Advances in Wireless Communications and Networks
2017; 3(4): 45-49
http://www.sciencepublishinggroup.com/j/awcn
doi: 10.11648/j.awcn.20170304.13

Game Theory Basics and Its Application in Cyber Security

Amadi Emmanuuel Chukwudi, Eze Udoka, Ikerionwu Charles

Department of Information Management Technology, School of Management Technology, Federal University of Technology Owerri, Owerri, Nigeria

Email address:
emmanuel.amadi@futo.edu.ng (A. E. Chukwudi), drezeudokaf@yahoo.com (E. Udoka), charles.ikerionwu@futo.edu.ng (I. Charles)

To cite this article:
Amadi Emmanuuel Chukwudi, Eze Udoka, Ikerionwu Charles. Game Theory Basics and Its Application in Cyber Security. *Advances in Wireless Communications and Networks*. Vol. 3, No. 4, 2017, pp. 45-49. doi: 10.11648/j.awcn.20170304.13

Received: May 25, 2017; **Accepted**: July 4, 2017; **Published**: July 27, 2017

Abstract: The concept of game theory has in recent times has found application extensively in the area of security usually called security games. A game could be normal form or extensive form and are used to model the behaviour of players in a simple or complex contest for resources within a given scenario. Game theory finds application in various areas including finance, economics, politics, auction, sciences and cyber security. This work reviews the application of game theory in cyber security. A brief introduction to the concept of game theory is presented alongside a detailed review of research works carried out using the concept of game theory for cyber security.

Keywords: Game Theory, Cyber Security, Security Games, Players

1. Introduction

The traditional architecture of World Wide Web makes it vulnerable to serious kinds of threats including DoS/DDoS, Brut force, SQL injection etc. Researchers have over the years been exploring the applicability of game theoretic approaches to deal with cyber security issues and some of these approaches have been successful.

Game theory aims to help us understand situations in which decision-makers interact with each other in some ways. A game in the everyday sense is a competitive activity in which players contend with each other according to a set of rules or laid down moves. [1]

The complexity of the cyber world has grown over the years and has become more sophisticated even as attacks have also grown in complexity. One notable approach is the game theoretic model [2], which optimally allocates cyber security resources such as administrators' time across different tasks. This work modelled the interactions between an omnipresent attacker and a team of system administrators seen as the defender. The work also proposes Singular Value Decomposition (SVD) as an efficient technique to compute equilibria in games.

Another work by Lye and Wing [3] presented a game-theoretic method for analysing the security of computer networks. They viewed the interactions between an attacker and the administrator as a two player stochastic game and construct a model for the game. Using a non-linear program, they computed the Nash equilibrium or best-response strategies for the players (attacker and administrator). They then explain why the strategies are realistic and how administrators can use these results to enhance the security of their network.

Researchers are now on their toes to bring to organizations workable solutions to network security treats; one of such approach is the use of theories that fit into real life scenarios to develop mitigation approaches. Game theory is one of such approaches researchers are exploring and it depicts a competitive activity used to model the behaviour of attackers and defenders of a network.

2. Concept of Game Theory

A game is a description of the strategic interaction between opposing, or co-operating, interests where the constraints and payoff for actions are taken into consideration. On the other hand, a player is a basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.

Game theory describes multi-person decision scenarios as games where each player chooses actions which result in the best possible rewards for self, while anticipating the rational actions from other players. A player is the basic entity of a game that makes decisions and then performs actions. A

game is a precise description of the strategic interaction that includes the constraints of, and payoffs for, actions that the players can take, but says nothing about what actions they actually take [4].

A solution concept is a systematic description of how the game will be played by employing the best possible strategies and what the outcomes might be. The consequence function associates a consequence with each action the decision makers take. A preference relation is a complete relation on the set of consequences which model the preference of each player in the game. A strategy for a player is a complete plan of actions in all possible situations throughout the game. If the strategy specifies to take a unique action in a situation then it is called a pure strategy. If the plan specifies a probability distribution for all possible actions in a situation then the strategy is referred to as a mixed strategy.

There are four basic characteristics of a typical game as it applies to game theory. They include:

a Multiple player, two or more
b Competitive in nature
c Rules that guide every game
d Payoffs for player

Nash Equilibrium

A very important concept in game theory is the Nash Equilibrium point. A Nash equilibrium is the intersection of best response i. e each player is playing his best response to the actions of all the other players. [5]

A Nash equilibrium is a solution concept that describes a steady state condition of the game; no player would prefer to change his strategy as that would lower his payoffs given that all other players are adhering to the prescribed strategy. This solution concept only specifies the steady state but does not specify how that steady state is reached in the game. The Nash equilibrium is the most famous equilibrium, even though there are many other solution concepts used occasionally. This information will be used to define games that have relevant features for representing network security problems. [4]

Consider the strategy profile for an N player game

$$a_1, a_2, a_3, ...a_N^* \tag{1}$$

Where a_N^* is the Nash equilibrium, if each player i, has payoff of Ui, then

$$U_i(a_i^*, a_{-i}^*) \geq U_i(a_i, a_{-i}^*) \tag{2}$$

has to hold for each player i where a_i^* is the action profile of player i and a_{-i}^* is the equilibrium action of all other players

Two important concepts hold for every game. They are Rationality and common knowledge. Rationality is simply consistency in decision and does not put into consideration the likes or dislikes of each player in the game. Common knowledge consists of both the first time knowledge of outcomes and the mutual knowledge of each player about the outcomes. [1]

Consider a simple game like the prisoners dilemma involving two players. The game can be represented in a matrix as shown in figure 1

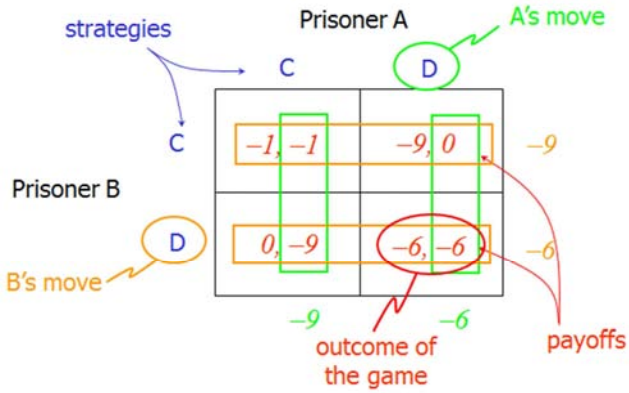

Figure 1. *Prisoners Dilemma game description.*

Two individuals have been arrested for possession of guns. The police suspects that they have committed some form of crime; if nobody confesses to the police, they will be jailed for 6 years. If only one confesses, she'll go free and her partner will be jailed for 9 years if they both confess, they get 1 year each. In this game, a Nash equilibrium point will occur such that both prisoners will deny the crime since they don't have a previous knowledge of what the other player will do. See figure 1 (outcome of the game -6,-6)

3. Simple Game Types

3.1. Perfect Information Game

A game in which each player is aware of the moves of all other players that have already taken place. Examples of perfect information games are: chess, tic-tac-toe, and go. A game where at least one player is not aware of the moves of at least one other player that have taken place is called an imperfect information game.

3.2. Bayesian Game

A game in which information about the strategies and payoff for other players is incomplete and a player assigns a 'type' to other players at the onset of the game. Such games are labelled Bayesian games due to the use of Bayesian analysis in predicting the outcome.

3.3. Static/ Strategic Game

A one-shot game in which each player chooses his plan of action and all players' decisions are made simultaneously. This means when choosing a plan of action each player is not informed of the plan of action chosen by any other player. In the rest of this paper, this class of game is referred to as 'static game'.

3.4. Dynamic/ Extensive Game

A game with more than one stages in each of which the

players can consider their action. It can be considered as a sequential structure of the decision making problems encountered by the players in a static game. The sequences of the game can be either finite, or infinite. In the rest of this paper, this class of game is referred to as 'dynamic game' [6].

3.5. Stochastic Game

A game that involves probabilistic transitions through several states of the system. The game progresses as a sequence of states. The game begins with a start state; the players choose actions and receives a payoff that depend on the current state of the game, and then the game transitions into a new state with a probability based upon players' actions and the current state [7].

A description of a game can be modelled under the following game characteristic headings:

3.6. The Game Type

a List of Players/"on-player" participants and their roles.
b When does a player get to move in the game (order of moves)?
c What are the actions available to players when they get to move in the game?
d How much do the players know before they get to move?
e Pay-off for each player

4. Information Warfare as a Game

Global networks continue to undergo dramatic changes resulting in ever-increasing network size, interconnectivity, and accessibility, and a consequent increase in its vulnerability. Several recent Federal policy documents have emphasized the importance of cyber security to the welfare of modern society. The President's National Strategy to Secure Cyber Space describes the priorities for response, reduction of threats and vulnerabilities, awareness and training, and national security and international cooperation. Cyber Security: A Crisis of Prioritization describes the need for certain technologies for cyber security [4]

Security should be an integral part of advanced hardware and software from the beginning, as described by Sun Microsystems, Cisco Systems, and Microsoft at the 2006 RSA Conference. Next generation information infrastructure must robustly provide end-to-end connectivity among computers, mobile devices, wireless sensors, instruments, etc. Cyber-security is an essential component of information and telecommunications, which impacts all of the other critical producing secure and reliable software. NSA has an effort on high-assurance computing platforms. The Trusted Computing Group has an ongoing effort. Microsoft has an effort on next-generation secure computing. In future warfare, cyberspace will play a major role where no one is guaranteed to have information dominance in terms of intelligence and accessibility. As a result, a game-theoretic approach of collaboration (carrot) and compelling (counter) moves (stick) need to be played efficiently. This notion is not unlike the mutually assured destruction (MAD) of nuclear warfare. The question then becomes: How do we construct such a game theoretic approach in cyberspace? In general, a game-theoretic approach works with at least two players. A player's success in making choices depends on the choices of others. In game theory, players are pitted against each other taking turns sequentially to maximize their gain in an attempt to achieve their ultimate goal. In the field of cyber security, game theory has been used to capture the nature of cyber conflict. The attacker's decision strategies are closely related to those by the defender and vice versa. Cyber-security then is modelled by at least two intelligent agents interacting in an attempt to maximize their intended objectives.

Different techniques available in game theory can be utilized to perform tactical analysis of the options of cyber threat produced either by a single attacker or by an organized group. A key concept of game theory is the ability to examine the huge number of possible threat scenarios in the cyber system [4]. Game theory can also provide methods for suggesting several probable actions along with the predicted outcome to control future threats. Computers can analyse all of the combinations and permutations to find exceptions in general rules, in contrast to humans who are very prone to overlooking possibilities. This approach allows identification of the what-if scenarios, which the human analyst may not have considered.

The use of game theory in modelling good and evil has also appeared in several other areas of research. For example, in military and information warfare, the enemy is modeled as an evil player and has actions and strategies to disrupt the defense networks. Browne describes how static games can be used to analyse attacks involving complicated and heterogeneous military networks [8].

5. Game Theoretical Models Review on Security

Hamilton, miller, Otti and Sydjari in their research [9], outlined the areas of game theory which are relevant to information warfare. The paper analysed a few scenarios suggesting several potential courses of actions (COA) with predicted outcomes and what-if scenarios. Alpha-beta, alpha-beta star, and beta pruning with min-max search are suggested approaches.

Chakrabarti & Manimaran focused on the Internet and its infrastructure as being the basis for highlighting attacks and security. Where majority of research focused on securing the data being transferred, this research discussed attacks on the infrastructure which can lead to considerable destruction due to different Internet infrastructure components having various trust relationships with one another. [10]

Markovic and Reiher [11], presented a taxonomy of Distributed Denial of Services (DDoS) attack and defense

mechanisms in aim to classify attacks and defense strategies. Their work highlighted attack commonalities and important features of attack strategies

Hespanha and Bohacek, [12], discussed routing games in which an adversary tries to intersect data packets in a computer network. The designer of the network has to find routing policies that avoid links that are under the attacker's surveillance.

FRIARS cyber-defence decision system capable of reacting autonomously to automated system attacks was developed by McInerney and his friends. Their objective was to use good to fighting evil in cyberspace. [13] Syverson [14], talks about "good nodes fighting evil nodes" in a network and suggested using stochastic games for reasoning and analysis. Marti, Giuli, Lai, & Baker [15], proposed an IDS scheme for MANET which consists of two different modules, viz. the Watchdog and the Path rater.

Liu, Comaniciu, & Man [16] proposed a game theoretic framework to analyse the interactions between pairs of attacking/defending nodes using a Bayesian formulation in wireless Ad-hoc Networks. (Shuang-can, Chen-jun, & Zhang [17], proposed a framework that applies two game theoretic schemes for economic deployment of intrusion detection agent. A game theoretical framework to model the interaction between the service provider and the attacker as an intrusion detection game was proposed by Kodialam & Lakshman [18]. In this scheme, the game is represented as a two person zero-sum game, wherein the service provider tries to maximize its payoff by increasing its probability of successful detection while the attacker tries to minimize its probability of being detected by the IDS. Agah, Das, Basu, Alpcan & Basar [19] [20], addressed the attack defense problem in a sensor network as a two-player non cooperative, non-zero-sum game. In their model, the game is assumed to have complete information and the payoff function of the opponent player decides each player's optimal strategy. The drawback of their work is the assumption that the players have complete information about the game.

Attacks on Infrastructure can be stochastic, where different layers of infrastructure can be compromised because of the various trust relationship existing between them as established by Chakrabarti & Manimaran [10], taxonomy of attacks. Their categorization can help reduce attacker payoffs and mitigate game transition to a new state. Browne describes how static games can be used to analyse attacks involving complicated and heterogeneous military networks [8].

Syverson [21], talks about good" nodes fighting evil" nodes in a network and suggested using stochastic games for reasoning and analysis. We are suggesting that dynamic game can also be used to analyse the several wrong decisions made by the evil player in his attempt to hack into the computer network. This will enable network administrators develop a sophisticated strategy which will be used to frustrate the effort of the evil player (hackers).

6. Conclusion, Recommendation and Future Work

Game theoretic has been an important concept in various security situations and has found great application in cyber security. Recent research works have seen game theory being applied to network security, web security and lots more. Games can be designed and analysed, optimal moves of players are used to determine how best to approach security in the cyber world to a large extent.

One key issue with the game theory is the ability to come up with feasible mathematical solutions to the game problem. We recommend more systematic solution to cyber security problem using game theory that will involve realistic mathematical solution. One of such approaches currently being explored by the researcher is the use of linear programing. The area of integer programming can also be explored in providing a more realistic solution to DDoS attacks in the cyber space.

References

[1] M. J. Osborne, "An Introduction to Game Theory by Please send comments to Department of Economics This version ," 2000.

[2] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Game Theory Meets Information Security Management," in Information Security and Privacy Conference, 2014, 2014, pp. 15–29.

[3] K. Lye and J. Wing, "Game Strategies in Network Security," Copenhagen, Denmark, 2002.

[4] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," Syst. Sci. (HICSS), 2010 43rd Hawaii Int. Conf., pp. 1–10, 2010.

[5] John. F. Nash, "Equilibrium Points in n-Person Games," in Proceedings of the National Academy of Sciences of the United States of America, Published by : National Academy of Sciences, 2013, vol. 36, no. 1, pp. 48–49.

[6] C. F. Camerer, T. Ho, and J. K. Chong, "Behavioural Game Theory: Thinking, Learning and Teaching ∗."

[7] A. Gueye, "A Game Theoretical Approach to Communication Security," 2011.

[8] K. Leyton-Brown and Y. Shoham, Essentials of game theory. Morgan & Claypool Publishers series, 2008.

[9] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "Challenges in Applying Game Theory to the Domain of Information Warfare," Proc. 4th Inf. Surviv. Work., 2002.

[10] A. Chakrabarti and G. Manimaran, "Internet Infrastructure Security: A Taxonomy," IEEE Netw., no. December, pp. 13–21, 2002.

[11] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, 2004.

[12] J. P. Hespanha and S. Bohacek, “Preliminary Results in Routing Games,” Am. Control Conf. 2001. Proc. 2001. IEEE, vol. 3, pp. 1904–1909, 2001.

[13] J. McInerney, S. Stubberud, and S. Anwar, “Friars: a feedback control system for information assurance using a markov decision process,” Technol. 2001, 2001.

[14] P. F. Syverson, “A different look at secure distributed computation,” in Proceedings 10th Computer Security Foundations Workshop, 1997, pp. 109–115.

[15] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” Proc. 6th Annu., 2000.

[16] Y. Liu, C. Comaniciu, and H. Man, “Modelling misbehaviour in ad hoc networks: a game theoretic approach for intrusion detection,” Int. J. Secur. Networks, vol. 1, no. 3/4, p. 243, 2006.

[17] Z. Shuang-can, H. Chen-jun, and W. Zhang, “Distributed intrusion detection system based on BP neural network,” Int. J. Secur. its Appl., vol. 8, no. 2, pp. 183–192, 2009.

[18] M. Kodialam and T. V Lakshman, “Detecting Network Intrusions via Sampling: A Game Theoretic Approach,” Infocom, vol. 0, no. C, 2003.

[19] A. Agah, S. K. Das, and K. Basu, “A game theory based approach for security in wireless sensor networks,” in IEEE International Conference on Performance, Computing, and Communications, 2004, 2004, pp. 259–263.

[20] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrusion detection,” in 42nd IEEE International Conference on Decision and Control (IEEE Cat. No.03CH37475), 2003, vol. 3, pp. 2595–2600.

[21] Syverson, P. F, "A different look at secure distributed computation". In Proceedings 10th Computer Security Foundations Workshop, IEEE Comput. Soc. Press. http://doi.org/10.1109/CSFW.1997.59679, 1997, pp. 109–115.