Proceedings of Dynamic Systems and Applications 7 (2016) 303–310

Dynamic Game Theories in Cyber Security

Kandethody Ramachandran and Zheni Stefanova

Department of Mathematics and Statistics
Interdisciplinary Data Sciences Consortium (IDSC), University of South Florida
Florida, FL 33620, USA

ABSTRACT: The Internet is an integral way of conducting daily business from government agencies to entertainers. Protection from attack, damage, or unauthorized access is necessary with the increase of mobile users, digital applications and data networks. A cyber security problem can be viewed as a conflict-resolution scenario that typically consists of a security system and at least two decision makers (e.g. attacker and defender) each with competing objectives. For instance, on one hand, the defender may be interested in ensuring that the system performs at or above a certain acceptable level. The attacker's objective, on the other hand, may be to disrupt the system and degrade it. Game theory is a well-established tool that can be used to analyze such problems. In this work, we present a brief survey of how game theory can be used to find appropriate strategies for both the hacker (attacker) and the administrator (defender). We model the interactions between them as a stochastic game. Various formulations of game theory will be presented that can deal with different cyber security situations. We will present mathematical models of security systems to analyze the system's performance and to predict the likely behavior of the key decision makers that influence/control the system.

1 INTRODUCTION

The purpose of this paper will be to provide a brief survey of stochastic game methods in cyber security. The rapid development of this area explains the abundance of literature and models. Due to our specific emphasis and unintentional overlook, deserving references may not appear in this work. The primary accent when describing the variety of theories will be on how to apply these models in a cyber security set-up. In addition, the focus will be on assisting in an approachable way the potential users of this paper to discover an efficient defense mechanism that will protect their network system. As an example of the crucial role of the cyber security, the progressively-increasing use of wireless technology is making networks even more vulnerable to attacks. Nevertheless, advanced and sophisticated challenges make the classical security measures, such as a firewall, inadequate. If a hacker wants to steal data, he will not try to penetrate the firewall, but he will search for the least secure access to take over control of the system. New techniques are being constantly invented by the cyber-criminals. Therefore, we need to find effective solutions that can dynamically and adaptively defend our systems.

2 STOCHASTIC GAMES

John Von Neumann (mathematician) introduced game theory in 1928 for the first time as a mathematical instrument, used to define and solve games [37]. It is a useful, analytical and quantitative approach for characterizing interactive decision situations and also deals with problems where multiple players with conflicting objectives compete with each other. Game theory has the capability of examining several possible scenarios, before taking the best possible action, therefore it can sophisticate the decision process of the players.

2.1 A Formal Definition of a Stochastic Game

A stochastic game is a system, which consists of two or more players that follow some rules with probabilistic transition, strategically interact with each other, make decisions based on their current or past information, search for a best resolution for their current (or future) outcome and act accordingly. They can continue to play the game forever or just win or lose. A security game models the interaction between malicious attackers to system and intrusion detection systems (IDS) which allocates system resources for detection and response. A quantitative decision framework is necessary to target subjects like attack modeling, distribution of finite system resources and choices on response actions, [1], [3], [8],[13],[15],[19], [23], [24] and [36]. In this paper, we will adopt the idea that the game is played under the assumption of rationality. In cyber security situations, the following entities are basic elements of the game:

- **Players**: Players are the key agents participating in the game. We can divide them into two categories: attackers, those who attempt to harm a specific network system, and defenders, for example the administrators that are protecting it. The goal of the administrator is an optimal allocation of the resources (e.g. power, time, etc.) to successfully protect the system, while the goal of the attacker is to penetrate into our system. He might or might not be interested in minimizing his use of resources, nevertheless he would definitely like to increase the potential harm to the targeted system. Let us describe as an example, one of the most straightforward methods in the network securities used so far in a small network set-up: the firewall. Firewalls are substantially-known as a basic and a primary protection instrument, used against possible intrusion attacks (spam, Trojan horses, spyware, etc) to our system. The hackers arbitrarily search for unprotected systems by sending out pings via the Internet. The process can be compared to randomly dialing phone numbers and the computers that answer the phone are the possible victims. Any computer or a machine connected to an external network is at risk, so the firewall is like a shield between the target and the external networks. It examines the network traffic before entering the network and authorizes the transferred data using some security rule. If the data packet is uncertain, the firewall will block it. The action choices that the defender may have, are to control the access through different levels for diverse people, to train users to take preventive measures and to examine the access log continuously, etc.

- **Actions**: In each state the player makes an action. In a primary cyber security set-up the set of actions consists of two sub-sets (attack, do not attack) for the attacker and (defend, take no action) for the administrator.
- **Returns**: After all of the actions have taken place in the game, each of the players will obtain either a negative or a positive payoff. For the attacker that may be the count of penetrations in the system, the degree of trouble that he caused (the severity of the damage) and the dollar value of the resources (bandwidth, time) that he spent or saved, etc. For the defender, we can quantify the payoff as saved time, used resources and the level of importance of the information that she protected, etc.
- **Strategies**: A strategy is the players' plan of action. They consider the information from the past and also the currently-available information and make a plan to maximize their return. This will lead to the concept of Equilibrium or a solution to the game.
- **Solution**:Solution of a game is a specific state called an Equilibrium, where the attackers and the defenders, following their strategies, act accordingly to reach an optimal solution. If the Equilibrium is achieved, we will be able to build an effective response mechanism in cyber security that can run for finite or an infinite period of time.John Nash (1928-2015) was an economist and a mathematician with fundamental contributions to the game theory because of the Equilibrium that he proposed as a solution. According to the Nash Equilibrium, named by him, the goal of each game is to find a solution that provides the players with maximum possible returns, minimum costs for the specific game set-up and finally nobody is willing to deviate from this state, because it will lead to smaller returns. In this paper, we will concentrate our effort on describing stochastic games and to evaluate the different types of games, according to a specific informational structure. Since the players make their actions and strategies based on the available past or current knowledge, it is crucial to recognize the informational structure first, so that we can think of an appropriate solution to the game.

2.2 A Mathematical Definition of a Stochastic Game

Stochastic game is a dynamic game with a probabilistic transition function, which is played by one or more players. Each one of them selects a set of strategies and corresponding actions and obtains a return that depends on the current knowledge about the environment. The game can evolve to a new stage, where the player builds a strategy and acts accordingly, depending on the available information about the other players. The process can be repetitive and may be finite or infinite.

A two-player stochastic game can be represented as a set, consisting of the following elements $\{S; A^1; A^2; H; B^1; B^2; \rho\}$, where:

$S = \{s_0, s_1 \ldots s_t \ldots s_N\}$ is a nonempty state set.

$A^n = \{\alpha_1^n, \alpha_2^n \ldots \alpha_t^n \ldots \alpha_N^n\}$ is the action set of player n and α_N^n is the action of player n at state s_N. The action set for player n at state s_t is a subset of A^n, or $A_s^n \subseteq A^n$ and $\bigcup_{t=0}^{N} A_{s_t}^n = A^n$.

$H : S \times A^1 \times A^2 \times S \to [0, 1]$ is a state transition probability;

$B^n : S \times A^1 \times A^2 \times S \to \mathbf{R}$ is the benefit (payoff) function of player n;

$0 < \rho \leq 1$ is a discount factor for discounting future payoffs at the current state, described in [22].

A state transition has a payoff that is equal to the calculated value of the reward during that state; however, the reward for the next state is worth ρ times its value at the current state. The game is played as follows: game begins at an initial state $s_0 \in S$, or at a discrete time instant t , where the game is in state $s_t \in S$. Player one for example decides to select an action ${\alpha^1}_t$ from A^1 and player two selects an action ${a^2}_t$ from A^2. The reward of player one, then is $\beta_t^1 = B^1(s_t, a_t^1, a_t^2)$ and the corresponding one for player two is $\beta_t^2 = B^2(s_t, a_t^1, a_t^2)$. Then the game moves to a new state s_t or s_{t+1}, where we can define the resulting conditional probability P($s_{t+1}|s_t,\ a_t^1, a_t^2)$ which can be also represented by $H(s_t, a_t^1, a_t^2)$.

2.3 Solution of a Stochastic Game

There are a variety of algorithms that have been proposed for the stochastic game modeling. Nevertheless, solving the optimality equations and improving strategy methodology have been the most significant methods, used to define the solution to the game. Hoffman developed strategy methodology for general stochastic games [14] . In this method, the initial strategy for one of the players improves with each iteration by switching positions at which choices are not locally optimal. Furthermore, the local optimality equation method is based on building a system of constraints for the optimal expected payoffs in the game. Having optimal payoffs, one can easily create a competitive strategy. For one-player games, the local optimality equations are linear; hence, such game can be solved in polynomial time using linear programming techniques. However, for two-player games, the constraints are no longer linear and thus other methods are used, involving approximation techniques. The Nash Equilibrium suggests that despite knowing the actions of their opponents, none of the players has an incentive to modify their strategy, therefore they are better off at that state. Consequently each deviation of the Nash Equilibrium will lead to a higher level of losses. We now return to the formal model for stochastic games.

Let $\Omega^k = \{p \in \Re^k | \sum_{i=1}^{n} p_i = 1, p_i \geq 0\}$ be a set of probability vectors of length k, $w^n : S \rightarrow \Omega^{N^n}$ is a stationary strategy for player n, $w^n(s)$ is the vector $[w^n\,(s, a_1) \ldots w^n\,(s, a_N)]^T$, where $w^n\,(s, \alpha)$ is the probability that player n should use action α at state s. If we have a stationary strategy w^n, that implies that the process will not depend on time. A mixed randomized stationary strategy is the one, where $w^n\,(s, a_i) \geq 0$, for every $s \in S$ and every $\alpha \in A^n$. A pure strategy is the one, where $w^n\,(s, a_i) = 1$ for some $a_i \in A^n$.

The objective of each player is to maximize his expected return. Let s_t be the state at time t and β_t^n be the reward received by player n at time t. Therefore, the expected return will be a column vector $v_{w^1,w^2}^n = [v_{w^1,w^2}^n\,(s_1) \ldots\; v_{w,w^2}^n\,(s_N)]^T$, where:

$$v_{w^1,w^2}^n\,(s) = E_{w^1,w^2}\{\beta_t^n + \rho\beta_{t+1}^n + \rho^2\beta_{t+2}^n + \ldots \rho^N\beta_{t+N}^n\,|s_t = s\} = E_{w^1,w^2}\{\sum_{k=0}^{N}\rho^K\beta_{t+k}^n\,|s_t = s\} \tag{1}$$

$E_{W^1,W^2}\,\{.\}$ is the expected value when player n chooses an action, using probability $w^n\,(s_{t+k})$ at s_{t+k} and obtains the corresponding reward:

$$\beta_{t+k}^n = w^1\,(s_{t+k})\,B^n(s_{t+k})p^2(s_{t+k}), fork = 0. \tag{2}$$

$B^n\,(s) = [B^n\,(s, a^1, a^2)]_{a^1 \in A^1, a^2 \in A^2}, n = 1, 2$ is the player n's reward matrix in state s. If $N = \infty$ and also $\rho < 1$, then $v^n(s)$ is the expected total discounted reward that player n will receive when he starts at state s. If $0 < N < \infty$ and $\rho = 1$, v^n is the value vector of player n and if we have a stationary process the Nash Equilibrium is defined by:

$$v^1(w_*^1, w_*^2) \geq v^1(w^1, w_*^2) \forall w^1 \in \Omega^{N^1} \tag{3}$$

$$v^2(w_*^1, w_*^2) \geq v^2(w_*^1, w^2) \forall w^2 \in \Omega^{N^2} \tag{4}$$

Here w^1, w^2 is the value vector of the game for player n, when both players play their stationary strategies $w^1 \text{ and } w^2$ and $\geq$ is used to denote that the left-hand-side vector is, component wise, greater than or equal to the right-hand-side vector. At this Equilibrium, there is no mutual incentive for either one of the players to deviate from their Equilibrium strategies w_*^1 and w_*^2 A deviation will mean that one or both of them will have lower expected returns. A pair of Nash Equilibrium strategies is also known as best responses, if player one plays w_*^1 , player two's best response is w_*^2 and vice versa. Here, $w^1 \text{ and } w^2$ corresponds to the attacker's and administrator's strategies respectively. $v^1(w^1, w^2)$ is the expected return for the attacker and $v^2(w^1, w^2)$ is the expected return for the defender, when they decide to use strategies w^1 and w^2. w_*^1 and w_*^2 are the best response strategies, so Nash Equilibrium is achieved [32]. There are different concepts for a solution of a game, like min-max strategy, in Nash sense, Bayesian Equilibrium and numerous modifications of Nash Equilibrium [39]. For the purpose of this paper, we will not go over each single one of them, but we will try to outline the most important game types that exist in the relevant literature so far. We will only highlight some other possible solutions as we emphasize analyzing the interplay between the administrator and the hacker.

3 CLASSIFICATION ACCORDING TO THE INFORMATION STRUCTURE

Information plays a crucial role in game theory. The high level of importance is mainly because it provides us with an outline of different possible strategies that the players might undertake.

3.1 Dynamic Games with Complete Information

Complete information implies that each agent knows both the strategies and returns of the other agents participating in the game, but they may not be aware of the particular actions of the other players in the game.

3.1.1 Complete and Perfect Information.

A game in which each player possesses knowledge about the actions of all other players that have already taken place, is called a game with complete and perfect information. They know the strategies and the returns of the other players. In these games, the agents are aware of the complete history of the game. Usually there is one leader and then the rest of the players are being followers. As examples of complete and perfect information games, we can consider the so called two-player (administrator, attacker) general-sum and zero sum games. Let us take into account a game with two players with payoffs, represented by the following matrices:

$$\mathbf{B^1} = \begin{bmatrix} \beta_{11}^1 & \beta_{12}^1 \\ \beta_{21}^1 & \beta_{22}^1 \end{bmatrix} \text{ and } \mathbf{B^2} = \begin{bmatrix} \beta_{11}^1 & \beta_{12}^1 \\ \beta_{21}^1 & \beta_{22}^1 \end{bmatrix}$$

If the administrator has an action set of A^1= $\{{\alpha_1}^1, {\alpha_2}^1\}$ and the hacker has an action set of A^2= $\{{\alpha_1}^2, {\alpha_2}^2\}$, the payoff to the administrator is matrix B^1 and to the hacker is B^2 . When we have a zero sum game the payoff for both players is always zero:

$$\mathbf{B^1} + \mathbf{B^2}\mathbf{=0}$$

If there is a stochastic game, then we have the following situation as before: $w^1\left(s, a_1\right)$ is the probability that the administrator chooses action α in state s and $w^2\left(s, \alpha_2\right)$ is the probability that the attacker chooses action α in state s and $w^n(s)$ is the vector $\left[w^n\left(s, \alpha_1\right), w^n\left(s, \alpha_2\right)\right]^T$, where $w^n\left(s, \alpha\right)$ is the probability that player n, $n \in \{1, 2\}$ should use action a in state s. Let s_t be the state at time t and β_t^1 be the reward received by the administrator at time t , then his expected return will be a column vector : $v_{w^1,w^2}^1 = \left[v_{w^1,w^2}^1\left(s_1\right) \ldots\ v_{w^1,w^2}^1\left(s_N\right)\right]^T$, where:

$$v_{w^1,w^2}^1\left(s\right) = E_{w^1,w^2}\{\beta_{11}^1\left[w^1\left(s\right)\right] * \left[w^2\left(s\right)\right] + \beta_{22}^1\left[1 - w^1\left(s\right)\right] * \left[1 - w^2\left(s\right)\right] + \beta_{12}^1\left[w^1\left(s\right)\right]\left[1 - w^2\left(s\right)\right] \\ + \beta_{21}^1\left[1 - w^1\left(s\right)\right]\left[w^2\left(s\right)\right]|s_t = s\} \tag{5}$$

Analogically we can find the expected return for the attacker.

$$v_{w^1,w^2}^2\left(s\right) = E_{w^1,w^2}\{\beta_{11}^2\left[w^1\left(s\right)\right] * \left[w^2\left(s\right)\right] + \beta_{22}^2\left[1 - w^1\left(s\right)\right] * \left[1 - w^2\left(s\right)\right] + \beta_{12}^2\left[w^1\left(s\right)\right]\left[1 - w^2\left(s\right)\right] \\ + \beta_{21}^2\left[1 - w^1\left(s\right)\right]\left[w^2\left(s\right)\right]|s_t = s\} \tag{6}$$

The strategy pair $\left(w^1\left(s\right), w^2\left(s\right)\right)$ is the solution of the game and the Nash Equilibrium is the same as before . Lye et al. [23] suggested a two-player general sum game with complete and perfect information set-up on the cyber security situation. The authors described a game that was presented as a four node graph: file server, work station, web server and external world. There were three scenarios that were considered and also two perspectives the defenders and the attackers point of view. Nash Equilibria was calculated for both the players and then it was explained why these strategies make sense and are useful for the administrator.

There are many authors that use twoplayer zero-sum game for modeling a successful protective mechanism. For example, in the model of Nguyen et al. [28], the attacker and the network defender play a two-player zero-sum stochastic game. Again, they used nodes to model the system, but this time they made the nodes correlated to each other, depending on some weighted factors related to the security assets involved in the process and the vulnerability dependency of the nodes. The same idea was developed in [26], where the authors considered a practical example to explain and test their idea of finding an optimal strategy.

In the Stackelberg model, one of the players chooses a mixed strategy first, and the second player chooses a strategy after observing the choice of player one. Let us refer to player one as a defender (administrator) and player two as an attacker (hacker). The attacker's response function is g(.) : $w^1 \rightarrow w^2$. When we have a sequence of actions, the standard solution concept is Strong Stackelberg Equilibrium (Leitmann, 1978; von Stengel & Zamir, 2010).

A set of strategies {C, g} builds a Strong Stackelberg Equilibrium (SSE)[17] if they meet the next three conditions and order:

1.$v^1\left(w_*^1, g_*(w_*^1)\right) \geq v^1(w^1, g_*(w_*^1)), \forall w^1 \in \Omega^{N^1}$
2.$v^2(w_*^1, g_*(w_*^1)) \geq v^2(w_*^1, g(w_*^1), \forall g(w^1) \in \Omega^{N^2}, \forall w^1 \in \Omega^{N^1}$
3.$v^1\left(w_*^1, g_*(w_*^1)\right) \geq v^1\left({w_*}^1, t(w^1)\right), \forall w^1 \in \Omega^{N^1}$, where $t(w^1)$ is a set of the attackers best responses.

The difference between Nash and Stackelberg Equilibriums is mainly based on the fact whether the players will move simultaneously or one of the players will move first (the leader) and then the second one will move second (the follower). The player one's (defender's) SSE payoff has been always at least as high as his payoff in any NE.

3.1.2 Complete and Imperfect Information.

Players move at different, sequential moments and their return functions are common knowledge. At each stage of the game, they move simultaneously and at least one player is not aware of the actions of at least one other player that have taken place. Solution of that type of game is provided by Selten (1965) Sub-game-perfect Nash Equilibrium (SGPNE). A Nash Equilibrium is sub-game perfect if the strategies of the players establish a Nash Equilibrium in each sub-game. SGPNE includes not only the optimal feedback to the unique action, played in the first stage, but also provides a full plan of action (strategy) with a suggestion of what would be the most optimal approach to reply to any possible action in the unknown portion of the game (subgame).

The main problem discussed in these types of games is to determine the best strategies for the defender to diversify the risk when he builds his strategy against the attacker and to find an optimal defense strategy. Since we have a sequence of actions and there is a transition process involved, some of the authors describe the system as a Markov process. Several approaches to find a solution of the game were described in the past. Some of the most popular methods are Q-learning [7], NPL1 [9], which is an algorithm that help us to find an optimal solution with Nash Equilibrium and Shapleys method [35].

Sallhammar et al. [34] presents the network security game as a two-player zero-sum stochastic game in which there is not any interaction between the actions of the players, involved in the system. The state of the network, may or may not be a subject to change. For example, in one normal set up where there is a defending mechanism, it is possible the system to reboot because of different reasons. We can model the game as a continuous Markov process with a transition probability that can be represented by a matrix. The relationship of the players in the game will affect this transition matrix in a way that depends on the different strategies that they use. The whole process is represented as a Markov decision process (MDP) by Filar and Vrieze [9], where the transition probabilities are subject to change, depending on the players actions and also the future state can be derived from the current and previous states. The MDP turns out to be one of the most helpful approaches, which can provide us with a tool that is convenient to be calculated. It also takes into account changes that might occur in the system. In [5] we can find different optimizing mechanisms and tools for dynamic programming.

The interaction between attackers and the IDS (intrusion detection system) was presented by Alpcan et al. [2], [3] and [4] as a Markov game. They considered three possibilities for information availability, if: (a) the attacker and the defender have full information about the system, (b) the attacker has no information (c) nobody has any information for their opponent, but only about their own costs, actions in the past and the previous states. Main tools for solving the Markov decision processes (MDP) were minimax-Q [20] and naive Q-learning, described in [5] and [7]. They were used to find the best strategies of the players.

Xiaolin et al.[38] stressed the importance of risk assessment in cyber security, the authors proposed an automatic generated reinforcement Markov model that will assist the administrator in protecting the system. They considered the potential and the current security status and assessed the risk as a combination of vulnerabilities and threats. They also created a function to measure the harm caused by the attacker and it represented the level of risk involved in the process. According to this function, the administrator will select a strategy that will minimize the maximum possible damage to the system. To assess their model they considered four different sub-systems, which are united together, so a best decision process to be made. Fault Tree Analysis (FTA) were presented in [31] and [18]. They were based on Chain-of-Events Model, together with COBIT 15 [25], and were described as the basic methods for analyzing the reasons for hazards in our system . FTA consists of four steps: system definition, fault tree construction, qualitative analysis and quantitative analysis. Tree construction requires a deep evaluation of the system, stressing system issues and facilitating improvements by an analyst.

3.2 Dynamic Games with Incomplete Information

Incomplete information games are games in which at least one of the players is not aware of the possible payoffs and strategies for all other players or at least one other player. We can evaluate the case when the attacker has superior information and exploits the defender.

3.2.1 Incomplete and Perfect Information.

In this type of game the players have little information about their opponent payoff functions, but they know the past actions of all other players. An example for these games is the two-player zero-sum game that also serves as a base for the Intrusion detection mechanism. It models the interaction between malicious attackers to the system and intrusion detection systems (IDS) that allocates system resources for detection and response [3] and [6]. IDSs observe diverse events in the cyber security and examines them for signs of safety problem in the protection process. It is becoming more and more clearer that the traditional protective measures such as firewalls and reactive measures such as virus and malware detection, are not adequate to deal with sophisticated attackers. The majority of literature on intrusion detection (ID) relies on ad-hoc schemes and experimental work. A quantitative decision structure is necessary in order to utilize issues like attack modeling, the distribution of finite system resources, and outcome of the resulting actions.

Patcha et al. [30] incorporates a signaling game to present the intrusion detection mechanism. The defender has an incomplete information because he doesn't know what type his opponent is, which can be an attacker or a regular node. The authors define Θ as a set with elements θ, and this set represents the type of the attacker. Player one (the defender) for example knows his type and his actions, that are represented by α_1^1,where $\alpha_1^1 \in A_1^1$ is the action set for player one. Analogically let us suppose that player two (the attacker) will choose $\alpha_1^2 \in A^2$ and that he will experience some prior beliefs about the characteristic of the defender. In other words, let us assume the administrator believes that the probability of the attacker being a specific type is $p(\theta)$, where $\theta \in \Theta$. The return of player n will be similar as before; however, now he will also need to consider the type of the player as a part of the reward function:

$B^n\left(s\right) = \left[B^n\left(s, \alpha^1, \alpha^2, \theta\right)\right]_{\alpha^1 \in A^1, \alpha^2 \in A^2, \theta \in \Theta}, n = 1, 2$

The defender will have the following strategy: $w^1\left(s|\theta\right)$ over the actions α_1, which is conditional on the type of opponent. Analogically for the attacker the strategy will be represented by the following distribution function $w^2\left(s|\alpha^1\right)$ over actions α^2 conditional on α^1.

The payoff of θ with strategy $w^1\left(s|\theta\right)$, assuming that player two has played $w^2\left(s|a^1\right)$ is the following:

$$[B^1\left(s, \alpha^1, \alpha^2, \theta\right)]_{\alpha^1 \in A^1, \alpha^2 \in A^2, \theta \in \Theta} = \sum_{\alpha^1}\sum_{\alpha^2} w^1\left(s, \alpha^1|\theta\right) w^2\left(s, \alpha^2|\alpha^1\right) B^1\left(s, \alpha^1, \alpha^2, \theta\right)$$

If one of the players selects strategy $w^1\left(s|\theta\right)$ then the other one's reward function to strategy $w^2\left(s|a^1\right)$ will be the following:

$$[B^2\left(s, \alpha^1, \alpha^2, \theta\right)]_{a^1 \in A^1, a^2 \in A^2, \theta \in \Theta} = \sum_{\theta} p(\theta) \sum_{\alpha^1}\sum_{\alpha^2} w^1\left(s, \alpha^1|\theta\right) w^2\left(s, \alpha^2|\alpha^1\right) B^2\left(s, \alpha^1, \alpha^2, \theta\right)$$

Player two amends his beliefs about θ in order to obtain the following posterior distribution $\mu\left(s \mid \alpha^1\right)$ over Θ, where μ is a belief or a function that relates every information set with a probability measure from the past information set. In this type of game, instead of Nash Equilibrium, we will be interested to obtain Bayesian Equilibrium [21]. Therefore let $w_*^1\left(s|\theta\right)$ be the strategy used, then having information about this strategy by observing α^1, player two may use a Bayes rule to update $p\left(.\right)$ and $\mu\left(s \mid a^1\right)$.

A perfect Bayes Equilibrium of this type of game is strategy $w^*$and posterior beliefs $\mu\left(s \mid a^1\right)$, such that

$$Player1 : \forall\theta, w_*^1\left(s|\theta\right) \in arg\max_{\alpha^1} B^1\left(s, \alpha^1, \alpha^2, \theta\right)]$$

$$Player2 : \forall\alpha^1, w_*^2\left(s|\alpha^1\right) \in arg\max_{\alpha^2} \sum_{\theta} \mu(\theta|\alpha^1) B^2\left(s, \alpha^1, \alpha^2, \alpha\right)$$

$$\mu\left(\theta \mid \theta^1\right) = \frac{p\left(\theta\right) w_*^1\left(s, \alpha^1|\theta\right)}{\sum_{\theta' \in \Theta} p(\theta') w_*^1\left(s, \theta^1|\theta'\right)} \tag{7}$$

Where $\sum_{\theta' \in \Theta} p(\theta^{'}) w_*^1\left(s, \theta^1|\theta^{'}\right)$ is strictly positive and $\mu\left(s \mid \alpha^1\right)$ is a probability distribution on Θ.

A Perfect Bayesian Equilibrium is a set of strategies and beliefs that at any stage of the game we have an optimal strategy, conditional on the beliefs that are obtained from the game using Bayes rule. Perfect Bayesian Equilibrium is always Nash Equilibrium, but not the other way around. Given the players' beliefs, the strategies must be sequential, i.e. at each information set the actions taken must be optimal [30].

Nguyen et.al [27] described the network security problem as a many nonzero-sum games that are played in a sequence by the attacker and the defender. Nguyen et al. observed this type of game as a fictitious play, because the participants did not know the previous actions of their opponents. The authors observed the influence of the so called error probabilities in the process and they considered the implementation of a sensor system based on two main scenarios: (a) each player knows the error probabilities, and (b) none of them knows it. Other authors also considered the fictitious play in their analysis. For example, in [22], Luo et al. proposed a model to handle uncertainty between one attacker and the attacked object. In a similar way Liu et al. [21] developed a Bayesian game in a wireless network. Each node was assigned a transition probability and two schemata were discussed: a fictitious and a gradient play, as the players amend their probabilities at the end of each stage.

3.2.2 Incomplete and Imperfect Information

Incomplete and imperfect information implies that at least one player is not aware of the previous actions and payoff functions of the other players. Depending on the methodology the different authors use, there might exist two main categories: Dynamic games of Incomplete and Imperfect information using a Bayesian approach and Dynamic games of Incomplete and Imperfect information using the non-Bayesian approach.

3.2.3 Dynamic games of Incomplete and Imperfect information using a Bayesian approach

One possible representation of these types of games is the Two-payer hybrid Bayesian type of a game, the players amend their beliefs about the type of the their opponent. The solution of the game is a sequence of optimal one-stage strategies, based on the new beliefs. For example, in [21] the authors suggest several possible solutions with the Bayesian approach to solve a game with incomplete and imperfect information. Each player tries to maximize his return function and the game has a mixed-strategy Perfect Bayesian Equilibrium. They considered a novel Bayesian hybrid detection approach and the Equilibrium strategies is helpful for reducing energy and resources on one hand and to find highest payoff for the hybrid detection approach on the other.

3.2.4 Dynamic games of Incomplete and Imperfect information using a non Bayesian approach

The authors in [39] designed a model of interaction between the hacker and the defender. They suggested that this model could be represented as a repeated game of incomplete information. The solution of their game was made with linear algorithms and they provided a deep insight of the Bayesian and Nash Equilibriums. They also suggest that the Mini-Max Theorem [29] and the linear programming [22] can be used to solve this kind of two-player zero-sum game. Additional research for these type of games is made in [3], [27] and [30].

4 OTHER RELATED WORK

Game theories are a useful tool for modeling and predicting the behavior of the attackers and the defenders in the system. There are many challenges involved when we have to find the solution of the game or the Equilibrium, because of computational problems, data availability, or practical implementation of the different stochastic games. Although all of the upper mentioned authors dedicated their research to formulating the problem as a strategic game, there are many challenges because of the difficulties in measuring the risk, the resources and all factors, involved in the process.

Sallhammar, et al. [33] and proposed an approach of integrating reliability and cyber security. They implemented a stochastic game to predict the hackers' behavior. The basic idea is to evaluate the connection between hacker and administrator as a two-player zero-sum game. They were able to analyze each state and to model the relationship between the sets of the system of states and each single state in the stochastic game model. Then, they have calculated the transition probabilities and solved the Markov model.

Hansman and Hunt [12] proposed a taxonomy involving four distinct dimensions. As a whole their classification system covers network and computer attacks, providing assistance in network security by improving the consistency in the language which is describing the different types of attacks. They suggested that a reliable language with detailed description of the distinct attack types, can ameliorate the system. The first dimension is helping the administrator to categorize the attack, the second dimension stresses on the classification of the targets. The third dimension represents the process of grouping in different vulnerability levels. The final dimension describes the potential effects that will be involved before the final action.

Hausken [11] also used a strategic reliability approach to describe the game model. His work recommends different techniques, depending on the type of the network. He uses Markov analysis to repeated games and studies the strategic defense of a system, which has been targeted by multiple attackers. Hausken takes into account the essential dissimilarities of the network elements and considers several parallel and complex series of defensive techniques. In [10], the authors describe the optimality process of a possible interaction between the hackers, depending on the information structure and availability. They consider a process of building a shared information platform among the hackers so that the hackers can be aware of the level of vulnerabilities among the different protected systems. That implies that the weakest systems will be targeted and there are better chances of a successful attack on the protected system.

Kjaerland [16] proposed a taxonomy of cyber-intrusions to profile cyber-criminals and victims. He's major insight is an emphasis on the examination of both the attacker and the defender. He also focuses on reported cyber intrusions by Computer Emergency Response Team CERT. These attacks were analyzed using facet theory and multidimensional scaling (MDS) represented by the following categories: a Method of Operation, Target, Source, and Impact. He concluded the paper by comparing the incidents of commercial versus government attacks and stressed the importance of understanding intrusions.

5 CONCLUSION

This paper demonstrates a promising future application and efficiency of the game theory. Additional research needs to be done in analyzing the strategies and the solutions of the players, according to the different informational structure in cyber security. Furthermore, there is the existence of different challenges associated with the theoretical framework and the practical application of the possible variety of games. It can be stated that there are some problems in quantifying the diverse factors that define the game. So far, the applied research on game theories has been limited to the computation of the Nash Equilibrium and the use of other related classical theories. However, new and advanced methods need to be implemented to account for the fast developing cyber environment and the innovative strategies, invented by the attackers nowadays. Firewalls and other intrusion detection mechanisms may be useful for our basic protection, but new and high-tech software and hardware applications are needed in order for the administrator to be able to create a quick and adequate response to each possible attack.

REFERENCES

[1] A. Agah, S. Das, K. Basu, and M. Asadi, *Intrusion detection in sensor networks: A non-cooperative game approach*, 3rd IEEE International Symposium on Network Computing and Applications (2004) 343-346.

[2] T. Alpcan and L. Pavel, *Nash Equilibrium design and optimization*, International Conference on Game Theory for Networks, GameNets, (2009).

[3] T.Alpcan and T.Basar, *An intrusion detection game with limited observations*, 12th Int. Symp. on Dynamic Games and Applications, Sophia Antipolis, France, (2006).

[4] T. Alpcan, and T. Basar, ***Network Security A decision and game-theoretic Approach***, Cambridge University press, (2011).

[5] D.Bertsekas, ***Dynamic programming and optimal control***, 2nd ed. Belmont, MA: Athena Scientific, 2 (2001).

[6] M. Bloem, T. Alpcan, and T. Basar, *Intrusion response as a resource allocation problem*, IEEE Conference on Descision and Control, (2006).

[7] P. Bommannavar, T. Alpan and N. Bambos, *Security Risk Management via Dynamic Games with Learning*, IEEE International Conference on Communications, (2011) 1-6.

[8] A. Burke, *Towards a game theoretic model of information warfare* Masters thesis, Air Force Institute of Technology, Air University, 1999.

[9] J. Filar and K. Vrieze, ***Competitive Markov decision processes***, Springer, Berlin Heidelberg. New York, (1996).

[10] A. Ghose, and K. Hausken, *A Strategic Analysis of Information Sharing Among Cyber Attackers*,Social Science Research Network (2007).

[11] L. Hausken, H.R. Rao, S.J. Upadhyaya *Security Investment, Resource Allocation and Information Sharing for Strategic Defenders and Attackers of Information Assets and Networks*, Annals of Emerging Research in Information Assurance, Security and Privacy Services, A Handbook in Information Systems, Elsevier, Forthcoming, (2008).

[12] S. Hansman and R. Hunt, *A taxonomy of network and computer attacks*, Computer and Security, (2005).

[13] D. Han, D. Niyato, W. Saad, T. Baar, and A. Hjorungnes, ***Game Theory in Wireless and Communication Networks: Theory, Models, and Applications***,Cambridge University Press, (2011).

[14] A.J. Hoffman,R.M. Karp, *Nonterminating Stochastic Games*, Management Sciences (Series A),12 (1966) 359-370.

[15] E.O. Ibidunmoye ,B.K. Alese , O.S. Ogundele, *A Game-theoretic Scenario for Modelling the Attacker-Defender Interaction*, Computer Engineering Information Technology, (2013).

[16] M. Kjaerland, *A taxonomy and comparison of computer security incidents from the commercial and government sectors*, Computers and Security, 25 (2005) 522-538.

[17] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, Journal of Artificial Intelligence Research, 41 (2011) 297-327.

[18] G. Leveson, *Fault Tree Analysis* in Safeware, Addison-Wesley, (1995) 317-326.

[19] Y. Lin, Y. Wang, Y. Wang, and H. Zhu, *Stochastic Game Nets and Applications in Network Security*,Journal of Computers, (2009) 461-467.

[20] M. L. Littman. *Markov games as a framework for multiagent reinforcement learning*, Proc. of the 11th International Conference on Machine Learning, (1994) 157-163.

[21] Y. Liu, C. Comaniciu, and H. Man, *A bayesian game approach for intrusion detection in wireless ad hoc networks*, Proc. 2006 workshop on Game theory for communications and networks, (2006).

[22] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, *Game Theory Based Network Security*, Journal of Information Security, 1 (2010) 41-44.

[23] K.W. Lye and J. Wing,*Game strategies in network security*, Foundations of Computer Security Workshop in FLoC 02, Copenhagen, Denmark, (2002).

[24] D. McMorrow, ***Science of Cyber-Security***, MITRE Corporation report, (2010).

[25] R. Meadows, ACA, *COBIT 5 for Information Security*, in COBIT 5 for Information Security, IL, 23 (2012) 55-59.

[26] A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell, *Security investment games of interdependent organizations* Proceedings of the 46th Allerton Conference, (2008).

[27] C. Nguyen, T. Alpcan, and T. Basar. *Security games with incomplete information*, Proc. of IEEE Intl. Conf. on Communications (ICC), (2009).

[28] C. Nguyen, T. Alpcan, and T.Basar, *Stochastic Games for Security in Networks with Interdependent Nodes*, IEEE, (2009) 697-703.

[29] G. Owen, ***Game Theory***, Academic Press, 3rd edition, (2001).

[30] A. Patcha and J. Park, *A game theoretic approach to modeling intrusion detection in mobile ad hoc networks*, Proc. 2004 IEEE workshop on Information , Assurance and Security, (2004) 280 - 284.

[31] Y. Patil, P. Zavarsky, D. Lindskog and R. Ruhl, *Fault Tree Analysis of Accidental Insider Security Events*, International Conference on Cyber Security, Washington D.C., (2012).

[32] K. M. Ramachandran, and C. P. Tsokos, ***Stochastic differential games: Theory and Applications***, Atlantis Studies in Probability and Statistics, Volume 2, Atlantis/Springer Press, (2012).

[33] K. Sallhammar, B. E. Helvik and S. J. Knapskog, *Towards a Stochastic Model for Integrated Security and Dependability Evaluation*, 1st International Conference on Availability, Reliability and Security, Washington, (2006).

[34] K. Sallhammar, S. Knapskog, and B. Helvik, *Using stochastic game theory to compute the expected behavior of attackers*, Proc. 2005, International Symposiu on Applications and the Internet Workshops, (2005) 102-105.

[35] L. Shapley, *Stochastic games*, Proc. National Academy of Science USA, Vol 39, Issue 10, (2007), 1095-1100.

[36] S. Shiva, R. Sankardas, H. Bedi, D. Dasgupta, Q. Wu, *A Stochastic Game Model with Imperfect Information in Cyber Security*, Computational Intelligence in Cyber Security CICS, (2011) 129-136.

[37] J.von Neuman *Zur Theorie der Gesellschaftsspiele*, Math. Ann. ,100 (1928) 295-332.

[38] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng. *A markov game theory-based risk assessment model for network information systems*, International conference on computer science and software engineering, (2008) 1057-1061.

[39] X. You and Z. Shiyong, *A kind of network security behavior model based on game theory*, Proc. Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, (2003) 950-954.