. Based on the behavior of the opponent players will make their decisions.

Complete Information Games: All the players involved in the game will have complete knowledge about the behavior of the opponents. Each player is fully aware of the strategies of all other opponents.

Incomplete Information Games: Any one of the set of players playing the game will have zero information about the opponents. Results in player will not be able to make perfect strategy to win the game.

Perfect Information Games: A game in which each player knows all the past actions of the opponent before making his move.

Imperfect Information Games: A game which involves at least one player who does not know the previous actions of the opponent. It will be very difficult make a move if a player has no idea on the behavior of the opponent. Cyber Security is categorized under this type of game.

D. Game theory and Cyber Security:

Two broad categories of application of game theory in cyber security are:

1. The Cyber-Attack-Defense Analysis
2. The Cyber Security Assessment

By modeling the defense behaviors as games the actions of cyber attacker can be predicted in Cyber-Attack-Defense analysis. It also analyses the possible states of attack-defense equilibrium. The counter defense strategies can be determined ideally based on the state of equilibrium.

The equilibrium state of cyber-attack-defense can be scrutinized and the prognosis of the attack and defense strategies can be used as the rationalization of cyber security and assessment. Owing to the quantitative facets of game analysis security and reliability is viewed as a quantitative assessment which gives a computation of cyber security and reliability.

The classification of game theory methods in the field of cyber security has been classified as shown in the table [Table 1]. Cyber security adopts non cooperative dynamic game model. But in all the earlier researches all the non-cooperative

models were classified under static models. But the attacker strategies in Cyber-attacks are not static and to achieve ideal effect analysis of dynamic model is very crucial because dynamic models are very much closer to real to time cyber security issues. And for Cyber-defense analysis purpose incomplete information game model is used [4].

E. Game Theory Methods for Cyber Security Applications:

Game Theory for cyber security applications can be divided into six categories:

1. Physical Layer Security.
2. Self-Organised Network Security.
3. Intrusion Detection and Prevention.
4. Privacy preservation and Anonymity.
5. Economics of Cyber Security
6. Cloud Computing Security.

For our discussion purpose we shall consider Self-Organized Network Security and Cloud computing Security.

Self-Organised Network Security (SON): Game theoretic approaches that are used for designing security protocols for SONs are Vehicular Networks (VANETs), Wireless Sensor Networks and Mobile Ad Hoc Networks (MANETs).
Most of the game theoretic approaches consider that only two players will be there in the game.

Attacker: The attacker is an opponent who makes malicious entry into the system with the intendment of threatening its security. The strategies of the attacker can vary from a single action to a sequence of differed counter activities. In this study, we limit our interests to such attacks that consist of a series of activities that directs towards an ultimate goal.

Defender: The defender on the other side is responsible for applying proper defense techniques to secure the system from various malicious attacks from attacker. The defender has a set of counter strategies to monitor and protect the system. The main aim of this player is to make pre-emptive responses in a manner where he has limited knowledge of the system status, purely relying on the counter strategies.

These assumptions on players are not practical in MANETs. The strategic decisions of each node in MANETs can be computed in a fully distributed approach, where the decision can be made without centralized administration and each node only needs to know the information of its own state and thereby aggregate effect of the other node in the MANET[5].

In few networks Digital signature is widely used, it may provide security but it introduces delay due to signature verification which in turn reduces Quality of Service QoS.

Cloud Computing Security: Traditional security is not suitable for Cloud computing concepts such as multi-tenancy, resource sharing and resource outsourcing. These are the new challenges for security researches.

Security-aware virtual machines (VM) have been proposed by researchers with the combination of game theory in public cloud, where multiple Nash Equlibria has been included for security game in public cloud i.e., defender has counter actions for each one of the attackers strategies. Nash Equilibrium is a combination of Set of strategies and payoffs which results in stable state where no player has benefit when there is change in strategies on any player in the game.

Scalable security risk assessment model using game theory has also been proposed for cloud computing in order to evaluate the risk. Main aim of this risk assessment is to decide who should fix the risk in the system i.e. by the cloud provider or tenant of the system [6].

CHALLENGES

The main challenges faced while designing the game theory model are [7]:

Defining payoff function for each player in the game is practically impossible. But payoff function is a key procedure in game theory because result of the game is directly dependent on the result of payoff function.

All the game models and strategies are based upon assumptions. But in reality the strategies involves in cyber security problems are infinite and dynamic. Based on assumptions result of the payoff function may be good. But if it is implemented practically it is difficult to achieve good result from payoff function.

Defining payoff functions for attacker and defender is practically impossible. Strategies based on assumptions cannot be implemented in real time.

The proof for existence of Nash Equilibrium is only logical not constructive. There are not methods available to implement Nash Equilibrium practically. All these assumptions cannot be used without proof because it may result in security compromise.

CONCLUSION

Game theory in literature has proven results for its capability in solving problems of applications like e-Commerce. With this background, the paper attempts to unfold the security issues, challenges and the research which are ongoing in the field of game theory to researchers.

For now, an exhaustive theoretical explanation of game theory is available to readers, but for the practical implementation of game theory concepts is still an open research area. In this paper, many aspects, applications of game theory are discussed especially in the areas of Self-Organized Networks and Cloud Computing.

REFERENCES

[1] Russouw von Solms and Johan van Naikerk "From information security to cyber security" Computers & Security, Volume 38, 97-102, October 2013.

[2] Yuan Wang, Yongjun Wang, Jing Liu, Zhijian Huang and Peidai Xie "A Survey of Game Theoretic Methods for Cyber Security" 2016 IEEE First International Conference on Data Science in Cyberspace.

[3] Seth T. Hamman, Member, IEEE, Kenneth M. Hopkinson, Senior Member, IEEE, Ruth L. Markham, Andrew M. Chaplik, and Gabrielle E. Metzler "Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students" IEEE Transactions On Education, Vol. 60, NO. 3, August 2017.

[4] G. Owen, Game Theory, New York: Academic Press, 3rd ed., 2001.

[5] Y. Wang, F. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile Ad hoc networks." IEEE Trans. on Wirel. Commun., 13(3): 1616-1627, 2014.

[6] L. Kwiat et al., "Security-aware virtual machine allocation in the cloud: a game theoretic approach," Proc. IEEE 8th Int'l Conf. on Cloud Computing, 2015.

[7] E. Furuncu and I. Sogukpinar (2015). "Scalable risk assessment method for cloud computing using game theory," Computer Standards & Interfaces, 38: 44-50, 2015.