Game-based Analysis of the Network Attack-Defense Interaction

Boniface K. Alese, Emmanuel O. Ibidunmoye, D.I. Haruna, Aderonke F. Thompson, Iyare Otasowie.

Abstract-**The interactive behavior between the attacker and the defender in a network environment is similar to information warfare where both attacker and defender may have several available strategies to achieve maximum gratification. The process of positioning security within a network environment is synonymous to a decision-making process. Security decision-making involves the allocation of scarce network security resources to counter or mitigate security attacks. To ensure effective security, security decision-makers must ensure that the resources are allocated and deployed in the most optimum manner. Game theory provides a quantitative framework for the analysis and modeling of such network security cases. Game-theoretic models view network security scenarios as an optimization game comprising of multiple players notably the attackers (malicious users) and the defenders (system administrators) and has become a major source of attraction in security research. These types of games are referred to as security games. Security games and their solutions are potential tools for security decision making and algorithm development as well as for predicting attacker behavior. In this paper, we first explore the fundamentals of game-theory with respect to security, and then presents a two-player zero-sum game model of the interaction between malicious users and network administrators. A description of the major components of such game is presented and a solution technique for solving such game scenario is proposed. We then describe how expected results can be analyzed to show the optimality of resulting strategies and how they may be employed by system administrators to better protect the network.**

Index Terms **- security games, strategies, attackers, defenders, stochastic games, deterministic games, game theory.**

I. INTRODUCTION

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 [1].

The huge growth of the Internet has significantly extended the importance of Network Security [2]. It is obvious that many Internet systems and components are prone to security risks [3]. Such risks are inevitable since some parts of a large system such as the Internet with many computers and a wide range of software are expected to have weaknesses that expose them to security attacks. Such risks have led to successful and well-publicized attacks. Typically, an attack exploits the discovery of loopholes in the security mechanisms of the Internet; the latter are also known as defenses.

Security attacks and defenses are currently attracting a lot of interest in major forums of communication research. The contemporary technical jargon is information warfare and network security, and there are valid reasons for their rise in importance. Throughout the evolution of networking and the internet, the threats to information and networks have risen drastically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. A current challenge is to invent and study appropriate theoretical models of security attacks and defenses for emerging networks similar to the Internet [4].

Network security, when viewed from a game theoretic perspective, can be seen as a game comprising multiple players; the attackers (malicious users) and the defenders (network/system administrators). Game theory can provide us with the mathematical framework for analysis and modeling of network security problems, and it can be used to compute optimal strategies for all party. The benefit of quantifying network security using game-theoretic approach is enormous. Most importantly, it may help network administrator to find the optimal defense strategies of a system and to calculate the expected loss associated with different defense strategies [5].

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 [6]. 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 [7].

Manuscript received August 29, 2013; Revised on October 11, 2013.

B.K. Alese is with the Federal University of Technology, Akure, Nigeria, e-mail: bkalese@futa.edu.ng , +2348034540465

E.O. Ibidunmoye is with the Federal University of Technology, Akure, Nigeria, e-mail: muyi.ibidun@gmail.com, +2348066851683

D.I Haruna is with the Nigerian Building and Road Research Institute, Sango-Otta, Akure, Nigeria.

A.F. Thompson is with the Federal University of Technology, Akure, Nigeria, e-mail: afthompson@futa.edu.ng, +2348034897857

O. Iyare is with the Federal University of Technology, Akure, Nigeria, e-mail: oiyare@futa.edu.ng, +2347033513174

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Security games vary from simple deterministic to more complex stochastic; they are applicable to security problems in various areas, ranging from intrusion detection to social, wireless, and vehicular networks. In stochastic games, the play proceeds by steps from position to position, according to transition probabilities controlled by the two players [8]. [7], in addition, stated that stochastic games aim to capture the unknown and uncontrollable parameters in security problems. It analyses the behaviour of rational attackers as a probability distribution over the possible attacks

II RELATED WORKS

Network security has gained significant attention in research and industrial communities as a result of the global connectivity provided by the Internet [9]. This has led to a variety of traditional defense mechanisms ranging from cryptography, firewalls, antivirus software, to intrusion detection systems.

Security decisions have recently been investigated analytically. Analytical approaches present a number of advantages compared to heuristic and adhoc approaches [7]. Many mathematical models have been used to model and analyze the decision making problems in security. Machine Learning [10], Control Theory [11], and Data Mining [12] are mathematical models that have been utilized to model security problems. However, these attempts fail to capture the ability of attackers to intelligently choose their targets and alter their attack strategies based on the defensive schemes that are put in place by defenders [13]. Thus, they are not suitable for modeling the interaction with dynamic, pro-active, and cognitive adversaries [14]. [6] provides a formal way of describing the security of a system via his attack trees which are, though novel, often exponentially explosive.

The use of game-theoretic approaches to quantify security has gained enormous research attention. More recently, Game Theory has been used to study network security problems [15], [7], [16], [5]. Recently, there has been increased interest in probabilistic method for quantifying the operational security of networked computer systems [17]. Security games provides the capability of examining hundreds of attack scenarios and offers methods for indicating several potential course of actions with accompanying predicted outcomes [16]. Computer implementations of those methods can result in intelligent and automated security decision engines that are fast and time scalable. A study of [15] and other researches view stochastic games as a non-linear programming problem that could be solved using dynamic programming algorithms, iteration algorithms or any other similar approaches. Furthermore, the works of [7], [5] consider attacker-defender interactions as general-sum games. Consequently, in this paper we investigate how attack scenarios can be analysed as a zero-sum two-player games and the possibility of viewing such as linear programming problems that could be solved using simple linear algorithms.

III GAME-THEORY

Game theory is 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. In providing a mathematical basis for understanding intelligent actors' interactions with each other, game-theoretic approaches assumes that these intelligent actors will anticipate each other's moves, and act appropriately [18]. Each player has a number of strategies (feasible actions), which determine the outcome of the game and the pay-off to each player. 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. This happens only when a max-min strategy of one player gives the same outcome as a min-max strategy of another player [19].

Over the years, game theory has been applied to different decision problems, it was not until mid 1990's that it was applied to networking problems such as flow control, congestion control, routing and pricing of Internet services. More recently, there has been growing interest in adopting game-theoretic methods to model today's leading communications and networking issues, including power control and resource sharing in wireless and peer-to-peer networks [20].

Game Theory shares many common concerns with the information security problem [21]. In Game Theory, a player's outcome depends not only on his decisions, but also on those of his opponents. Similarly, the success of a security scheme depends not only on the actual defense strategies that have been implemented, but also on the strategic actions taken by the attackers to launch their attacks. It also depends on the actions of the users that are sharing the systems, and on the actions of their peers situated in other networks. All these agents act rationally according to their various incentives. It provides means to represent these complex, competitive, and multi-agent interactions into mathematical models that allow a rigorous analysis of the problem [21]. This also helps the agents predict each other's behavior and suggests a course of action to be taken in any given situation.

A game is typically made up of several basic components as defined below.

i. Player: A basic entity in game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.
ii. Action: An action constitutes a move in the given game.
iii. Payoff: The positive or negative reward to a player for a given action within the game.
iv. Strategy: Plan of action within the game that a given player can take during game play.

Games are represented in two ways; Extensive form games or Normal form games. The extensive form can be used to formalize games with a time sequencing of moves. Games are

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

played on trees where each vertex (or node) represents a point of choice for a player. The player is specified by the numbers listed by the vertex. The lines out of the vertex represent a possible action for that player. The payoffs are specified at the bottom of the tree. The extensive form can be viewed as a multi-player generalization of a decision tree [22] which can be analysed directly or converted to equivalent strategic normal game. The normal or strategic form game is a matrix representation of a simultaneous game. For two players, one is the "row" player, and the other, the "column" player. Each row or column represents a strategy and each box represents the payoffs to each player for every combination of strategies. Generally, such games are solved using the concept of Linear Programming and Nash equilibrium [23].

There are different types of games used in modeling different situations;

a. Cooperative vs. Non-Cooperative Games

A game is cooperative if the players are able to form binding commitments. In non-cooperative games this is not possible. Often it is assumed that communication among players is allowed in cooperative games, but not in non-cooperative ones. Non-cooperative games are able to model situations to the finest details, producing accurate results. Cooperative games focus on the game at large. The essential difference between the two branches is that in non-cooperative game theory the basic modeling unit is the individual (including his beliefs, preferences, and possible actions) while in cooperative game theory the basic modeling unit is the group [24].

b. Zero-Sum and Non-Zero-Sum Games

Zero-sum game is a mathematical representation of a situation in which a participant's gain (or loss) of utility is exactly balanced by the losses (or gains) of the utility of other participant(s). Therefore, the total benefit to all players in the game, for every combination of strategies, always adds to zero. Zero-sum games depicts situation in which the choices by players can neither increase nor decrease the available resources. Informally, in non-zero-sum games, a gain by one player does not necessarily correspond with a loss by another. Such games are called Constant-Sum or General-Sum Games correspond to activities like theft and gambling, but not to the fundamental economic situation in which there are potential gains from trade [23].

c. Simultaneous and Sequential Games

A sequential game is one in which players make decisions (or select a strategy) following a certain predefined order, and in which at least some players can observe the moves of players who preceded them. Sequential games are represented by game trees (the extensive form) and solved using the concept of rollback, or sub-game perfect equilibrium [23]. A simultaneous game is one in which all players make decisions without knowledge of the strategies that are being chosen by other players [23]. Simultaneous games are represented by the normal form and solved using the concept of Nash equilibrium.

d. Perfect Information and Imperfect Information Games

A game is perfect if all players know the moves previously made by all other players. It is an important subset of sequential games, and thus, only sequential games can be games of perfect information, since in simultaneous games not every player knows the actions of the others. Research in artificial intelligence has addressed both perfect and imperfect (or incomplete) information games that have very complex combinatorial structures (like Chess, Go, or Backgammon) for which no provable optimal strategies have been found.

Depending on their representations and classification, games are solved using different concepts. A solution is an outcome of a game that is interesting in some aspect. The solution concepts for different classes of games are:

a. Normal form general-sum games - Dominant strategy equilibrium, Rationalizability, Iterated strict dominance, Nash equilibrium, and Correlated equilibrium.
b. Normal form zero-sum games: Linear Programming, Value Iteration Algorithm
c. Extensive form games - Backward induction, Subgame perfect equilibrium, and Sequential equilibrium.
d. Incomplete information games - Bayes-Nash equilibrium and Perfect Bayesian equilibrium.

IV SECURITY AS A DECISION-MAKING PROCESS

In [7], it is opined that there is a fundamental relationship between security and decision making. Whether it is about buying a simple lock versus installing an expensive alarm system in a house, deploying a security suite on a personal computer, or applying a patch to a production server, decisions on allocating limited resources while balancing risks are at the center of network security, making such decisions in a principled way instead of relying on heuristics provides numerous advantages.

Security decisions allocate limited resources, balance perceived risks, and are influenced by the underlying incentive mechanisms. Although they play an important role in everyday security, they are often overlooked in security research and are usually made in a very heuristic manner. Relying on human security expertise is problematic due to the sheer scale and complexity of modern networks. Alternatives to human-base security decision-making are quantitative approaches based on mathematical models (such as provided by game-theory) which can then be solved automatically with computers and deployed in real-time. Game theory provides the mathematical tools and models for investigating multi-person strategic decision making where the decision makers compete for limited and shared resources. The strength of game theory is the methodology it provides for structuring and analyzing problems of strategic choice.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

V THE SECURITY ATTACK-DEFENSE GAME MODEL

How to quantify the threat probability in network security risk assessment is an important problem to be solved. However, the decision to perform the attack is a trade-off between the gain from a successful attack and the possible consequences of detection; meanwhile, the defender's security strategy depends mostly on the knowledge of the intentions of the attacker. Here, an Attack-Defense game model which quantifies the probability of threats is proposed. Due to the complexity of practical computer networks and hence their security provisioning procedure, this framework is two pronged. First we describe the attack-defend scenario as a zero-sum stochastic game due to the stateful and probabilistic nature of such interaction. Secondly we then describe a one-shot deterministic game played at each state of the game.

Consider a two-player zero-sum game played on a finite state space, where each player has a finite number of actions to choose from. We formally define our two-player stochastic game as a tuple as defined in (1).

$$G = (S, P, (A_i, \propto_i, U_i)_{1 \le i \le |P|}, Q) \quad (1)$$

Game G is composed of a finite set of states S, and players P and for every player, there exists a finite set of actions A_i. At every state, α_i is a mapping of the set of actions available to a player in that state i.e. $\alpha_i : S \to A_i$. Let $S\alpha$ be the set of all possible action profile for each player such that $S\alpha = \{(s, a): s \in S, a = (a_i),\ a_i \in \alpha_i(s);\ 1 \le i \le |P|\}$, then the mapping $U_i : S\alpha \to R$ assigns a state payoff to each player when the corresponding action profile is played while mapping $Q : SA \to P(S)$ is a probability distribution over the state space S. The values of Q determins whether the game ends at a particular state or whether the game transit to another state.

a The Network Environment

A typical security game is played over a computer network environment made up of several interconnected components (assets) and game actors. The game actors often are network/virtual users, normal users attempting to accomplish a task, attackers who exploit vulnerabilities and defenders whose responsibility is to secure the network from malicious threats to both internal and external factors. Figure 1 depicts a typical network environment which consists of several interconnected components. These components include:

(i) Application Server: This provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

(ii) Web Server: This refers to either the hardware (the computer) or the software (the computer application) that helps to deliver Web content (web page) that can be accessed through the Internet.

(iii) Database Server: This refers to a computer program that provides database services to other computer programs or computers, as defined by the client–server model (MySQL, oracle) that rely exclusively on the client–server model for database access.

(iv) Print Server: This is a device (usually computer) that connects printers to client computers over a network. It accepts print jobs from the computers and sends the jobs to the appropriate printers.

(v) Client: This is an application or system that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network.

(vi) Network Hardware: This refers to the equipment which typically enables computers to network and communicate, include hardware such as switches, routers, cables(wires that connects the computing devices together in a network)

(vii) The Internet: This is the global system of interconnected computer networks that use the standard Internet protocol suite to serve billions of users worldwide.

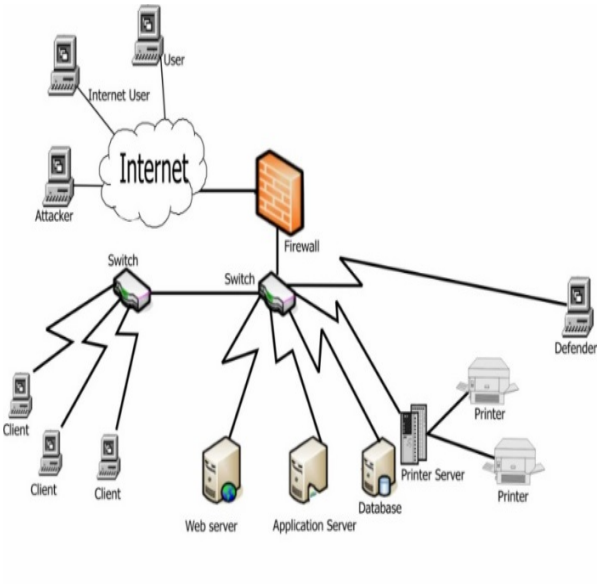

Fig 1: Typical Network Environment

b. Game Cost, Actors & Strategies

Attacker's actions are mostly associated with rewards measured in the amount of damage done to any network asset, while defenders mostly have loss in terms of cost. When an attacker successfully wreck havoc on a network component, it may take the *defender* say *X* to *Y* minutes to figure out which service or component is affected and restore it to operation. Therefore, in this work, the *attacker's* rewards are defined in terms of the amount of time required by the *defender* to put the affected asset to a working state. In practical cases it is expected that assigned cost of each network component is dependent on its perceived value. Actors in a game are the players whose intents are to either maximize gains or minimize losses. Let a player p_1, be the *defender* with strategy set $p_1^a = \{a_1, a_2 \ldots . a_n\}$, and p_2 be the *attacker* with strategy set $p_2^a = \{a_1, a_2 \ldots . a_n\}$.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

c Modeling Game States & Movements

Stochastic security games are played between players on a finite state space (representing the environment upon which the game is played) that moves probabilistically from state to state. We adopt the [7] design of state as an operational mode of the networked system, in which units are fully, partially operational, or completely out of operation. [15] modeled the state of a network as one containing various kinds of information or features such as type of hardware, software, connectivity, bandwidth and user privileges. Our game transits from one state to another according to a probability distribution. The state transition probability is a function of both the players' actions, and the current state. These probabilities do not only determine state movements they are also incorporated into a solution method to influence both the value of the game and the optimal mixed strategies for the players. A Stochastic game G, consists of a finite set of states or positions $S = \{s_1, s_2, s_3, \dots \dots, s_t\}_{1 \le t \le |S|}$ that represent the underlying network environment, one of which is assigned the *start* state. Associated with each state s_k is a matrix game G^k. Transitions from state s_k to another s_l depends on the outcome of G^k and a probability$P(s_l)^k$ interpreted as, at state s_k, the game transit to state s_l with a probability $P(\ s_l)^k$. Where P^k is a probability distribution over the state space and so it holds that $0 \le P^k \le 1,\ \sum_{k=1}^{|S|} P^k\ \forall\ k$. Game matrix G^k is however a one-shot deterministic game whose outcomes determines the next course of the game.

The choice of encoding scheme is a factor of the problem and the complexity of the network under modeling. For complex networks (such as the Internet), the components and interconnections are modeled as nodes/vertices and link/edges of a giant graph network. For small-scale networks (intranets), we propose a linear binary representation scheme. The binary representation scheme encodes a state as a binary string of zeroes (0's) and ones (1's) of length equal to the number of network components. Each component is represented with a 1 (ON) if in operation and 0 (OFF) if not. Therefore the total possible number of state could easily be factored. A sequence of bits to represent each state string is generated according to a priority indicate the security importance of an asset and the position of such asset in the network or the order in which packets traverse the network.

d. Computing Game Payoff Matrices

At each state, a one-shot deterministic game is played between the two players. Each state game is in the strategic form represented as a two-dimensional matrix. Let the *defender* be the row player, while the *attacker* be the column player. The elements of the matrices are payoffs to be either gained or lost when each player play the corresponding action in their strategy profile for that state. The base matrix (start game) is purely deterministic while movements to subsequent state matrices are mostly probabilistic due to the influence of transition probabilities. At s_k, we define $G^{(k)}$ as;

$$G^{(k)} = (a_{i,j}^k + \sum_i^N P_i^{(l)}\, G^{(l)})\ , k = 1..N \qquad (2)$$

At each state k, players simultaneously choose a row i and a column j of the state matrix causing the attacker to win the amount $a_{i,j}^k$ from the defender who apparently looses same amount and with a probability that depends on i, j and the state, the game either stops or moves to another state or itself. The probability that the game ends at state k is denoted as s^k and the probability that the next state is l is denoted by $P_i^{(l)}(l)$ [25]. Therefore, it holds that, $s^k + \sum_i^N P_i^{(l)}(l) = 1$, $P^{(l)}$ is defined as the total probability that the game goes to state l from any state i.e. $P^{(l)} = \sum_i^N P_i^{(l)}$.

To generate the state matrices, we look at defining the payoffs from the perspective of the defender since our interest lies in analyzing the defender's game. We value each asset as the amount of time (perceived or measured) it takes to it back to a working state after an attack. This value could also be referred to as the mean time to repair of the asset. It is believed that when an attacker successfully compromise an asset she's gains an amount of time equal to the mean time to repair such asset and can take that time-advantage to propagate another attack.

We use the following methodology to determine elements of the base matrix. Let A be the asset that *attacker's* action a_i affects, so C can be defined as the MTTR of asset A. Also, let B be the asset that *defender's* action d_j affects, then K can be defined as the MTTR of asset B. Therefore, suffix to say

$$U = \begin{cases} C + K & i \ne j \\ C & otherwise \end{cases} \qquad (3)$$

The resulting bi-matrix therefore contains the game matrix for both the *attacker* and *defender*. For this model the intent is to analyse defender's moves against the attacker's, so the defender's component of the bi-matrix is extracted. The base (starting game) matrix is captured as a bi-matrix as $G = (a_{i,j}, -a_{i,j})$ where for $0 < i < m, 0 < j < n$, $m = |p_1^a|$, and $n = |p_2^a|$

e. Computing Game Values and Optimal Strategies

According to [8] associated with each state s_k is a matrix game $G^{(k)}$ and each game $G^{(k)}$ has a value $V(k)$ [25]. For all games matrices, the game values are the unique solutions of [14] with game values given as (4)

$$V(k) = Val(\ a_{i,j}^k + \sum_i^N P_i^{(l)} V(l)\ ) \qquad (4)$$

Stochastic games are characterized by games that may themselves have other games as components where the outcome of a particular choice of pure strategies of the players may be that the players have to play another game depending on some probability. We use this knowledge as a way of modeling transitions between states. To get the solution of such games, our algorithms has to recursively iterate over each game to obtain its value. [25] notes that if the matrix of a

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

game G has other games as component, the solution of G is the solution of the game whose matrix is obtained by replacing each game in the matrix of G by its value.

Every finite 2-person zero-sum game has a value, called the value of the game. The value of the game can be defined in terms of the *min-max* theorem: *"There is a mixed strategy for player I such that I's average gain is at least V no matter what II does and there is a mixed strategy for Player II such that II's average loss is at most V no matter what I does. Also, If* $V = 0$ *, the game is fair. If* $V > 0$ *the game is said to favour Player1, otherwise if* $V < 0$ *the game favours PlayerII"* [25].

The first step to solving each state game is to determine if there exists a saddle point, if it does the value of the game is the saddle point. If not, we convert the matrix game into a linear programming problem that could be solved using any linear programming (LP) solution method. Next, each game matrix in the defender's game is converted to a *min* linear programming (LP) problem that is then solved using a variant of the Simplex Algorithm called the Pivot Method. The linear programs are constructed in a way that minimizes the payoff of the defender the average loss of the defender as well as minimizes the average gain of the attacker. According to [25], the following LP ensures that his average gain is v;

Choose v *and* $p_1, \ldots, p_m$ *to maximize* v
Subject to the constraints

$$v \leq \sum_{i=1}^{m} p_i a_{i1} \ldots\ldots\ldots\ v \leq \sum_{i=1}^{m} p_i a_{in} \qquad (5)$$
$$p_1 + \cdots + p_m = 1\ , p_i \geq 0 \quad \text{for } i = 1, \ldots, m$$

Similarly, the dual of the above program gives the LP problem for the defender, ensuring that his average loss is v;
Choose w *and* $p_1, \ldots, p_m$ *to minimize* v
Subject to the constraints

$$w \geq \sum_{j=1}^{n} p_j a_{1j} \ldots\ldots\ldots w \geq \sum_{j=1}^{n} p_j a_{mj} \qquad (6)$$
$$p_1 + \cdots + p_n = 1,\ p_j \geq 0 \quad \text{for } j = 1, \ldots, n$$

The expected output are two vectors representing the optimal mixed strategies for both the attacker and the defender at each state of the game, and a vector of real game values containing the values of games played in all states.
The optimal mixed strategies produced by this algorithm can be represented as;

$$X^* = \{p = (p_1, \ldots, p_m) : 0 \leq p_i,\ p_i \leq 1\ \forall\ i = 1, \ldots, m \text{ and } \sum_{i=1}^{m} p_i = 1\} \qquad (7)$$

$$Y^* = \{q = (q_1, \ldots, q_n) : 0 \leq q_i,\ q_i \leq 1\ \forall\ i = 1, \ldots, n \text{ and } \sum_{i=1}^{n} q_i = 1\} \qquad (8)$$

Also, the expected vector of game values is represented as follows: $V = (v(0), v(1), \ldots\ldots, v(N))$ where N is the number of states.

VI RESULT AND DISCUSSION

At every state, there exists an optimal pair of vectors X^*, Y^* generated by the algorithm and there exist an element in both X^* and Y^* with the highest probability value. These high probabilities indicate that corresponding actions in the action sets for both players are optimal. The reason for that is in the rationality of the players, since defenders make their moves in response to that of the attackers, and so they tend to make moves that minimize their average loss regardless of the actions taken by the attackers. However, the attacker too may change the dynamics of the game by conspicuously ignoring the assets that defenders may possibly fortify (assets directly affected by the action having the maximum optimal strategy) and instead attack those assets with next highest optimal strategy. Nevertheless, the defender at the same time may, while defending the most vulnerable asset, also fortify asset with next highest optimal strategy.

The vector of game values V, helps analysts to determine the nature of the game at each state. It helps to identify if the game favours the defender or the attacker. For the defender's game vector elements indicate the average loss of the defender for the corresponding state while for an attacker's game it depicts average attacker's gain. When these dynamics is observed and analysed over all game states, the defender can easily determine the most vulnerable network assets, the possible attacker's behaviour and the corresponding counter-measures.

VII CONCLUSION

Game-theoretic modeling of computer networks allows researchers to be able to model and analyse the both defender's and attacker's behaviour with the respect to underlining system environment. This work gives a brief introduction on the concept of Game-theory with emphasis on its strength as a quantitative method for analysing network security. A practical game model was developed to study the interaction between network administrators and attackers over a network. The method demonstrated how the real-time behaviour of the system in response to player actions can be assessed. It has also been shown how the complexity of network components, the dynamic nature of underlying network environment, and probabilistic nature of player strategies can be captured in one model to predict the behaviours of players. By computing and analysing the optimal mixed strategies of the games, it has been shown the possibility of predicting adversary's attacks, determine the set of assets that are most likely to be attacked, and possibly suggest defense strategies for the defender.

In future works, we intend to carry out a full scale simulation using our model to achieve the concrete results. Also, in order to properly model threats/vulnerabilities attack graphs would be employed with stochastic petri nets to analyse how vulnerabilities are exploited by attackers and serve as a basis for risk computations while security games

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

would be used for formal analysis and prediction of adversaries' behaviour. This serves as a basis for recommending appropriate optimal counter-measures for defenders to enhance network infrastructures management.

REFERENCES

[1] Manshaei, M. H., Zhu, Q., Alpcan,T., Basar,T. and Hubaux, J.P.(2010) "Game Theory Meets Network Security and Privacy," EPFL, Lausanne, Tech. Rep.,2010.[Online].http://infoscience.epfl.ch/record/151965/Files/GamesecSurvey-SubmittedVersion.pdf

[2] Stallings, W; Cryptography and Network Security: Principles and Practice, Prentice Hall, Third edition, 2003.

[3] Cheswick E.R. and .Bellovin, S.M Firewalls and Internet Security, Addison-Wesley, 1994

[4] Marios M., Vicky P., Paul S. (2006). "Algorithmic Game Theory and Applications". Wiley- Inter Science, John Wiley and Sons publication.

[5] Karin Sallhammar, Knapskog S. J. and Helvik B. E. (2005) *"Using Stochastic Game Theory to Compute the Expected Behavior of Attackers"*, In Proceedings of the 2005 International Symposium on Applications and the Internet (Saint 2005). Trento, Italy.

[6] Schneier B. (1999), "Attack trees: Modeling security threats," Dr. Dobb's Journal, December.

[7] Alpcan T. and Baser T.(2010), "Network Security: A Decision and Game-Theoretic Approach", 1st ed. Cambridge University Press.

[8] Shapley L. S. (1953) *"Stochastic Games"*. Proceedings of the National Academy of Science USA, vol 39, pp. 1095-1100.

[9] Arome G. (2010) *"Modelling of Internet Protocol Security Policies in a Networking Environment"*. M.Tech. Thesis, Department of Computer Science, Federal University of Technology, Akure. Nigeria.

[10] Adetunmbi A.O., Alese B.K., Ogundele O.S. and Falaki S.O. (2007) "A Data Mining Approach to Network Intrusion Detection", Journal of Computer Science & its Applications, Vol. 14 No. 2.pp 24-37.

[11] Khanna R. and Liu H.(2007), "Distributed and Control Theoretic Approach to Intrusion Detection" Proceedings of the 2007 International Conference on Wireless Communications and Mobile Computing, ser. IWCMC '07. New York, NY, USA: ACM.

[12] Adetunmbi A.O. Falaki S.O., Adewale, O.S. and Alese, B.K. (2008) "Intrusion Detection based on rough Set and k- Nearest Neighbour", International Journal of Computing and ICT Research, vol. 2 No. 1. pp. 60-66. http: www.ijcir.org/volume-number2/artcle7.pdf

[13] Cavusoglu H., Raghunathan S., and Yue W.(2008), "Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment" Journal of Management Information Systems, vol. 25, pp. 281 September.

[14] Assane Gueye "A Game Theoretical Approach to Communication Security" (2011), Electrical Engineering and Computer Sciences University of California at Berkeley. Technical Report No. UCB/EECS-2011-19 http://www.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-19.html

[15] Lye Kong-wei, Jeanette Wing (2002) "Game Strategies In Network Security", Extended Abstract for FCS

[16] Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V. and Wu Q (2010). *"A Survey of Game Theory as Applied to Network Security"*. Proc. of the 43rd HICSS, Hawaii.

[17] Karin Sallhammar, Knapskog S. J. (2004) *"Using Game Theory in Stochastic Models for Quantifying Security"* In Proceedings of the 9th Nordic Workshop on Secure IT-systems (Nordsec 2004). Espoo, Finland.

[18] Milind T. and Manish J. "Introduction and Overview of Security Games" Cambridge University Press 978-1-107-09642-4 - Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned Milind Tambe Excerpt.

[19] Bell, M.G.H, Kanturska, U, Schmöcker, J.D and Fonzone A (2008)"vulnerability Attacker-defender models and road network" Phil. Trans. R. Soc. A 2008 366, 1893-1906, doi: 10.1098/rsta.2008.0019 Downloaded from rsta.royalsocietypublishing.org on June 12, 2012.

[20] Allen B. MacKenzie and Luiz A. DaSilva (2006) "Game Theory for Wireless Engineers" Synthesis Lectures on Communications, Vol. 1, No. 1 , Pages 1-86. Virginia Polytechnic Institute and State University, Morgan & Claypool.

[21] Burke, D. A. (1999) "Towards a Game Theoretic Model of Information Warfare," Air force Institute of Technology, Tech. Rep., 1999.

[22] Fudenberg Drew, Tirole Jean (1991), "Game Theory", MIT Press, ISBN 978-0-262-06141-4

[23] Shor Mikhael (2005), "Dictionary of Game Theory Terms", Available: <http://www.gametheory.net/dictionary/ url_of_entry.html> Web accessed: 8/11/2011

[24] Leyton-Brown Kevin, Shoham Yoav (2008), "Essentials of Game Theory: A Concise, Multidisciplinary Introduction", San Rafael, CA: Morgan & Claypool Publishers, ISBN 978-1-598-29593-1, http://www.gtessentials.org

[25] Ferguson S. T. (2007) *"Game Theory II – Two-Person Zero-Sum Games"*, http://www.scholar.google.com. Retrieved 20/04/2011.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)