A Survey of Game Theory as Applied to Network Security *

Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, Qishi Wu
Department of Computer Science
University of Memphis
Memphis, TN, USA
{sroy5, ceellis, sshiva, ddasgupt, vmshndly, qishiwu}@memphis.edu

Abstract

Network security is a complex and challenging problem. The area of network defense mechanism design is receiving immense attention from the research community for more than two decades. However, the network security problem is far from completely solved. Researchers have been exploring the applicability of game theoretic approaches to address the network security issues and some of these approaches look promising. This paper surveys the existing game theoretic solutions which are designed to enhance network security and presents a taxonomy for classifying the proposed solutions. This taxonomy should provide the reader with a better understanding of game theoretic solutions to a variety of cyber security problems.

1 Introduction

Recent incidents in cyberspace [38, 13, 35] prove that network attacks can cause huge amounts of loss to governments, private enterprises, and the general public in terms of money, data confidentiality, and reputation. The research community has been paying attention to the network security problem for more than two decades. However, the problem is far from being completely solved. We frequently see a race between the security specialists and the attackers in the following sense: one day an intelligent solution is proposed to fix a network vulnerability, and the next day the attackers come up with a smarter way to circumvent the proposed countermeasure. The most important factor which makes this problem difficult is that the local network, which needs to be secured, is typically connected to the Internet and major parts of the Internet are beyond the control of network administrators. However, the Internet has become an integral component of running the daily business of government, financial institutions, and the general public. As a result, there is a pressing need to design countermeasures for network attacks.

Traditionally, network security solutions employ either protective devices such as firewalls or reactive devices such as Intrusion Detection Systems (IDSs) and both of them are used in conjunction. The intrusion detection algorithms are either based on identifying an attack signature or detecting the anomalous behavior of the system. Once an attack is detected the employed IDS notifies the network administrator who then takes an action to stop or mitigate the attack. However, currently IDSs are not very sophisticated and they rely on ad-hoc schemes and experimental work. The current IDS technology may prove sufficient for defending against casual attackers using well known techniques, but there is still a need to design tools to defend against sophisticated and well organized adversaries.

The weakness of the traditional network security solutions is that they lack a quantitative decision framework. To this end, a few groups of researchers have started advocating the utilization of game theoretic approaches. As game theory deals with problems where multiple players with contradictory objectives compete with each other, it can provide us with a mathematical framework for analysis and modeling network security problems. As an example, a network administrator and an attacker can be viewed as two competing players participating in a game. In addition, game theory has the capability of examining hundreds of thousands of possible scenarios before taking the best action; hence, it can sophisticate the decision process of the network administrator to a large extent. As a result, several game theoretic approaches have recently been proposed to address network security issues.

This paper surveys the existing game theoretic solutions which are designed to enhance network security and presents a taxonomy for classifying them. Highlighting the basic game type used in the defense mechanisms, while abstracting detailed differences, this taxonomy provides the reader with a global view of the problem and solution space. This paper does not advocate any specific defense game,

*This work is supported by the Office of Naval Research (ONR) under grant N00014-09-1-0752.

IEEE computer society
978-0-7695-3869-3/10 $26.00

rather the main purpose is to provide the reader with the current solution possibilities.

The rest of this paper is organized as follows. Section 2 provides an overview of game theory. Section 3 explains how network security problems can be modeled as a game. Section 4 classifies the current state of research and proposes a taxonomy. Finally, Section 5 and 6 highlight the differences between this report and other surveys in the field, and provide a summary.

2 An overview of game theory

This section identifies the premise of game theory to aid the understanding of the games referred later (in Section 4). For a detailed introduction to game theory refer *A Course in Game Theory* [32]. Game theory describes multi-person decision scenarios as games where each player chooses actions which result in the best possible rewards for self, while anticipating the rational actions from other players.

A player is the basic entity of a game who makes decisions and then performs actions. A game is a precise description of the strategic interaction that includes the constraints of, and payoffs for, actions that the players can take, but says nothing about what actions they actually take. A *solution concept* is a systematic description of how the game will be played by employing the best possible strategies and what the outcomes might be.

The *consequence function* associates a *consequence* with each action the decision makers take. A *preference relation* is a complete relation on the set of consequences which model the preference of each player in the game. A *strategy* for a player is a complete plan of actions in all possible situations throughout the game. If the strategy specifies to take a unique action in a situation then it is called a *pure strategy*. If the plan specifies a probability distribution for all possible actions in a situation then the strategy is referred to as a *mixed strategy*.

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

2.1 Definitions

Game
A description of the strategic interaction between opposing, or co-operating, interests where the constraints and payoff for actions are taken into consideration.

Player
A basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.

Action
An action constitutes a move in the given game.

Payoff
The positive or negative reward to a player for a given action within the game.

Strategy
Plan of action within the game that a given player can take during game play.

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

Complete Information Game
This is a game in which every player knows both the strategies and payoffs of all players in the game, but not necessarily the actions. This term is often confused with that of perfect information games but is distinct in the fact that it does not take into account the actions each player have already taken. Incomplete information games are those in which at least one player is unaware of the possible strategies and payoffs for at least one of the other players.

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

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

Dynamic/Extensive Game
A game with more than one stages in each of which the

players can consider their action [32]. It can be considered as a sequential structure of the decision making problems encountered by the players in a static game. The sequences of the game can be either finite, or infinite. In the rest of this paper, this class of game is referred to as 'dynamic game'.

Stochastic Game

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

3 Information Warfare as a Game

Global networks continue to undergo dramatic changes resulting in ever-increasing network size, interconnectivity, and accessibility, and a consequent increase in its vulnerability. Several recent Federal policy documents have emphasized the importance of cyber security to the welfare of modern society [8, 12]. The President's National Strategy to Secure Cyber Space [8] describes the priorities for response, reduction of threats and vulnerabilities, awareness and training, and national security and international cooperation. *Cyber Security: A Crisis of Prioritization* [12] describes the need for certain technologies for cyber security. Security should be an integral part of advanced hardware and software from the beginning, as described by Sun Microsystems, Cisco Systems, and Microsoft at the 2006 RSA Conference.

Next-generation information infrastructure must robustly provide end-to-end connectivity among computers, mobile devices, wireless sensors, instruments, etc. Cyber-security is an essential component of information and telecommunications, which impacts all of the other critical US infrastructures [14]. However, traditional cyber-security methods involve a never-ending cycle of detection and response to new vulnerabilities and threats. It is recognized that this patches-on-patches approach is a short fix and attests to the failure of the present cyber-security paradigm, and points to the need for a new and bold approach. The US-CERT [38] web site has currently more than 20,000 vulnerabilities (increasing by 50 to 60 per month), implying a world-wide cost more than 1 trillion dollar. The open web application security project also lists top ten vulnerabilities of the year for web-based applications. "Build Security In" (BSI) [33] is a project of the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the US Department of Homeland Security is for use by software developers, who want information and practical guidance on producing secure and reliable software. NSA has an effort on high-assurance computing platforms. The Trusted Computing Group [15] has an ongoing effort. Microsoft has an effort on next-generation secure computing [26].

In future warfare, cyberspace will play a major role where no one is guaranteed to have information dominance in terms of intelligence and accessibility. As a result, a game-theoretic approach of collaboration (carrot) and compelling (counter-) moves (stick) need to be played efficiently. This notion is not unlike the mutually assured destruction (MAD) of nuclear warfare. The question then becomes: How do we construct such a game theoretic approach in cyberspace?

In general, a game-theoretic approach works with at least two players. A player's success in making choices depends on the choices of others. In game theory, players are pitted against each other taking turns sequentially to maximize their gain in an attempt to achieve their ultimate goal [1]. In the field of cyber security, game theory has been used to capture the nature of cyber conflict. The attacker's decision strategies are closely related to those by the defender and vice versa. Cyber-security then is modeled by at least two intelligent agents interacting in an attempt to maximize their intended objectives.

Different techniques available in game theory can be utilized to perform tactical analysis of the options of cyber threat produced either by a single attacker or by an organized group. A key concept of game theory is the ability to examine the huge number of possible threat scenarios in the cyber system [16, 17]. Game theory can also provide methods for suggesting several probable actions along with the predicted outcome to control future threats. Computers can analyze all of the combinations and permutations to find exceptions in general rules, in contrast to humans who are very prone to overlooking possibilities. This approach allows identification of the what-if scenarios, which the human analyst may not have considered.

4 Taxonomy: Classification of current research

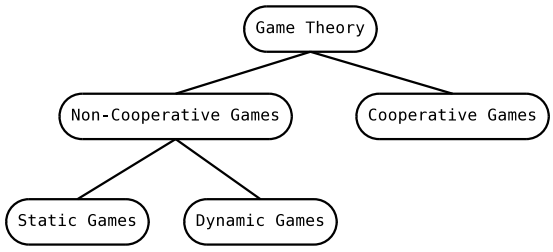

Figure 1. Classification of games

Figure 1 illustrates the basic classification of game the-

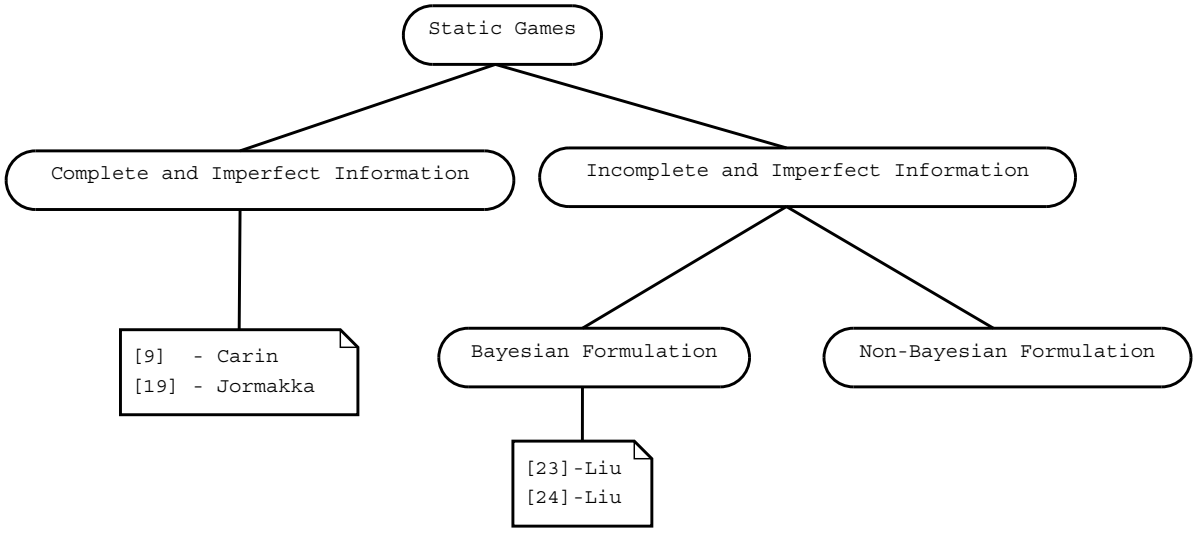

Figure 2. Classification of Static Games: Each rectangular leaf node lists the research works which fall under the corresponding category. Each research work is represented by the reference number and the first author name.

ory. The existing game-theoretic research as applied to network security falls under non-cooperative games. As such, this paper does not further expand upon 'cooperative games'. Figure 2 illustrates the classification of static games and lists the existing research works (related to network security) falling under each class. Figure 3 does the same for dynamic games.

Section 4.1 discusses existing works involving static games while Section 4.2 deals with existing works involving dynamic games. Section 4.3 discusses a few other works which do not directly fall under these classes. Finally, Section 4.4 presents some directions for future research.

4.1 Static games

Since a static game is a one-shot game, by definition all static games are of imperfect information. According to the completeness of information, static games can be classified into two sub-classes as listed below. We briefly discuss the existing research works which fall under each sub-class of static games.

4.1.1 Complete imperfect information

Jormokka et al. [19] introduced a few examples of static games with complete information where each example represents an information warfare scenario. For each scenario the authors found the best strategy of the players in a quantitative form. In particular, they investigated if more than one Nash equilibria exist and if so, then which one is most likely to appear as the outcome given the players' strategies. These examples show that depending on the scenario the players could get the benefit of a bold strategy or a mixed strategy.

Carin et al. [9] presented a computational approach to quantitative risk assessment for investment efficient strategies in cyber security. The focus of this work was how to protect the critical intellectual property in private and public sectors assuming the possibility of reverse engineering attacks. The authors proposed an *attack/protect economic model* cast in a game theoretic context.

4.1.2 Incomplete imperfect information

Liu et al. [23] presented a methodology to model the interactions between a DDoS attacker and the network administrator. This approach observed that the ability to model and infer attacker intent, objectives, and strategies (AIOS) is important as it can lead to effective risk assessment and harm prediction. An *incentive-based* game-theoretic model to infer AIOS was discussed in this work. A few bandwidth parameters were used as the metric to measure the impact of the attack and the countermeasure, which in turn measures the attacker's, and defender's, incentive. The work also observed that the best game model to choose depends on the degree of accuracy of the employed IDS and the degree of correlation among the attack steps. The work reported simulation results involving game plays following the Bayesian model while the simulation experiment was performed on ns-2. The topology considered in the simulation experiment consists of 64 source hosts connected to one victim machine via 4 levels of routers. Each router is capable of employing

the *pushback* mechanism as part of the defense strategy. A set of Nash equilibrium strategies were computed via the simulation.

Liu et al. [24] focused on the intrusion detection problem in mobile ad-hoc networks. Their two-player game model is based on a Bayesian formulation and they analyzed the existence of Nash equilibria in static scenario. The defender updates his prior beliefs about the opponent based on new observations. This work investigated the Bayesian Nash Equilibria (BNE) in the static model. The authors also presented some results from the experiments performed on the ns-2 simulator.

4.2 Dynamic games

A dynamic game can be either of complete or incomplete information. Moreover, a dynamic game may involve perfect or imperfect information. So, there are four sub-classes of dynamic games as listed below. For each sub-class of dynamic games, we briefly discuss the existing research works which fall under the corresponding sub-class.

4.2.1 Complete perfect information

Lye et al. [25] proposed a game model for the security of a computer network. In this work, an enterprise network was envisioned as a graph of 4 nodes (web server, file server, work station and external world) along with the traffic state for all the links. It is a two-player (administrator, attacker), stochastic, general-sum game and the authors focused on 3 attack scenarios namely, defaced website, denial-of-service, and stealing confidential data. The game was described from the point of view of both players. A formal model defined the game as a 7-tuple— the set of network states, the action set for each player, the state transition function, the reward function and a discount factor. In particular, this work considered a stochastic game involving 18 network states and 3 actions for each player at each state. The state transition probabilities and the reward matrices are assigned using the domain knowledge. With different initial conditions a set of Nash Equilibria were calculated using a nonlinear program in Matlab.

Xiaolin et al. [39] proposed a Markov game theory based model for risk assessment of network information system considering the security status of both present and future. They identified that threats acting on vulnerability can induce risk and the risk will be larger and larger by threat spreading. On the other hand, the risk will be smaller and smaller by the system administrator's repairing the vulnerability. Thus, they established a game of threats and vulnerabilities. Essentially, the experiment involves a game of complete and perfect information with two players. Authors formulated a function to capture the damage and used it to assess the risk. Using the damage function the system administrator would select the repair strategy which minimizes the maximum damage. To evaluate their model they constructed a risk assessment platform with four subsystems which are Malicious code Detection Subsystem, Vulnerability Detection Subsystem, Asset Detection Subsystem and Risk Assessment Subsystem. They used Trojan.Mybot-6307 as a threat, and three assets to define states. Their results are similar or better than the traditional assessment model like Fault Tree Analysis (FTA) because they effectively incorporated the potential risk also. They came up with a repair table of vulnerability states and threat states. They claimed that the model also leads to the best system repair scheme.

In Nguyen et al.'s [31] model, an attacker and the network administrator participate in a two-player zero-sum stochastic game. This work assumed that the network consists of a set of interdependent nodes whose security assets and vulnerabilities are correlated. It utilized the concept of linear influence networks [28] and modeled the interdependency among nodes by two weighted directed graphs, one signifying the relationship of security assets and the other denoting vulnerability correlation among the nodes. This research presented one numerical example considering a small network of three nodes to explain how to compute the optimal strategies of the players.

4.2.2 Complete imperfect information

Alpcan et al. [3] modeled the interaction between malicious attackers to a system and the IDS using a stochastic (Markov) game. They captured the operation of the IDS sensor system using a finite-state Markov chain, and considered three different information structures: (a) the players have full information about the sensor system characteristics and the opponents, (b) the attacker has no information about the sensor system characteristics, and (c) each player has only information about his own costs, past actions, and past states. A few illustrative examples and numerical analysis were presented for these three cases. Tools such as value iterations to solve Markov decision processes (MDP) [5], minimax-Q [22], and naive Q-learning [5] were used to find the best strategies of the players.

Nguyen et al. [30] viewed the network security problem as a sequence of nonzero-sum games played by an attacker and a defender. This game model, called 'fictitious play (FP)', conservatively considers that the players cannot make perfect observations of each other's previous actions. This work studied the impact of the error probabilities associated with the sensor system on the Nash equilibrium strategies of the players considering two scenarios— (a) each player is aware of these error probabilities, and (b) neither player knows these error probabilities. Both classical and stochas-

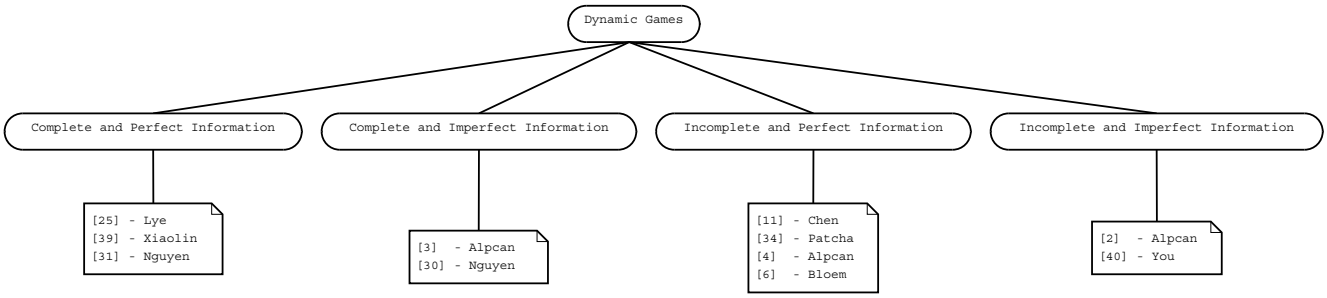

Figure 3. Classification of Dynamic Games: Each rectangular leaf node lists the research works which fall under the corresponding category. Each research work is represented by the reference number and the first author name.

tic FP games are investigated via simulation.

4.2.3 Incomplete perfect information

Chen [11] in his doctoral dissertation used game theoretic model to design the response for the importance-scanning Internet worm attack. The main idea is that defenders can choose how to deploy an application, that is the group distribution, when it is introduced to Internet to minimize the worm propagation speed. The attacker can choose the optimal group scanning distribution to maximize the infection speed. Thus a game would be played between the attacker and the defender. The attacker should choose so as to maximize the minimum speed of worm propagation, while defender wants to minimize the maximum speed of worm propagation. By framing the problem this way it turns out to be a zero sum game and a min-max problem. The optimal solution for this problem is that defender should deploy the application uniformly in the entire IP-address space or in each enterprise network, so that the best strategy that the attacker exploits is equivalent to random scanning strategy. This work gave a game theoretical framework to design the locations of vulnerable and high value hosts over a network.

Patcha et al. [34] proposed a game theoretic approach to model intrusion detection in mobile ad-hoc networks. The authors viewed intrusion detection as a game played between the attacker node and the IDS hosted on the target node. The objective of the attacker is to send a malicious message with the intention of attacking the target node. The modeled game is a basic signaling game which falls under the domain of multi-stage dynamic non-cooperative game.

Alpcan et al. [4] investigated the problem of Nash Equilibrium Design for quite a general class of games from an optimization and control theoretic perspective. The work is theoretical and the analysis is general though aimed at information networks. They restricted their treatment to a class of games where players do not manipulate the game by deceiving the system designer and where utility functions accurately reflect user preferences. They further discussed the games with incomplete information with two objective functions: Quality of service (QoS)-based and utility maximization. They concluded that though the tragedy of commons or price of anarchy is unavoidable in pure games, it is circumvented altogether when additional mechanism such as "pricing" are included. They explored the pricing dynamics in different conditions. They inferred that "loss of efficiency" is not an inherent feature of a broad class of games with built-in pricing systems, but merely a misconception that often stems from arbitrary choice of game parameters. Finally, they give a brief overview of Nash Equilibrium dynamic control. They focused on how long does the game approach Nash equilibrium when many players are trying to solve it in a distributed way. They suggested a feedback control system approach with pricing as a control input to make the system robust and to control the system's progress and investigated system's controllability in general.

Bloem et al. [6] modeled intrusion response as a resource allocation problem based on game theory. A cost is associated with attacks and responses. This problem, including imperfections in the sensor outputs, was first modeled as a continuous game. The strategies are discretized both in time and intensity of actions, which eventually leads to a discretized model. The reaction functions uniquely minimize the strictly convex cost functions. After discretization, this becomes a constrained integer optimization problem. To solve this they introduced their dynamic algorithm, Automatic or Administrator Response algorithm (AOAR). They classified attacks into those resembling previous attacks and those that do not, and many such intuitive classes with Kohonen self-organizing maps, a neural net, and the response cost is minimized. The simulations captured variation in vulnerability, value and cost of actions. Their results showed system performs improves after using AOAR.

Though majority of Liu et al.'s [23] approaches fall under static games with incomplete and imperfect information

(Section 4.1.2), one of their approaches falls under this category.

4.2.4 Incomplete imperfect information

Alpcan et al. [2] modeled the interaction of an attacker and the network administrator as a repeated game with 'finite steps' or 'infinite steps'. This work assumed that the sensor system which is deployed to detect the attacks is imperfect and considered the sensor system as a third 'fictitious' player similar to the 'nature' player in standard game theory. It found the Nash equilibrium in a repeated game via simulation considering a simple scenario with three specific attacks. The Nash equilibrium strategies were computed assuming simple cost functions for the players.

You et al. [40] described how to model the network security scenario considering the interaction between the hacker and the defender as a two player, zero sum game. It gave a taxonomy of relevant game theory and network security terms and suggested a correlation between them. They pointed out at the utility of Nash and Bayesian Equilibria in representing the concepts to predict behavior and analyzed the interaction between the attacker and the defender. They gave a list of game theory terms that are relevant in the network security scenario and explained them. They explained how min max theorem for this game is formulated. They concluded by suggesting that to solve this problem linear algorithms would be appropriate.

The research reported in [3], [30] and [34] which are described under other classes of games also contain additional approaches that fall under this class of game.

4.3 Other work

Bursztein et al. [7] presented a model for evaluating the plausibility of successful attacks on a given network with interdependent files and services. This work provided a logic model that accounts for the time needed to attack, crash, or patch network systems. Rather than providing a game theoretic model, the work used the given time and topology constraints to determine if an attack, or defense, would be successful. The example presented described a high-availability web server configuration with interdependent elements and considered the strategic actions of the attacker as well as the defender.

Sun et al. [37] analyzed information security problem in the mobile electronic commerce chain. They claimed that the application of game theory in information safety is based on the hypothesis of player's perfect rationality, while in reality, the main body of information security only has the bounded rationality, which is just the assumption of Evolutionary Game theory. They introduced the penalty parameter in the problem if an organization in the mobile electronic commerce chain does not invest in information security. They calculated replicator dynamics of this game. They analyzed Evolutionary Stable strategy to get the results which formulate that the pay off to the organizations for investing is higher than not investing. This is an application of evolutionary game theory to the investment strategy in the network security to obtain the best security pay off.

Sun et al. [36] used game theory to make the analysis and put forward strategy suggestions for defender organization to invest in information security. It is concerned about management and not the technology of the information security. They formulated the problem of two organizations investing in the security, with parameters such as for investment, security risk and disasters. They presented a pay off matrix. They did the Nash Equilibrium analysis for both pure and mixed strategy and showed them to be consistent. To make the investing a rational option they introduced a penalty parameter associated with not investing. They concluded by presenting an argument for encouraging organizations the investment in information security.

4.4 Discussion: scope of future research

Many of the current game-theoretic security approaches are based on either static game models [23, 24] or games with perfect information [25, 39, 4, 6] or games with complete information [31]. However, in reality a network administrator often faces a dynamic game with incomplete and imperfect information against the attacker. Some of the current models involving dynamic game with incomplete and imperfect information are specific to wireless networks [34] while a few others [2, 40] do not consider a realistic attack scenario.

In particular, some of the limitations of the present research are: (a) Current stochastic game models [25] only consider perfect information and assume that the defender is always able to detect attacks; (b) Current stochastic game models [25] assume that the state transition probabilities are fixed before the game starts and these probabilities can be computed from the domain knowledge and past statistics; (c) Current game models assume that the players' actions are synchronous, which is not always realistic; (d) Most models are not scalable with the size and complexity of the system under consideration.

5 Related work

This section briefly discusses the existing body of other research related to the survey topic of this paper, and mentions how the existing work differs from this paper. It also discusses a few research works which focus on the taxonomy of network attacks and cyber incidents. It is to be noted

that good understanding of the attack taxonomy is a prerequisite to design a countermeasure.

Hamilton et al. [17] outlined the areas of game theory which are relevant to information warfare. The paper analyzed a few scenarios suggesting several potential courses of actions (COA) with predicted outcomes and what-if scenarios. Alpha-beta, alpha-beta star, and beta pruning with min-max search are suggested approaches. Hill climbing algorithm was suggested for predicting the opponent moves. In the domain of checkers, a linear programming technique using pattern recognition was cited as finding the optimal weights in a follow up pass after hill climbing. Automatic tuning of evaluation functions by the chess program, DeepBlue is highlighted. They concluded with speculating about great possibilities in applying game theory to information warfare. Hamilton et al.'s work focusses on a motivating example to illustrate the use of game theory in network security problems while our paper provides a taxonomy of the existing game-theoretic solutions.

Hamilton et al. [16] identified the following seven challenges in applying game theory to the domain of information warfare: (i) There is a limited database of relevant games played by real players, (ii) Both the attacker and the defender can launch multiple moves simultaneously, (iii) Players can take as long as they want to make moves, (iv) The defender may not be able to correctly able to identify the end goal of the opponent, (v) At each step the flow of the game may change so that the known legal moves, both in number and kind, may change for each player, (vi) The defender may find it hard to keep track of any possible change in the opponents resources and also his end goals, (vii) It is hard to define precisely the timing for move and state updates. The authors expected that these challenges could be addressed with some non-trivial breakthroughs in the research. Our paper investigates how the existing game-theoretic solutions meet some of the above challenges.

Kjaerland [21] introduced existing body of research work related to computer crime profiling and proposed a taxonomy of cyber-intrusions, which provides insight into cyber-criminals and victims. In this research, Kjaerland focused on reported cyber intrusions reported from CERT. These attacks were analyzed using facet theory and multidimensional scaling (MDS) with Method of Operation, Target, Source, and Impact. Each facet contains a number of elements, each is mutually exclusive and elements exhaustively describe the facet. Kjaerland concluded the paper with comparing the incidents of commercial versus government incidents.

Hansman and Hunt [18] proposed a taxonomy consisting of four unique dimensions that provide a holistic classification that covers network and computer attacks, providing assistance in improving computer and network security as well as consistency in language with attack description. The first dimension is attack vector, which is used to categorize the attack into an attack class. The second dimension allows for the classification of attack targets, which can be classified to specific targets (e.g., OS:Linux:RedHat6.0). The third dimension consists of the vulnerability classification and the attack uses (e.g., CVE/CERT). The fourth and final dimension highlight the potential payload or effects involved (e.g., File Deletion). Within each dimension various levels of information are provided to successfully classify and supply attack details. Hansman and Hunt provided examples to conclude the proposed taxonomy is general to categorize attacks and mentioned the need of future work to improve classifying blended attacks. There are several research works,e.g. [20], [29], which study network attacks.

Chakrabarti et al. [10] focused on the Internet and its infrastructure as being the basis for highlighting attacks and security. Where majority of research focused on securing the data being transferred, this research discussed attacks on the infrastructure which can lead to considerable destruction due to different Internet infrastructure components having various trust relationships with one another. Chakrabarti et al. categorized possible Internet infrastructure attacks, identified attacks within each category, solutions within each category, and presented guidelines for less researched areas. In their taxonomy of attacks they provided four categories on Internet infrastructure attacks (DNS hacking, Route table poisoning, Packet mistreatment, and Denial of Service). They used the categories to develop a comprehensive understanding of the security threats.

Mirkovic and Reihner [27] presented a taxonomy of Distributed Denial of Services (DDoS) attack and defense mechanisms in aim to classify attacks and defense strategies. This work highlighted attack commonalities and important features of attack strategies. These strategies are vital in dictating the design of countermeasures. With focus on DDoS attacks, Mirkovic and Reihner created a taxonomy to examine the exploitation, the characteristics, and the victim impact of the attack. The taxonomy of DDoS attacks was categorized by Degree of Automation, Exploited Weakness, Source Address Validity, Attack Rate Dynamics, Possibility of Characterization, Persistent Agent Set, Victim Type, and Impact on Victim. Highlighting challenges defending against DDoS attacks, Mirkovic and Reihner developed a taxonomy of DDoS defenses consisting of Activity Level, Cooperation Degree, and Deployment Location. Mirkovic and Reihner concluded with the proposed taxonomies to provide communication of threats and related countermeasures aiming to foster cooperation between researchers for discussing solutions.

6 Summary

Hackers activities have significantly increased in cyber space, and have been causing damage by exploiting weaknesses in information infrastructure. Considerable efforts are continuously being made by the research community for the last two decades to secure networks and associated devices. Recently, researchers have been exploring the applicability of game theoretic approaches to address cyber security problems and have proposed a handful of competing solutions. Game theory offers promising perspectives, insights, and models to address the ever changing security threats in cyber space. This survey highlights important game theoretic approaches and their applications to network security and outlines possible directions for future research. It is to be noted that classes in the taxonomy could be divided into more detailed levels. It is obvious that new classes may need to be introduced in the taxonomy after new defense mechanisms are proposed in the future.

References

[1] A. Alazzawe, A. Nawaz, and M. M. Bayaraktar. Game theory and intrusion detection systems. *http://theory.stanford.edu/îliano/courses/06S-GMU-ISA767/project/papers/alazzawe-mehmet-nawaz.pdf*, 2006.

[2] T. Alpcan and T. Baser. A game theoretic analysis of intrusion detection in access control systems. *Proc. of the 43rd IEEE Conference on Decision and Control*, 2004.

[3] T. Alpcan and T. Baser. An intrusion detection game with limited observations. *Proc. of the 12th Int. Symp. on Dynamic Games and Applications*, 2006.

[4] T. Alpcan and L. Pavel. Nash equilibrium design and optimization. *International Conference on Game Theory for Networks, GameNets*, 2009.

[5] D. Bertsekas. Dynamic programming and optimal control. *2nd ed. Belmont, MA: Athena Scientific, vol. 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] E. Bursztein and J. Goubalt-Larrecq. A logical framework for evaluating network resilience against faults and attacks. *Lecture Notes in Computer Science; Vol. 4846*, 2007.

[8] G. W. Bush. National strategy to secure cyberspace, office of the president. 2003.

[9] L. Carin, G. Cybenko, and J. Hughes. Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology. *IEEE Computer*, 2008.

[10] A. Chakrabarti and G. Manimaran. Internet infrastructure security: A taxonomy. *IEEE Network*, 16:13, November 2002.

[11] Z. Chen. Modeling and defending against internet worm attacks. *PhD Dissertation at Georgia Institute Of Technology*, 2007.

[12] President's Information Technology Advisory Committee, Cyber Security: A crisis of prioritization, 2005.

[13] Security focus, http://www.securityfocus.com/archive, security focus bugtraq vulnerability notification database, 2009.

[14] The National Strategy for Homeland Security, http://www.dhs.gov/interweb/assetlibrary/nat-strat-hls.pdf, 2002.

[15] The Trusted Computing Group, http:// www.trustedcomputinggroup.org.

[16] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari. Challenges in applying game theory to the domain of information warfare. *Proceedings of the 4th Information survivability workshop (ISW-2001/2002)*, 2002.

[17] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari. The role of game theory in information warfare. *Proceedings of the 4 th information survivability workshop (ISW-2001/2002)*, 2002.

[18] S. Hansman and R. Hunt. A taxonomy of network and computer attacks. *Computers and Security*, 24:31–43, February 2005.

[19] J. Jormakka and J. V. E. Molsa. Modelling information warfare as a game. *Journal of Information Warfare; Vol. 4(2)*, 2005.

[20] D. Kienzle and M. Elder. Recent worms: A survey and trends. *Proceedings of the 2003 ACM workshop on rapid malcode*, 2003.

[21] M. Kjaerland. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, 25:522–538, October 2005.

[22] M. L. Littman. Markov games as a framework for multi-agent reinforcement learning. *Proc. of the 11th International Conference on Machine Learning*, pages 157–163, 1994.

[23] P. Liu, W. Zang, and M. Yu. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security (TISSEC)*, 2005.

[24] Y. Liu, C. Comaniciu, and H. Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. *ACM International Conference Proceeding Series; Vol. 199*, 2006.

[25] K. Lye and J. Wing. Game strategies in network security. *Proceedings of the Foundations of Computer Security*, 2002.

[26] Microsoft. Next-generation secure computing base. www.microsoft.com/resources/ngscb/default.mspx.

[27] J. Mirkovic and P. Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *Computer Communication Review 34, no. 2*, 2004.

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

[29] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. Inside the slammer worm. *IEEE Security and Privacy no.4*, 2003.

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

[31] K. C. Nguyen, T. Alpcan, and T. Basar. Stochastic games for security in networks with interdependent nodes. *Proc. of Intl. Conf. on Game Theory for Networks (GameNets)*, 2009.

[32] M. J. Obsborne and A. Rubinstein. A course in game theory. *MIT Press*, 1994.

[33] U.S. Department of Homeland Security, https://buildsecurityin.us-cert.gov/daisy/bsi/home.html.

[34] A. Patcha and J. Park. A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. *Proceedings of the 2004 IEEE workshop on Information Assurance and Security*, 2004.

[35] Packet storm vulnerability database, http:// packetstormsecurity.org/, 2009.

[36] W. Sun, X. Kong, D. He, and X. You. Information security investment game with penalty parameter. *The 3rd International Conference on Innovative Computing Information and Control*, 2008.

[37] W. Sun, X. Kong, D. He, and X. You. Information security problem research based on game theory. *International Symposium on Publication Electronic Commerce and Security*, 2008.

[38] US-CERT. http://www.us-cert.gov. *United States Computer Emergency Readiness Team*, 2009.

[39] 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.

[40] X. You and Z. Shiyong. A kind of network security behavior model based on game theory. *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2003.