Original Research Article

GAME-THEORETICAL APPROACHES TO CYBER-CRIME MONITORING

Abstract

Our society's diploma of reliance on IT and our online world is developing daily. Cyberspace, the call given to the worldwide and dynamic domain, composed of the infrastructure of the statistics era consisting of the net networks and statistics and telecommunications structures has supplied extraordinary globalization that gives new opportunities, but additionally includes new challenges, risks, and threats. Knowledge of its threats, dealing with the risks, and constructing suitable prevention, defense, detection, evaluation, investigation, and recuperation is essential. Given the present-day assessment of the statistics safety and intrusion detection, there's without a doubt a want for a choice and manipulation framework to cope with problems like assault modeling, evaluation of detected threats, and choice of reaction actions. We look at the goals of designing a mathematical version for gamified cybercrime tracking in a community environment.

Introduction

The recent evolution of Information Communication Technologies (ICTs) and the substantial innovation in all sectors of life have resulted in a significant increase in productivity as well as the emergence of a wealth of new goods and services. Today we live in a digital world, where information processing is inexpensive and telecommunications costs are decreasing. It is an increasingly interconnected world. The wealth of new technical possibilities give rise not only to new products and more efficient and effective ways of doing things but also to the possibility of misuse of the technology. Like other technologies, ICTs are essentially neutral and can be used in ways that most of us would consider beneficial, as well as in ways that are harmful to our society through the internet (Rabinovitch, 2001).

Different attacker profiles exploit technological vulnerabilities in order to gather information, steal valuable assets and threaten basic services that are essential. Hence, the need for cyber security strategy is essential to provide a response to the huge challenges. Alese (2014) defined cybercrime as a vague and actually refers to a collection of dissimilar form of criminal conducts that are powered by different motives. Singer and Friedman (2014) also highlighted several factors that contribute to the proliferation of criminal actions in cyberspace to include the following; the profitability of exploiting the economy, political and other terms, the ease and low cost of employing resources to stage attacks, and the ease with which attackers can hide make it possible to carry out these activities anonymously and from anywhere in the world. Cyber criminals are becoming more sophisticated and are targeting consumers as well as public and private organizations. Therefore, additional layers of defense are needed for network security (Cruz, 2013; Halder and Jaishankar, 2012).

The continuous evolution of computer networks and mobile applications has drastically changed the nature of their security and privacy. As networks play an increasingly important role in modern society, we have witnessed the emergence of new types of security and privacy problems

that involve direct participation of network agents. These agents are individuals, as well as devices or software, acting on their behalf (Manshaei *et al.,* 2010).

The huge growth of the Internet has significantly extended the importance of Network Security Stallings. The use of game theoretic approaches to quantifying security has gain enormous research attention. Recently, there have been an increased interest in probabilistic methods for enumerating the operational security of networked computer systems (Sallhammar *et al.*, 2005).

Game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers". Game theory is mainly used in economics, political science, and psychology, as well as logic in computer science and biology. Originally, it addressed zero-sum games, in which one person's gains result in losses for the other participants. Today, game theory applies to a wide range of behavioral relations, and is now an umbrella term for the science of logical decision making in humans, animals, and computers.

Game theory is also an abstract mathematical theory for analyzing interactions among multiple intelligent actors, where the actors may be people, corporations, nations, intelligent software agents, or robots. In a security context, the intelligent actors may be security forces or police, on one hand, and adversaries on the other with which each player has a number of strategies (feasible actions), that determine the outcome of the game and the pay-off to each player (Alese *et al.*, 2014). An equilibrium outcome of a game is achieved when each player has chosen a strategy, either pure or mixed, and neither has any incentive to move to a different strategy.

Game-theoretic approaches has been used in providing mathematical basis for understanding intelligent actors' interactions with each other which assumes that these intelligent actors will anticipate each other's moves, and act appropriately (Milind and Manish, 2011).

Security games provide a quantitative framework for modeling the interaction between attackers and defenders. These games and their solutions could serve as a basis for security decision making and algorithm development as well as to predict attacker's behavior (Alpcan, 2011).

Game theory is divided into two main branches. The first is *cooperative* game theory, which assumes that the players can communicate, form coalitions and sign binding agreements. Cooperative game theory has been used, for example, to analyze voting behavior and other issues in political science and related fields. While Non-cooperative game theory models situations where the players are either unable to communicate or are able to communicate but cannot sign binding contracts. An example of the latter situation is the interaction among firms in an industry in an environment where antitrust laws make it illegal for firms to reach agreements concerning prices or production quotas or other forms of collusive behavior (Bonanno, 2015).

The rest of the paper is structured as follows; section two discusses the literature review, section three presents the proposed system design, while section four reports the results and discussion and section five presents the conclusion.

Literature Review

First coined by William Gibson in his 1984 novel 'Neuromancer', the term 'Cyberspace' is a popular descriptor of the virtual environment in which activity of internet takes place. The term cyberspace has become so common that it seems to dominate the thinking of people who consciously or subconsciously feel that they are entering a place which has new meanings, dimensions, and purposes. Internet has created new public spaces and communities. These spaces and communities are known as virtual because they are no longer linked with place or time. However, they have common interests in social, cultural and psychological realms.

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time, but the basic crime ideas remain same. The significant change in modern time is on increase in personal computing power in a globalized communication network. The networked technology has become more than simply a force multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed.

According to (Russell and Gangemi, 1991), computer security infrastructure is based on the following three main security services: ***confidentiality, integrity,*** and ***availability*** in a computer system. Confidentiality is the keeping of sensitive information from unauthorized disclosure, which means that unauthorized parties cannot access information. It is also known as secrecy or privacy. Integrity concerns the protection of sensitive information against unauthorized modifications that are not detectable to authorized users. It provides a mechanism for protecting information against accidents or malicious tampering. Finally, availability is the prevention of unauthorized withholding of information and resources. It is responsible for keeping the computer system working without degradation of access to resources for authorized users when they need it.

In cyber security, the vast number of attacker exploits and strategies that are possible can be daunting to consider. Some attacks may be opportunistic, and some may be targeted. Many cyber security risk assessment methods focus on a systems susceptibility to known exploits rather than to best withstand zero-day attacks. In cyber security game, there is more interest to assess whether good security principles have been applied and whether defenses are employed to make it as difficult for the attacker as possible (Jajodia and Noel, 2010). Given the vast number of attack methods, cyber modeling is faced with the difficult question of how to comprehensively reason about all of the cyber incident instances that are possible. It is common to consider Confidentiality, Integrity and Availability (CIA) cyber incident effects.

Computational game theory has become a powerful tool to address critical issues in security and sustainability. Game-theoretic techniques have been used to model and mitigate a variety of network security threats. Cyber Security Game takes into account the widespread interconnectedness of cyber systems, where defenders must defend all multi-step attack paths and an attacker only needs one to succeed. It employs a game theoretic solution using a game formulation that identifies defense strategies to minimize the maximum cyber risk (MiniMax).

A solution to a game describes the optimal decisions of the players, who may have similar, opposed, or mixed interests, and the outcomes that may result from these decisions, (Morton *et al* 2018).

Related Works

The area of cyberspace defense mechanism design has received immense attention from the research community in recent times. However, the cyberspace security problem is far from completely solved. Traditionally, network security solutions employ either protective devices such as firewalls or reactive devices such as Intrusion Detection Systems (IDSs). The weakness of the traditional network security solutions is that they lack a quantitative decision framework.

Cyber-attacks have created a global threat, both in defending local and global networks. Attacks are becoming more sophisticated and possess the ability to spread to numerous vulnerable hosts in a matter of seconds. It is essential to provide tools necessary in detecting, classifying, and defending from various types of attacks.

Clark *et al*. (2015) presented a game-theoretic framework for modeling the strategic interaction between an external adversary and a network of decoy nodes. The framework consists of two

components. Firstly, the interaction between the adversary and a single decoy node was studied and modeled. The adversary attempts to identify decoy nodes by examining the timing of node responses, as well as the case where the adversary identifies decoys via differences in protocol implementations between decoy and real nodes was analyzed. Secondly, the games with an adversary who attempts to find a real node in a network consisting of real and decoy nodes, where the time to detect whether a node is real or a decoy is derived from the equilibria of the games in first component was formulated.

Zhiheng and Arvind (2020) presented a game-theoretic approach to secure estimation and control for cyber-physical systems with a digital twin. The work considered a stealthy estimation attack, where an attack can modify the estimation results to deviate the system without being detected. The work is a propose work which have not been fully implemented.

Zhang et al (2015) propose a game theoretic model for defending against stealthy attacks with limited resources. Their motivation was due to high stealthy attacks which have become a major threat for cyber security and base on their previous works that fail to capture the practical resource constraints and mainly focus on one node settings. In the model, the attacker can fully observe the defender's behavior and the system state, while the defender has zero feedback information.

Hayel and Zhu (2015) reported that economic and policies issues are parts of the challenges of cyber security. The work noted that a robust cyber insurance policy could help reduce the number of successful cyber-attacks by incentivizing the adoption of preventative measures in return for more coverage and the implementation of best practices by basing premiums on an insured level of self-protection. The work proposed a game-theoretic model that extends the insurance framework to cyber security, and captures the interactions between users, insurance company and attackers. The insurance policy designed by the insurer in the framework does not require constant monitoring of users' online activities, but instead, only on the measurement of risks.

Alese *et al*. (2014) proposed game-based analysis of the network attack-defense interaction to explore the fundamentals of game-theory with respect to security and then design a system to analyze interaction between attacker and defender in a network. They present a two-player zero-sum game model of the interaction between malicious users and network administrator which they can capture the probabilistic nature of player's strategies in one model to predict the behaviors of players. The authors did not carry out a full-scale simulation of the model to attain an established result.

Durkota *et al*. (2015) presented a class of attack graph games which models the problem of optimally hardening a computer network against a strategic attacker. One challenge in network security domains is to efficiently represent the complex space of possible attack strategies. The authors considered a case where the attacker only observes the current network, but is uncertain about how the network has been modified by the defender. The study showed that modeling imperfect information in this domain has a substantial impact on the optimal strategies for the game.

Akinwumi *et al*. (2017) presented a review of game theoretic-based model for cyber security risk management. The work was not experimented as only a review of existing game theoretical approaches was only carried out.

Game theory has become quite a strong area of research for cyber security analyst and network managers.

Proposed System Design

Firstly, the game theoretical model is set as a two-player non-cooperative game such that players are define as defender and attacker respectively. While each of these forces may realistically consists of multiple entities performing various simulation actions, the sequential action of an attacker-defender scenario is best captured when each force is treated as a singular entity.
Based on the above distinction, our analysis of game problem begins with the case of two-player strategic-form (equivalently normal-form) games. The basic notions of game theory comprise of Players, Strategies and Payoffs. In the sequel, we donate players by I and II. A normal-form game is organized in the following way:
Player *I* choose a certain strategy *x* from a set *X*, while player *II* simultaneously chooses some strategy *y* from a set *Y*. The set *X* and *Y* may possess any structure (a finite set of value, a subset of R^n, a set of measurable functions etc.). As a result, player *I* and *II* obtained the payoffs as:

$H_1(x, y)$ and $H_2(x, y)$ respectively.

We define our Antagonistic or Zero-Sum game as:

$$\Gamma = \langle I, II\ X, Y, H_1, H_2 \rangle \qquad 1$$

Where

X represents the set of players *1*

Y represents the sets of players *II*,

whereas H_1 and H_2 indicate their payoff functions, $H_i : X \times Y \rightarrow R,\ i=1, 2$ where players payoffs $H_1(x,y)$ and $H_2(x, y)$ represent arbitrary function defined on the set product $X \times Y$. However, there exists a special case of normal-form games when $H_1(x,y) + H_2(x, y) = 0$ for all (x, y). Such games are called Antagonistic game or Zero-sum Game. Here both the player-attackers and defenders have opposite goals-the payoff of a player equals the loss of the opponent. It suffices to specify the payoff function of player II (Defender) for complete description of a game.
We model the interaction between the attacker and the IDS as a two-person, non-zero sum, single act, finite game with dynamic information. Given the sensor output vector d, we obtain for each subsystem $t \in T$ a threat level, y_t, using the system matrix A. Hence, we define the threat level vector as:

$$y \coloneqq Ad \qquad 2$$

The elements of *T* are then grouped into non-overlapping information sets according to their respective threat levels in *y*. Since the IDS can distinguish between information sets but not actions within them, it is a dynamic information game. Figure 1 depicts a sample security game, where t1, t2, t3 denote the attacker's actions of targeting subsystems 1 to 3, nt1, nt2 indicate false alarms (attacker doing nothing), a1, a2, a3 represent the IDS's alarms for respective subsystems, and na1; na2 denote the IDS choosing not to set an alarm.

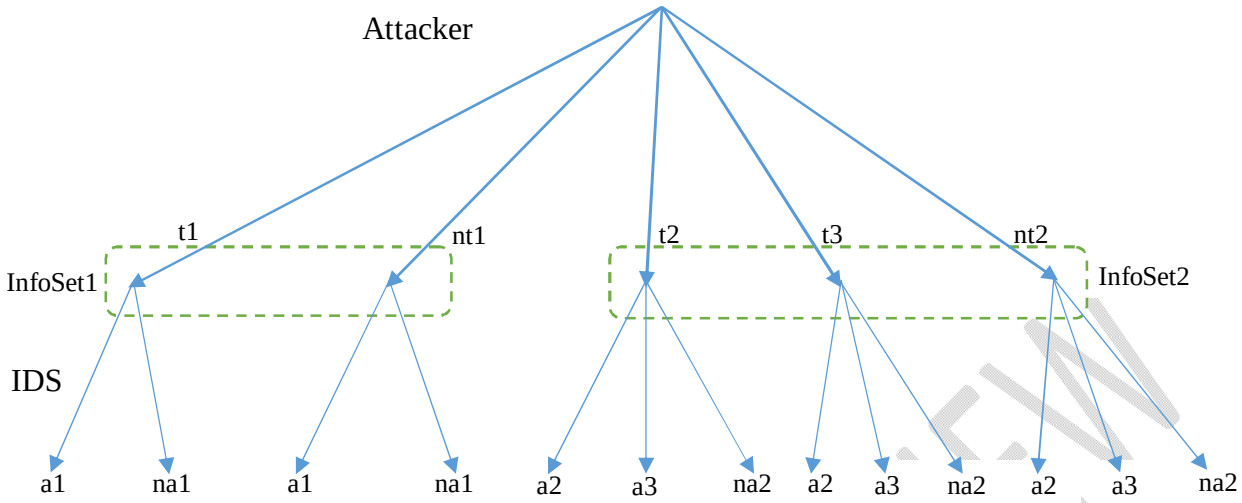

Figure 1: A security game with 3 subsystems and 2 information sets

While investigating the security game in Figure 1 recursively, information set 1 (InfoSet1) is the simplest case, where the attacker either targets subsystem one (t1) or does nothing (nt1) equivalent to a false alarm. The set of actions of the IDS are either to set the alarm for subsystem one (a1) or do nothing (na1). At information set 2, IDS has three options: set the alarm for subsystem 2 (a2) or set the alarm for subsystem 3 (a3) or do nothing (na2).
This portion of the game can be represented by the following 2 x 2 bimatrix game

$$M_{att} := \begin{array}{|c|c|c|} \hline t1 & \beta_h & -\beta_s \\ \hline nt1 & 0 & 0 \\ \hline & a1 & na1 \\ \hline \end{array} \qquad M_{ids} := \begin{array}{|c|c|c|} \hline Ti & -\alpha_h & \alpha_m \\ \hline nt1 & \alpha_f & 0 \\ \hline & a1 & na1 \\ \hline \end{array} \qquad 3$$

where the entries of M_{ids}, (M_{att}) represent the cost values, and columns (rows) correspond to the strategy spaces of the IDS and the attacker, respectively. The value $-\alpha_h$ is the gain of the IDS for detecting the target. On the other hand, α_f and α_m are the IDS's costs for false alarm and missing the attack, respectively. The cost β_h represents the detection penalty for the attacker whereas $-\beta_s$ represents the gain from an undetected intrusion. Notice that, although missing an attack is associated with a cost for the IDS, false alarms cost nothing to the attacker. The parameters α and β are always positive unless otherwise stated.
The IDS's security strategy, however, depends on the relative values of α_f and α_m, false alarm and missing (an attack) costs. If $\alpha_f > \alpha_m$ then the IDS chooses not to alarm at all (na), and if $\alpha_f < \alpha_m$ then the IDS always sets on the alarm (a1). We note that the security strategies are extremely conservative in this setting and give little insight into the dynamics of the game.

The *min-max* or security strategy of a player guarantees a maximum cost. The IDS's security strategy, however, depends on the relative values of α_f and α_m, false alarm and missing (an attack) costs.

We next investigate the existence of a Nash equilibrium (NE) in the matrix game. Notably, there is no NE in pure strategies. Therefore, we extend the analysis by considering mixed strategies of players defined as probability distributions on the space of their pure strategies.

Let p_1 and $1 - p_1$ be the probabilities for strategies (t1) and (nt) of the attacker respectively. Also let q_1 and $1 - q_1$ be the probabilities for strategies (a1) and (na) of the IDS. The pair (p^*, q^*) is said to constitute a non-cooperative Nash equilibrium (NE) solution to the bimatrix game (M_{att}, M_{ids}) if the following inequalities are satisfied:

$$p_1^*\left(\beta_h q_1^* - \beta_s(1 - q_1^*)\right) \leq p_1\left(\beta_h q_1^* - \beta_s(1 - q_1^*)\right), p_1^*\alpha_m + q_1^*\left[\alpha_f - \left(\alpha_f + \alpha_h + \alpha_m\right)p^*\right] \leq$$

$$p_1^*\alpha_m + q_1[\alpha_f - \left(\alpha_f + \alpha_h + \alpha_m\right)p^*],$$

where $0 \leq p_1, q_1 \leq 1$ and the Nash Equilibrium of the game is given as:

$$p_1^* = \frac{\alpha_f}{\alpha_f + \alpha_h + \alpha_m} \; and; \qquad 4$$

$$q_1^* = \frac{\beta_s}{\beta_h + \beta_s} \qquad 5$$

Each player pays attention only to the average cost function of his co-player, rather than optimizing his own average cost function. The probability of attacker targeting subsystem one at Nash equilibrium point decreases with decreasing α_f since the smaller the false alarm cost for the IDS, the more it is inclined to set an alarm and catch the attacker.

The equilibrium costs of the attacker V_{att}^* and the IDS V_{ids}^* for this subgame are given by

$$V_{att}^* \coloneqq [p_1^*(1 - p_1^*)]M_{att}[q_1^*(1 - q_1^*)]^T \qquad 6$$

and;

$$V_{ids}^* \coloneqq [p_1^*(1 - p_1^*)]M_{ids}[q_1^*(1 - q_1^*)]^T \qquad 7$$

where $[.]^T$ denotes the transpose of a vector.

In order to simplify the analysis, we associate the same costs with subsystems two and three. This game can also be represented as a 2 x 2 bimatrix game given by:

t2	β_h	$-\beta_d$	$-\beta_s$

$M_{att} :=$

t3	$-\beta_d$	$-\beta_h$	$-\beta_s$
nt2	0	0	0
	a2	a3	na2

8

$M_{ids} :=$

t2	β_h	$-\beta_d$	$-\beta_s$
t3	$-\beta_d$	$-\beta_h$	$-\beta_s$
nt2	0	0	0
	α_f	α_f	na2

9

where α_d (β_d) is the cost (gain) of a deception for the IDS and the attacker respectively. The sample game can be made arbitrarily large. Although increasing complexity prevents derivation of a closed form solution.

Results and Discussion

The game model provides examples of foundational game types within the context of cyber-crime scenarios as well as their solution methods. The game types and solution method therein form a basis for solving the model outlined in the research.

Figure 2 shows the explicit structure of the game model which represents the chances, players-attacker and defender (IDS). The colors represent differenct players of the game. The red stand for attacker while the blue stand for defender (IDS).

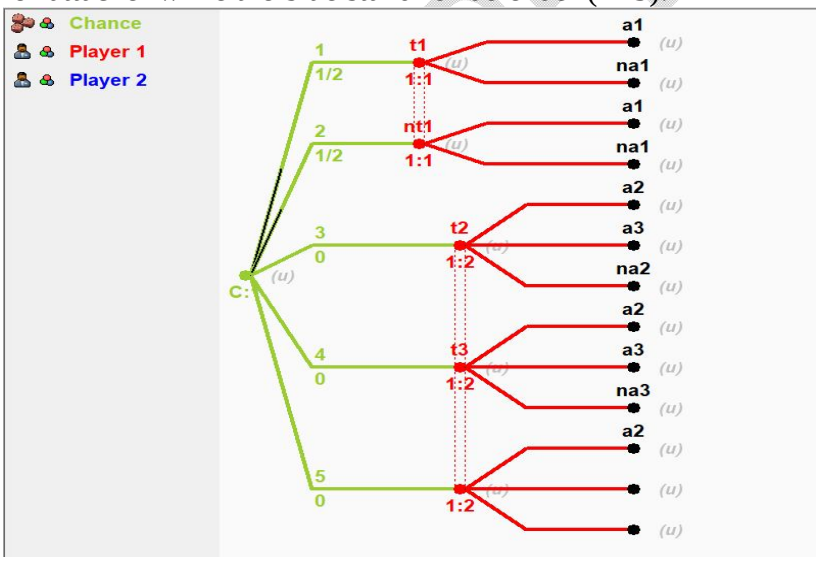

Figure 2: Explicit structure of the proposed game

The graphical user interface provides an "integrated development environment" to help visually construct the games and to investigate their main strategic features.

Computing the Nash Equilibria

The system offers broad support for computing Nash equilibria in both extensive and strategic games as shown in Figure 3.

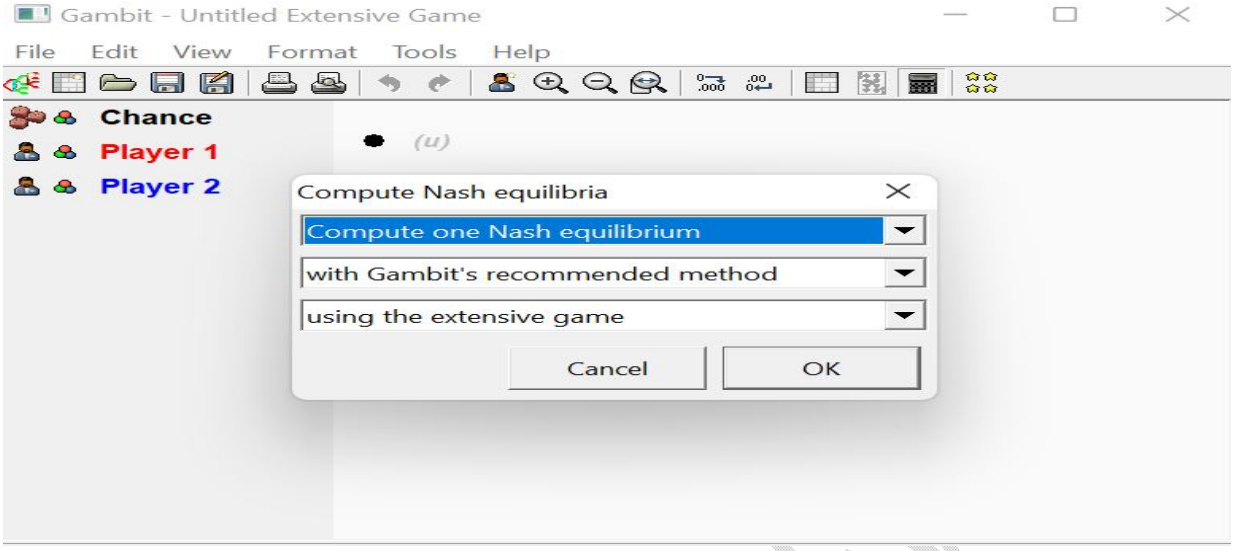

Figure 3: Computing the Nash Equilibria

The process of computing Nash Equilibria in both extensive and strategic games is similar. The system guides the options for computing Nash Equilibria in a dialog. The methods applicable to a particular game depend on three criteria:

a. The number of equilibria to compute, whether the computation is to be done on the extensive or strategic games,
b. details of the game, such as whether the game has two players or more,
c. whether the game is constant sum.

In every game, the player must first be added through the strategy table and each player is represented with different colors- red for attacker and blue for the defender (IDS) while the strategies (values) are shown accordingly in Figure 4.

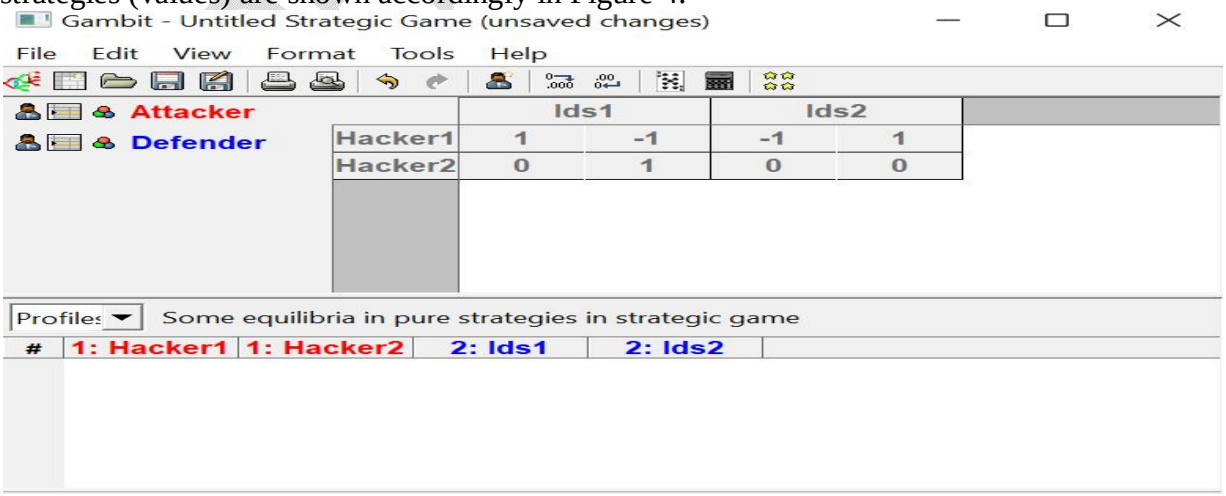

Figure 4: Computation of Nash Equilibria in pure strategy in strategic game

To validate the effectiveness, efficiency, and process of the game models, we compare different methods used to compute Nash Equilibria based on various computational methods.

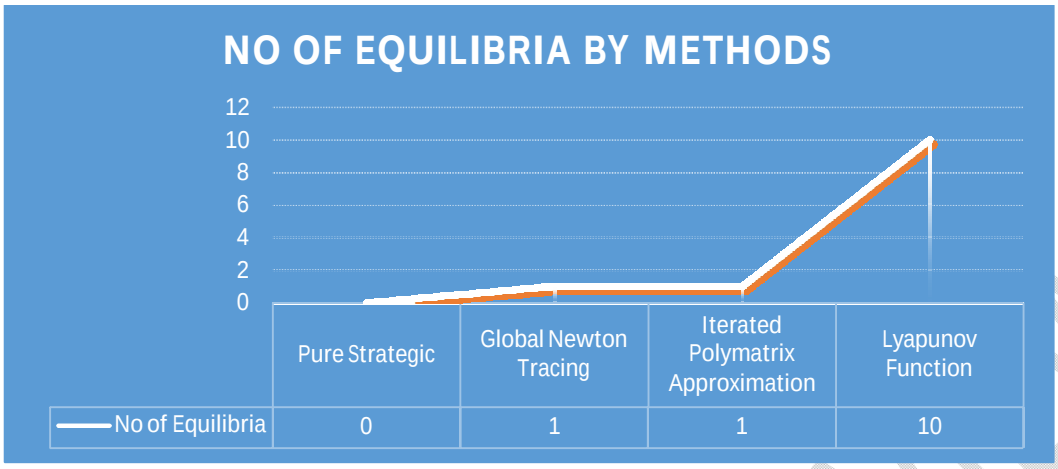

Figure 5: Nash Equilibria representation by methods

The Nash Equilibria are divided into two types. The Pure strategy Nash Equilibria which are Nash Equilibria where all players are playing pure strategies while Mixed strategy Nash Equilibria are equilibria where at least one player is playing a mixed strategy.
To validate the effectiveness, efficiency, and process of the game models, we compare different methods used to compute Nash equilibria of both extensive and strategic games. Below show the basic evaluation tables.

Table 1: Evaluation of the models

Desire Methods	Extensive game	Strategic game
Pure strategy	By default, the program computes all pure strategy Nash Equilibria. This switch instructs the program to find only pure-strategy Nash Equilibria which are subgame perfect.	It has no effect on strategic games since there are no proper subgames of a strategic game.
Global Newton Tracing	After compute, the output of the algorithm if the option is not specified, only the equilibria found are reported	Not yet tested on strategic game
Iterated Polymatrix Approximation	The model has not been extensively tested	The computation of Nash Equilibria depends on the Global newton tracing algorithms in extensive Game.
Lyapunov function	The model displays multiple equilibriums, and it is shown that the Nash equilibriums of the static game are evolutionary stable equilibrium in the game theory evolutionary set up.	By default, the program uses behavior strategies for extensive games; the switch instructs the program to use reduced strategic game strategies for extensive games which does not affect strategic games since a strategic game is its own reduced strategic game

Conclusion

Cybercrime has a serious impact on society in the form of psychological disorder, social disorganization, and economic losses. Detecting, preventing, and monitoring such crime in our society has become an issue globally hence there is a need for continuous monitoring and management of cyber security for future plans.

Game theory has been a useful and potential tool for the understanding of human affairs and expounded as a part of a general theory of rational behavior. Modeling computer networks with game theory allow researchers to be able to model and analyze both the defenders' and attackers' behavior with respect to the underlining system environment. This research work presents a unique quantitative method for controlling and monitoring network security. Also, a framework for modeling the interaction between attackers and defenders (Ids) as a non-corporative or stochastic security game was presented. By computing and analyzing in both extensive and strategic games, the results showed the possibility of predicting the strategies of the attackers, determining the resources that are most likely to be attacked, and suggesting possible defense strategies for the defender.

References

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K. & Oluwadare, S. A. (2017). A Review of Game Theory Approach to Cyber Security Risk Management. *Nigerian Journal of Technology (NIJOTECH) Vol. 36, No. 4, pp.* 1271 – 1285. *Proceedings of 6th International Conference, GameSec 2015, London, UK. Springer.*

Alpcan, T., & Başar, T. (2011). *Network Security - A Decision and Game-Theoretic Approach.* Cambridge University Press.

Bonanno, G. (2015). *University of calofornia.* Retrieved sept 2, 2022, from www.econ.ucdavis.edu: http://www.econ.ucdavis.edu/faculty/bonanno

Clark, K. Sun, L. Bushnell, and R. Poovendran (2015). A Game-Theoretic Approach to IP Address Randomization in Decoy-Based Cyber Defense. *Proceedings of 6th International Conference, GameSec 2015, London, UK. Springer.*

Cruz, A. (2013). Cyber Crime and How It Affects You. *Monthly Newsletter, 7*(1).

Durkota, K., Lisy, V. Bosansky, B. & Kiekintveld, C. (2015). Approximate Solutions for Attack Graph Games with Imperfect Information. *Proceedings of 6th International Conference, GameSec 2015, London, UK. Springer.*

Halder, D., & Jaishankar, K. (2012). Cyber crime and the victimization of women: Laws, rights and regulations. *Information Science Reference*.

Hayel, Y. and Zhu, Q. (2015). Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks. *Proceedings of 6th International Conference, GameSec 2015, London, UK. Springer.*

Jajodia, S. & Noel, S. (2010). Topological vulnerability analysis. In: Cyber situational awareness. Boston, MA: *Springer*, pp.139–154.

Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J.-P. (2010). Game Theory Meets Network Security and Privacy. *ACM*.

Milind, T., & Manish, J. (2011). *Introduction and Overview of Security Games.* University of Southern California: Cambridge University Press.

Morton, D., Stephen, D., & BramsJ. (2022, August 4). *Encyclpedia Britannical*. Retrieved from Encyclpedia Britannical: Http://www.britannical.com/science/game-theory

Rabinovitch, E. (2001). The neverending saga of internet security: why? how? and what to do next? *IEEE Communications Magazine*, 56-58.

Russell, D. & Gangemi, G. (1991). Computer Security Basics", *O'Reilly and Associates, Sebastopol, CA0*.

Sallhammar, K., Knapskog, S., & Helvik, B. (2005). Using Stochastic Game Theory to Compute the Expected Behavior of Attackers. *Symposium on Applications and the Internet Workshops*, (pp. 102-105). Trento Italy: IEEE Xplore.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar:what everybody needs to know.* NY: OXFORD UNIVERISTY PRESS.

Zhang, M., Zheng, Z. & Shroff, N. B. (2015). A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources. *Proceedings of 6th International Conference, GameSec 2015, London, UK. Springer.*

Zhiheng, X., & Arvind, E. (2020). A game-Theoritic Approach to Secure Estimation and Control for Cyber Physical Systems with a Digital Twin. *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Sydney, Australia*, 20-29.