Enhancing Awareness of Cyber-Security and Cloud Computing using Principles of Game Theory

Anil Lamba

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.

Game theory is a mathematical model which deals with interactions between various entities by analyzing the strategies and choices. In today's world, Game Theory is being extensively used in fields like economics, sociology, political science, etc. due to its versatile nature and applications in myriad of conflicts and problems. The application of game theory has been extended to computer science also due to its versatility and robustness. In this paper we have discussed the applications of game theory in fields of cyber security and cloud computing along with the comparative study of different game models used in their respective fields. We have also discussed about Compositional Game Theory and its applications for solving complex problems.

Keywords: Cyber security; Cyber physical systems; Game theory; Cyber-attacks; Cloud Computing; Compositional Game Theory.

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.

One of the primary tasks performed by humans is interaction with other people. It is beneficial for humans to interact as this can result into mutual benefit for all the people involved in these interactions. However, this is not always the case, because people could have conflicting interests as well. Thus, in such situations, in order to resolve the

conflicts between the people involved, one of the approaches which can be used is Game Theory.

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.

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.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.

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.

A. Aspects of Game Theory:

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. Game theory depicts the game played between different players and the strategies of each player. A game can be defined as interaction of different players according to a set of rules.

Players may consist of individuals, machines, companies or associations. Unlike traditional approaches, the results of game theory not only depends on the actions of the current player but also behavior of other players present in the game. Due to this reason, this approach is extremely scalable and versatile. The outcome of game theory also depends on the estimated payoff by each player before making decisions, which is a measure of the satisfaction obtained by each player by making that decision. Hence the players will perform actions and take decisions which would provide them with maximum payoff.

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.

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.

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.

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.
- 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

In modern systems the traditional game theory concepts are hardly effective due to their complexity. These systems contain emergent effects due to which the compound system has a behaviour that is dependent on various components and isn't independent of simple behaviors of the system. Hence the compositional game theory helps in

accurately depicting the compound systems using a bottom-up approach by building larger games from smaller ones. It introduces the concept of open games which accurately represent the interactions. This models the game interactions as well as the interactions of the game with the other games and the environment. The key component of this is the selection function which is a pure strategy profile. This does not only make the model scalable but also economical according to the needs of the client and hence is the future of game theory in cyber security.

According to the NIST, cloud is defined as a model enabling the ubiquitous, on-demand network access to a shared pool of computing resources such as application, infrastructure etc. As discussed in, different types of cloud computing services are as follows:

- Infrastructure as a Service(IaaS): In this type of cloud computing, the infrastructure of the network is considered as a fully outsourced service.
- Platform as a Service(PaaS): It is an advanced type of IaaS cloud computing service which also uses platform as well as solution stack as a service.
- Software as a Service(SaaS): This type of cloud service provides application to its customers on demand. It mainly involves functions such as web conferencing, email, time management etc.

Due to variety of advantages offered by the cloud such as resource pooling, on demand service, and elasticity according to the end user, it is rapidly expanding and becoming more and more popular simultaneously posing various challenges along with it. Two basic problems associated with cloud with can be counteracted using game theory are:

Cloud Cyber Space Security

Cloud cyber space has expanded into a multi-dimensional space that extends over various areas due to which conventional methods cannot be used for cloud security. Some of the solutions proposed by the researchers to implement cloud security are:

- Secure Virtual Machines: In Iaas offers the on-demand resources in the form of Virtual Machines. This approach has been proposed for the public cloud where multiple Nash Equilibria are involved for the security. It analyzes the cause-effect interdependency in the public cloud. Despite the involvement of multiple Nash Equilibria, the players use specific profile of Nash Equilibria which does not depend on the degree of the extent of data that has been compromised. This reduces the externality factor.
- Scalable Security Risk Assessment Model: There are a lot of risks involved in cloud cyber space security such as data breaches, data loss, hacked interfaces, insecure APIs and DDOS attacks. This model is used to analyze and evaluate the risk and it further ponders upon the fact whether the risk evaluation is the job of the cloud service provider or the tenant.
- Cloud Security Transparency Problem: It can be modelled as a non-cooperative stochastic problem where the client and cloud provider are considered as players. The client has to choose whether to buy the services from the cloud providers based upon the level of transparency provided by the cloud provider or not based on Nash Equilibrium.

Pricing Strategies of different cloud service providers

Application of game theory which involves understanding and identifying the characteristics of different cloud beneficiaries and the actions performed by them to gain maximum financial advantage. The market model considered is an Infrastructure as a Service Model which efficiently depicts provider's and client's potential behaviour and rewards involved. Models depicting this behaviour are described as follows:

Extensive form game: The provider makes an offer to the client and the client is free to accept the offer or not. Hence there are two point of views in this case which are then combined according to Nash Equilibrium at which the client and provider both agree upon.:

  - Client's View - the client will comply to the provider's offer if it offers a lower cloud price or else he/she will build his/her own data centre.

- Provider's View - To gain the most while providing services at the highest possible prices.

Discriminatory pricing policy: It sets different pricing systems for different service providers and clients. The bids are sorted in a descending order by the marketplace and matches client in an ascending order.

Uniform Pricing Policy: In this type of policy the prices are set same for all concurrent matched pairs. It uses the equilibrium price as the service price. In this paper, Shi et al. prove that discriminatory pricing policy is better in performance than uniform pricing policy and hence cloud providers as well as the consumers converge towards the discriminatory policy.

- Resource Pricing - Stackelberg Approach: This model depicts the method by which the SaaS provider offers services using the resources allocated by the IaaS provider who uses a pay-per-use scheme constituting on demand, flat demand instances of virtual machines. This model assumes that the SaaS providers periodically allocate their services to the virtual machines. This involves a two stage procedure:

- Stage - 1: Each provider looks at the number of on-demand and flat services which qualify the performance level as per the agreed service level agreement with the client.

- Stage - 2: The provider then leases the unused instances as the spot instances. The IaaS provider determines spot instance prices after evaluating different bids in order to maximize their revenue.

CHALLENGES

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

1. 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.

2. 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.

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

4. 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 is one of the most important and efficient approaches towards conquering security issues in computer science. From above sections, we can say that using this concept of game theory we can analyze the optimal moves and strategies of the players involved in order to determine the best solution for each player. Cyber Security makes use of game theoretic models in order to protect the cyber space from intrusion attacks and physical level security.

Game theory in cloud basically provides solutions in Cloud Security and deciding the Pricing strategies. However, game theory is at its primitive stage in the field of research and new methods have to be implemented to account for exponential growth of the cyber space and the problems associated with it. Its scope can be enhanced by implementing different game theoretical models by integrating advanced mathematical concepts in it. One of the methods to upgrade the existing approaches of game theory is Compositional Game Theory, which takes the concepts of traditional game theory and makes it more scalable and practical for compound problems.

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