Game Theory and its application in Cyber Security

Drishti Agarwal[1,#], Preeti Nagrath[1], Jyoti Arora[2]
[1]Bharati Vidyapeeth's College of Engineering,
Maharaja Surajmal Institute of Technology,
#Corresponding Author, Email: jyotiarora@msit.in

***Abstract*—Game theory is an emerging area of mathematics that provides a diverse variety of multi-person rational decision-making mathematical methods that can be used to analyse decision-makers' relationships in cyber security problems that compete for scarce and shared resources. This paper presents an articulated study of this concept and its usage in the cyber security field. Further, it discusses the Bayesian Nash equilibrium in detail with its application in a meta-model developed for a bank transfer system.**

***Index Terms*—Actions, Bayesian game, Dynamic games, Interim, Meta-model, Nash Equilibrium, Payoff, Utility**

I. Introduction

In the era of technological revolution, new technologies and inventions are being adopted in every field of computer science with advanced networking methods and connectivity required to support this evolution[1]. This has completely changed the way of living, with high interconnectivity amongst the internet users in the field of business, entertainment, social media, healthcare, education, governance and even finances. The Internet has made every information easily accessible to everyone hence, tremendously increasing the security threats. These new threats and security breaches demand different approaches[2] to bring about a positive change in the way we secure our systems.

These attackers tend to breach anyone's system ranging from a specific individual to the government or financial agencies with the intent to gain valuable data which can be used in malicious activities and data theft. By using game theory, computer security experts and white hat hackers can build systems efficient in tackling every possible attack by the malicious programmers. Game theory deals with strategic interactions between various parties with each party ensuring their win. Further, the defence mechanism of any system depends upon the strategic interactions amongst the defenders and the attackers within themselves. This method provides tactical analysis support to investigate attacks and the region of its effect.

In this paper, we present a detailed study of the basic concept of game theory and its application in cyber security through a model implemented in a real system. First, we begin with understanding the branch of mathematics in, its basic terminologies and its classification, in section III followed by understanding the Nash Equilibrium as the solution concept of the method and its drawbacks, in section IV. Further, we will see the theory behind Bayesian games and its advantage over the Nash Equilibrium, in section V. Section VI explains the application of Bayesian game by defining a model for the general-purpose which we will be applied on a bank transfer system to understand its functioning over real-world problems. Finally, the paper presents its conclusion and results, in section VII.

II. Literature Review

There has been a plenitude of research and inventions in terms of the application of game theory in the network security framework. The focus on dynamic areas of the game theory model can be useful in analysing the interaction between the attackers and the defenders by involving multiple levels of attack/defence strategies [1]. Reviewing the existing game theory approaches for cybersecurity in terms of cyber-physical, security, communication security, and privacy can be seen in paper [3]. Deception is one of the most famous techniques used to provide false information to the attackers and manipulate them into believing the hypothetical system to ensure security. The perfect Bayesian Nash equilibrium[4] is the perfect solution concept to perform deception games and to analyse the attackers. Further, the paper [5], presents an excellent approach to study the risk likelihood in manufacturing systems quantifiably through game theory. While the game theory has been applied to many issues that require rational decision-making, there is a limitation on the use of such a method in security games when the defender has limited information on the opponent's strategies and payoffs. The paper[6] proposes QLearning to respond automatically to a suspect user's adversarial actions to protect the framework. A Risk-aware Computation Offloading (RCO) policy is advised in the paper[7] to safely spread computation tasks across geographically dispersed edge sites under server-side attacks in order to resolve these server-side risks. To create the RCO dilemma, which sets an effective relationship between the edge system (as a defender) and the attacker, the Bayesian Stackelberg game is employed. Whereas some researches propose game theory inspired defence architecture[8] in which a game model acts as the brain. This concentrates on one of our recently proposed game models, the stochastic game of imperfect knowledge.

III. Introduction to Game theory

Game theory is a branch of mathematics that deals with strategizing and deciding the course of a competition or a social, economic situation in which multiple entities or parties are involved, capable of making their own decisions and performing the required actions. This science of strategy

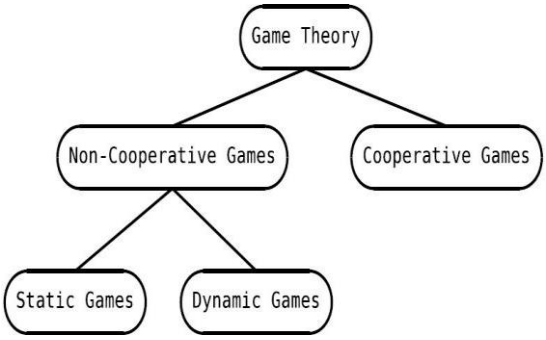

Fig. 1. Classification of various game theory techniques [9].

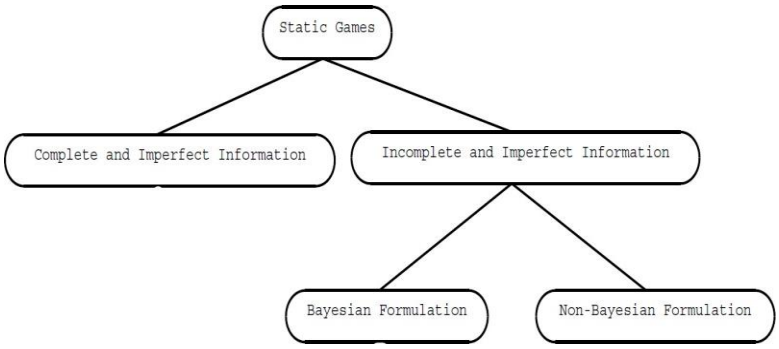

Fig. 2. Segregation of static games into further categories [9].

helps us to develop a framework of outcomes in the problem statement which can be considered as a multiplayer game where all players are assumed to be rational as a result of which they will seek maximum profit or win for themselves and are aware of consequences of their actions. Game theory is applied in economics[10], science, social science, psychology and natural science. The widespread application of game theory is because it's simply a decision-making mathematical tool. Game theory comes with essential components that can structure the problem statement in the language of this tool:

1) **Players-** The game players are the entities involved in the problem, a player can be an individual, a group of individuals, an institution or any interacting entity. These players participate in the game with goals and strategize their decision or moves to ensure maximum profit from the situation
2) **Actions-** These are the moves, choices or decisions made by the players of the game based on their strategies. Actions of the players define the course of the game and future outcomes. Every action has an impact which can be positive, negative or neutral.
3) **Payoff functions-** Every action has an impact that can be defined as the amount of profit or loss a player incurred while acting. Once the game ends, each player will get a certain amount of profit or loss or none, known as their payoff.
4) **Strategies-** It is the plan of action that defines the decisions of the players leading them to win or desired payoffs.

Now, game theory encompasses various kinds of frameworks depending upon the problem statement thus the games can be classified as:

1) **Co-operative games[11]–** These games as the name suggests inculcate cooperation amongst the players of the game. Here, the players are not individuals but a coalition of players.
2) **Non-Co-operative games-** These games are competitive in nature as each player aims at wining or maximize his/her payoff. In this type, all the players are selfish in nature and do not consider their opponents
3) **Static games-** In such games, every player is allowed to make a single decision at the start of the game which cannot be altered without any information about the strategies of other players.
4) **Dynamic games-** As opposed to static games, dynamic games consist of players who have some prior knowledge about the behaviour of their opponents and based on that they are allowed to make strategies and decisions.
5) **Complete Information games-** In this, the players are aware of their opponent's strategy and their decision-making skills.
6) **Incomplete Information games-** unlike complete information games, these games have a certain set of players who are unaware about their opponents and thus, its difficult for them to compete.
7) **Perfect information games-** these games allow players to be fully aware of the past actions of their opponents before taking a new action.
8) **Imperfect information games-** here, we have a minimum of one player who is unaware of past actions of other players. So, its id difficult for that player to compete against the others. Cyber security game theory approaches fall under this category.

IV. Nash Equilibrium

The game theory aims to make predictions about the outcomes of the game being played amongst the participants, for that the most basic approach will be the Nash equilibrium algorithm. This solution concept is defined as: Let us consider N players in a particular setup or game with S_i and U_i for $1 \leq i \leq N$ be the strategy spaces and the utilities or payoff, for each player, respectively. Now, every element of S_i for every i^{th} player is termed as the pure strategy. Thus, the game is defined as:

$$G : N; S1, S2, \ldots SN; U1, U2, \ldots UN \quad (1)$$

The probable outcome of the game is derived by analysis of the behaviour of the players as well as their strategy choices.

Let $s = s_1, s_{2,N}$ be the profile of pure strategies with $s_i \in S_i$. Let s_{-1} be the profile of strategies excluding player i. A strategy profile s with $s = s_i ; s_{-1}$ for all i , is a NE [5] such that for all $1 \leq i \leq N$ we have

$$U_i(s) \geq U_i(t; s_{-i}), \forall\ t \in S_i \quad (2)$$

It's also defined by stating that i which is each player's strategy, is the best response to the strategies of the other players. In the case of cyber security, the defenders' strategy profile (NE), will consist of a set of defensive schemes for each defender, such that each defender's strategy is the best response to the attackers' strategies.This is also defined by stating that i or the strategy of each player is the most appropriate response to the strategies of other players.

V. About Bayesian Game

A Bayesian game overcomes the drawbacks of the NE by predicting the outcome of the game with players having incomplete knowledge of the strategy of their opponents. In Bayesian games, we have the types or the state of nature defined for the players probabilistically by some legitimate source. Each player's probability distribution across states of nature is private to them and is only known to them. In Bayesian games, nature is authorised to reveal information about its state, which is referred to as the signals to the players. These signals can assist them in developing the payoff or expected utility in conjunction with the actions.

A Bayesian game[12] consists of a tuple $(N, \Omega, (S_i, T_i, C_i, \tau_i, p_i, U_i)_i)$ where Ω is the set of natural states, and for each player $i \in N$.

- S_i is the set of player i's all available actions
- T_i is the set of player i's signals/types, with $\tau_i \Omega \rightarrow T_i$ is the state-to-signal mapping
- $C_i\ T_i \rightarrow 2^{S_i}$ is the set of i's available actions after receiving $t_i \in T_i$
- p_i is the probability measure over Ω
- $U_i : \Omega \times S \rightarrow R$ is player i's utility function where R is the set of real numbers

As the solution concept of NE is implemented into Bayesian it is called as Bayesian Nash Equilibrium.

VI. Application of Bayesian NE in Cyber Security

This section will explain the application of a Bayesian nash equilibrium in the field of cybersecurity through a generic meta-model, used to develop actual models. In this case study, we will feed the characteristic of a bank transfer system to the model and modify it in terms of game theory by considering the system's participants into players of the game to gain a better understanding of its usage.

A. Definition of the model

Although Bayesian game models are effective in real life situation but some assumptions are required to state the model mathematically.

1) It is assumed that the number of agents or players are fixed.

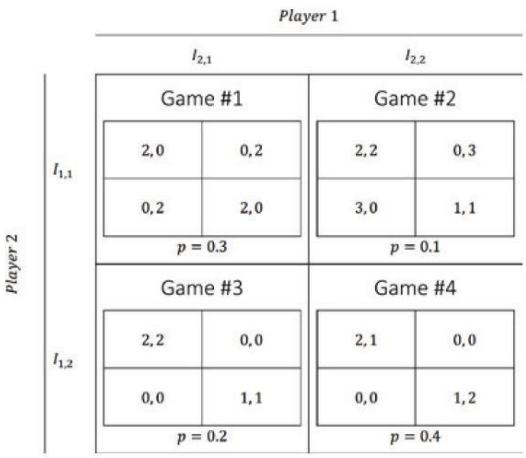

Fig. 3. Bayesian Game model between two players[5].

2) The number of agents will not vary in between the game.
3) Every agent's belief is further back in position[13] which means a common prior can be determined based on individual private information.

Although such games can be categorised as static and dynamic, the static division is mathematically explainable due to its simplicity. Also, because the number of agents and their beliefs can be modified during a dynamic approach with the acquired information, thus defining the realistic approach between the game.

The figure above shows four one-to-one games in which the belief of an agent is reflected in the columns and the belief of the other agent in rows. As a result, you can't study about the game you are playing. They must therefore develop a method that maximises pay-off and reduces losses due to incomplete information. Furthermore, the game's agents can be classified as follows:

1) **ex-ante-** At the beginning of a game, neither agent has any specific information on any of its own types. For example, the analyst does not know the position of the business while making long-term estimates for a company.
2) **interim-** An agent is aware of the information of its type but not of other types. This is the situation in our case, because the attackers' identities and motivations are unknown. In addition, the response of the bank is, to some extent, unknown.
3) **ex-post-** Every agent is well-versed in all types. This type of situation, for example, describes a real-life board game with friends.

This categorisation will help us to build the mathematical model of the system as it gives the definition of the player's expected utility, their individual payouts and their actions. So, the best suited model for us will be interim type.

So, through analysis and calculation certain traps can be defined, the three core aspects are:

1) **Pay-off of the action-** For an i^{th} agent the payoff based on the action a with type $\vartheta_i is u_i(a, |\vartheta_i, \vartheta_{-i})$.
2) **Probability of action-** Based on the present situation, the probability of a specific action for a type:

$$\sum_{a \in A} \left(\prod_{j \in N} s_j(a_j|\vartheta_j) \right) \quad (3)$$

S_j is a chance function which predicts how likely a certain action will be executed or provides the strategy depending upon the current situation for the type j. This function is situation specific, so it has to be re-evaluated every round.

3) **Probability of type-** The probability of an agent being certain type, based on previous action is given as:

$$\sum_{\vartheta_i \in \vartheta_{-i}} p(\vartheta_{-i}|\vartheta_i) \quad (4)$$

we can calculate expected utility value of an agent, considering the chance of it belonging to a specific type, and the chance that it might take a specific action based on the type:

$$EU_i(a|\vartheta_i) = \sum_{a \in A} \left(\prod_{j \in N} s_j(a_j|\vartheta_j) \right) u_i(a, \vartheta_i, \vartheta_{-i}) \quad (5)$$

B. Application of Model

Now in a banking transfer system the players can have three different roles:

1) **Bank-** the source or the target of all actions.
2) **Non-malicious-** the users of the bank, can be the employees or the customers.
3) **Malicious-** The hackers, intruding with the aim to steal information or money.

Some additional predictions that have to be incorporated to apply this segment to the dynamic theory of Bayesian matches: A new strategy for utility value assessment is required for constantly changing or even uncertain number of agents in the system. In this case, although testing of the conventional method is almost impossible, it is less important because every actor is evaluated against a fixed model based on the intended form of the agent from the other agents of the system. Another assumption is that we do not have a common prior, as a common position or agent exists, for example, banks with a common pior. Because there are three roles, the model will be converted into a three-party system with a 3D model structure. All three axes in this system will represent the various types of game players. Furthermore, the common prior or probability of the type is assigned according to the roles, reducing the challenges of non-malicious parties in the chance sets. In addition, in the common priors, we have knowledge sets specific to a particular actor. These specific sets assist an agent in carrying out the actions. Furthermore, the utility calculations found in the classic Bayesian game are no longer directly relevant because they take into consideration all types of agents, the current situation, and the expected behaviour of some remaining agents. The types of 87 agents, for the major aspect, require the application of abstraction to the current situation.

C. Utilisation of the model

This meta-model can be utilised in the identification of malicious system users, when the principal component, agent, is correct to find the role of an agent. In addition, we must demonstrate the relationship between the actual and calculated utility, which varies depending on the type of intention. In the situation, of information theft, the utility calculation should have all of the information-required procedures and feasible derivations, complicating the real calculation and adding some uncertainty. The three core identifiers are effective when used in conjunction with generalisation and action division: Prior-based identification- In this case, we specify how a hacker will enter the system, thereby identifying the agent's likely role. This can be applied by identifying entry points that can be supplemented with honeypots. Information-based identification- Each role has a known pool of information, which can gain information, overlap or contain information from the outside pool, which can encourage suspicious system activities. One way is to reduce the knowledge and expertise based on the true type of the agent, but it is risky since exact type estimates are not perfect and can also be incorrect. Utility-based identification- because the utility is the most important element that is strongly defined for each action of the agents involved, even the smallest deviation in its value can indicate the presence of malicious attacks. When combined with out-of-pool or uncertain knowledge, this causes a very strong belief in a malicious agent, which shows the real type and intent. The system- and type-specific measures are additional. type-specific.

VII. Results

The model did consist of a series of assumptions that aimed at filling the gaps and relate them closely to the real-world scenario. The model was developed on the concept of Bayesian game theory apart from all other analysis methods, this was because most of the other methods are based on confidentiality whereas in a money transfer system if we consider the case of attackers, they have to deal with the discrepancy in the information. Since major models heavily relied on modelling the entire system in all of its states, only this Bayesian one was able to stand against the information warnings. We also found out that one can study the interactions between different players and agents using a normal game theory method but the Bayesian game goes a step ahead since it makes it easier for players with hidden information to be involved in the model. It helps to find an unpredictable number of agents in the way it works in banking transaction systems. This specific method also has an advantage.

VIII. Conclusion

The paper meticulously defined every aspect of game theory as required in the final study. It discussed the basic framework of a game theory problem and the concept solutions like Nash equilibrium and Bayesian Nash equilibrium. Various topics were explained in this paper, including the importance of using the cyber risk analysis into the bank transfer systems, the

need to change Bayesian games to be relevant to the systems and the three key elements of safe bank transfers. Further, the paper went through the drawbacks of the generic model. Also, the utility of the meta-model was defined with certain assumptions.

REFERENCES

[1] A. Attiah, M. Chatterjee and C. C. Zou, "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-7, doi: 10.1109/ICC.2018.8422719.

[2] Kakkad, Vishruti Shah, Hitarth Patel, Reema Doshi, Nishant. (2019). A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing.. Procedia Computer Science. 155. 680-685. 10.1016/j.procs.2019.08.097.

[3] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game Theory for Cyber Security and Privacy. ¡i¿ACM Comput. Surv.¡/i¿ 50, 2, Article 30 (June 2017), 37 pages. DOI:https://doi.org/10.1145/3057268

[4] Zhang, Tao Huang, Linan Pawlick, Jeffrey Zhu, Quanyan. (2019). Game-Theoretic Analysis of Cyber Deception: Evidence-Based Strategies and Dynamic Risk Mitigation.

[5] Zarreh, Alireza Wan, Hung-da Lee, Yooneun Saygin, Can al Janahi, Rafid. (2019). Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. 10.31224/osf.io/mb5t9.

[6] K. Chung, C. A. Kamhoua, K. A. Kwiat, Z. T. Kalbarczyk and R. K. Iyer, "Game Theory with Learning for Cyber Security Monitoring," 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE), Orlando, FL, 2016, pp. 1-8, doi: 10.1109/HASE.2016.48.

[7] Yang Bai, Lixing Chen, Linqi Song, and Jie Xu. 2019. Bayesian Stackelberg Game for Risk-aware Edge Computation Offloading. In ¡i¿Proceedings of the 6th ACM Workshop on Moving Target Defense¡/i¿ (¡i¿MTD'19¡/i¿). Association for Computing Machinery, New York, NY, USA, 25–35. DOI:https://doi.org/10.1145/3338468.3356772

[8] Sajjan Shiva, Sankardas Roy, and Dipankar Dasgupta. 2010. Game theory for cyber security. ¡i¿Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research¡/i¿. Association for Computing Machinery, New York, NY, USA, Article 34, 1–4. DOI:https://doi.org/10.1145/1852666.1852704

[9] 9-S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and Q. Wu, "A Survey of Game Theory as Applied to Network Security," 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, 2010, pp. 1-10, doi: 10.1109/HICSS.2010.35.

[10] Y. Wang, Y. Wang, J. Liu, Z. Huang and P. Xie, "A Survey of Game Theoretic Methods for Cyber Security," 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), Changsha, 2016, pp. 631-636, doi: 10.1109/DSC.2016.90.

[11] Annapurna P Patil1 , Bharath S2 , Nagashree M Annigeri3 1Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, Karnataka-560054, India, Applications of Game Theory for Cyber Security System: A Survey , International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 12987-12990 © Research India Publications. http://www.ripublication.com 12987

[12] A. Iqbal, L. J. Gunn, M. Guo, M. Ali Babar and D. Abbott, "Game Theoretical Modelling of Network/Cybersecurity," in IEEE Access, vol. 7, pp. 154167-154179, 2019, doi: 10.1109/ACCESS.2019.2948356.

[13] Shinde, Rhythima Berg, Jan Veeken, Pieter Schooten, Stijn. (2016). Applying Bayesian game theory to analyse cyber risks of bank transaction systems. 10.1109/CAST.2016.7914945.