International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

A Review on the Application of Game Theory to Computer Security.

[1]Amadi E.C., [2]Ajanwachuku N. C., [3]Nwachukwu V., [4]Anyalewechi I.

[1-4]Department of Information Management Technology, Federal University of Technology, Owerri, Imo State, Nigeria.

ec.amadi@gmail.com

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 computer security problems and suggest mainstream approach.

Introduction

Recent incidents in cyberspace according to Roy, Sankardas, Ellis, Charles, Shiva, Sajjan, Dasgupta, Dipankar Shandilya, Vivek (2010) 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 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, educational institution, e-commerce and the general public. As a result, there is a pressing need to design countermeasures for network attacks. Why? Botnets have recently been identified as being among the most insidious threats to the security of the Internet.

A botnet is a network of compromised machines (bots) under the control of an attacker (the botnet herder). In a ten days infiltration into the Torpig botnet, the study by Gueye, (2011), revealed that more than 180,000 infected machines around the globe were zombies. Botnet herders typically get the bots to act on their behalf to send spams, spread viruses, or carry out phishing attacks. Botnets have also served to launch distributed denial of service attacks (DDoS). In recent years, DDoS attacks have been

launched against business and government websites in incidents that are attributed to organized and terrorist groups, and sometimes to nation-state intelligence agents. The Russia-Estonia conflict, the Google-China saga, the recent Wiki leak Operation "Payback" incident, and the many attacks on the White House and other US government agencies' websites are just a few examples(Gueye, 2011). In the Stuxnet case, many bloggers and security specialists have speculated that the virus was designed in Israel to target nuclear power plants in Iran. This list of security incidents is certainly not exhaustive; Gueye, (2011) gives a broad overview of cyber security incidents in the last three decades.

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(Roy et al., 2010). 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(Roy et al., 2010).

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(Roy et al., 2010).

An overview of game theory

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 (Roy et al., 2010).

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.(Roy et al., 2010)

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.

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. 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'(Camerer, Ho, & Chong, n.d.).

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 (Gueye, 2011).

Information Warfare as a Game

Global networks continue to undergo dramatic changes resulting in ever-increasing network size, interconnectivity, and accessibility, and a consequent increase in its vulnerability. Several recent Federal policy documents have emphasized the importance of cyber security to the welfare of modern society. The President's National Strategy to Secure Cyber Space describes the priorities for response, reduction of threats and vulnerabilities, awareness and training, and national security and international cooperation. Cyber Security: A Crisis of Prioritization describes the need for certain technologies for cyber security (Roy et al, 2010).

Security should be an integral part of advanced hardware and software from the beginning, as described by Sun Microsystems, Cisco Systems, and Microsoft at the 2006 RSA Conference. Next generation information infrastructure must robustly provide end-to-end connectivity among computers, mobile devices, wireless sensors, instruments, etc. Cyber-security is an essential component of information and telecommunications, which impacts all of the other critical producing secure and reliable software. NSA has an effort on high-assurance computing platforms. The Trusted Computing Group has an ongoing effort.

Microsoft has an effort on next-generation secure computing. In future warfare, cyberspace will play a major role where no one is guaranteed to have information dominance in terms of intelligence and accessibility. As a result, a game-theoretic approach of collaboration (carrot) and compelling (counter) moves (stick) need to be played efficiently. This notion is not unlike the mutually assured destruction (MAD) of nuclear warfare. The question then becomes: How do we construct such a game theoretic approach in cyberspace? In general, a game-theoretic approach works with at least two players. A player's success in making choices depends on the choices of others.

In game theory, players are pitted against each other taking turns sequentially to maximize their gain in an attempt to achieve their ultimate goal. In the field of cyber security, game theory has been used to capture the nature of cyber conflict. The attacker's decision strategies are closely related to those by the defender and vice versa. Cyber-security then is 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 (Roy et al., 2010).

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.

The use of game theory in modeling good and evil has also appeared in several other areas of research. For example, in military and information warfare, the enemy is modeled as an evil player and has actions and strategies to disrupt the defense networks. Browne describes how static games can be used to analyze attacks involving complicated and heterogeneous military networks (Browne, 2000).

THEORITICAL MODELS

Hamilton, S. N. Miller, W. L. Ott, A. and Saydjari, O. S.(2002). 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, "Deep-Blue" is highlighted. They concluded with speculating about great possibilities in applying game theory to information warfare. Hamilton et al.'s work focuses on a motivating example to illustrate the use of game theory in network security problems.

Chakrabarti and Manimaran (2002) 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 (2002) 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 Reiher (2004) presented a taxonomy of Distributed Denial of Services (DDoS) attack and defense mechanisms in aim to classify attacks and defense strategies. Their work highlighted attack commonalities and important features of attack strategies. 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.

In the study of network reliability, Bell considers a zero-sum game in which the router has to find a least-cost path and a network tester seeks to maximize this cost by failing a link (Bell, 2001). In the game

two players are in some form of control over the network and they have opposite objectives. Finding the least-cost path in their problem is analogous to finding a best defense strategy in ours. Hespanha and Bohacek discusses routing games in which an adversary tries to intersect data packets in a computer network (Hespanha and Bohacek, 2001). The designer of the network has to find routing policies that avoid links that are under the attacker's surveillance. Finding their optimal routing policy is similar to finding the least-cost path (Bell, 2001) and the best defense strategy in our problem in that at every state, each player has to make a decision on what action to take. Their game model is, again, a zero-sum game.

McInerney, J. Stubberud, S. Anwar, S. and Hamilton, S.(2001) use a simple one-player game in their FRIARS cyber-defense decision system capable of reacting autonomously to automated system attacks. Their objective is to use good to fighting evil in cyberspace. Instead of finding complete strategies, their single-player game model is used to predict the opponent's next move one at a time. Their model is closer to being just a Markov decision problem because it is a single-player game.

Syverson (1997), talks about good" nodes fighting evil" nodes in a network and suggested using stochastic games for reasoning and analysis.

Marti, Giuli, Lai and Baker, (2000) proposed an IDS scheme for MANET which consists of two different modules, *viz.* the Watchdog and the Path rater. In this scheme, the Watch dog acts as an IDS for the MANET and detects malicious node behaviors in the network by promiscuously listening to its next hop's transmission. If the Watchdog notices that its immediate next node fails to forward the packet within a given period of time then it increments the node's failure counter. If the failure counter of the monitored node exceeds a threshold value then the Watch dog reports the node as misbehaving. The Path rater is then employed to inform the routing protocol to avoid the reported nodes for further data transmission. The drawback of this scheme is that it requires continuous monitoring by the Watchdog for detecting intrusions.

Liu, Comaniciu, and Man, (2006) proposed a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation in wireless Ad-hoc Networks. They suggested a Bayesian hybrid detection approach for the defender, in which a less powerful lightweight module is used to estimate the opponent's type, and a more powerful heavyweight module acts as a last line of defense. They analyzed the obtainable Nash Equilibrium (NE) for the attacker/defender Bayesian game in both static and dynamic settings and concluded that the dynamic approach is a more realistic model, since it allows the defender to consistently update its belief about the maliciousness of the opponent player as the game evolves. The drawback of their work is that it is difficult to determine a reasonable prior probability about the maliciousness of the attacker player.

Chen, Wu and Wu, (2010) proposed a framework that applies two game theoretic schemes for economic deployment of intrusion detection agent. In the first scheme, the interaction between an attacker and the intrusion detection agent is modeled and analyzed within a non-cooperative game theory setting. The mixed strategy Nash Equilibrium solution is then used to derive the security risk value. The second scheme uses the security risk value derived by the first scheme to compute the Shapley value of the intrusion detection agent while

considering the various threat levels. This allows the network administrator to quantitatively evaluate the security risk of each IDS agent and easily select the most critical and effective IDS agent deployment to meet the various threat levels to the network. The drawback of this scheme is the computational overhead involved for calculating the Shapley values of the intrusion detection agents. A game theoretical framework to model the interaction between the service provider and the attacker as an intrusion detection game was proposed by Kodialam and Lakshman (2003). In this scheme, the game is represented as a two person zero-sum game, wherein the service provider tries to maximize its payoff by increasing its probability of successful detection while the attacker tries to minimize its probability of being detected by the IDS. The optimal solution for both players is to play the min-max strategy of the game. The drawback of this model is the assumption that both players (attacker and defender) have complete information about the topology of the network and all links in the network, which allows the players to choose the optimal path for playing the min-max strategy. However, this assumption is usually invalid in real networks where the players have an incomplete information about the network parameters.

Agah, Das, Basu, and Asadi, (2004) and Alpcan, Basar, (2003) addressed the attack defense problem in a sensor network as a two-player non cooperative, non-zero-sum game. In their model, the game is assumed to have a complete information and the payoff function of the opponent player decides each player's optimal strategy. The drawback of their work is the assumption that the players have complete information about the game.

Findings

Attacks on Infrastructure can be stochastic, where different layers of infrastructure can be compromised because of the various trust relationship existing between them as established by Chakrabarti et al,(2002) taxonomy of attacks. Their categorization can help reduce attacker payoffs and mitigate game transition to a new state.

Browne describes how static games can be used to analyze attacks involving complicated and heterogeneous military networks (Browne, 2000). We are suggesting that dynamic game can also be used in military and information warfare to analyze the several wrong decisions made by the evil player in his attempt to break the defense of the computer network. This will enable the military develop a sophisticated strategy which will be used to frustrate the effort of the evil player.

Syverson. (1997) talks about good" nodes fighting evil" nodes in a network and suggested using stochastic games for reasoning and analysis. We are suggesting that dynamic game can also be used to analyze the several wrong decisions made by the evil player in his attempt to hack into the computer network. This will enable network administrators develop a sophisticated strategy which will be used to frustrate the effort of the evil player (hackers).

Reference

Agah, A. Das, S. Basu, K. Asadi, M. (2004). Intrusion detection in sensor networks: a non-cooperative game approach, in: Proceedings of Third IEEE International Symposium on Network Computing and Applications, pp. 343–346.

Alpcan, T. Basar, T.(2003). A game theoretic approach to decision and

analysis in network intrusion detection, in: Proceedings of 42nd IEEE Conference on Decision and Control, pp. 2595–2600.

Bell, M.G.H (2001) . The measurement of reliability in stochastic transport networks. Proceedings, IEEE Intelligent Transportation Systems, pages 1183-1188.

Brown, R. (2000). C41 defensive infrastructure for survivability against multi-mode attacks. In proceedings, 21st Century Military Communications. Architectures and Technologies for Information Superiority, volume 1, pages 417-424.

Chakrabarti, A. and Manimaram, G. (2002) Internet internet infrastructure security: A taxonomy.

Camerer, C. F., Ho, T., & Chong, J. K. (n.d.). Behavioural Game Theory: Thinking, Learning and Teaching ∗.

Chen, Y.M. Wu, D. Wu, C.K.(2010) . A game theoretic framework for multi-agent deployment in intrusion detection systems, in: Security Informatics, vol. 9, Annals of Information Systems, Springer, 2010, pp. 117–133.

Gueye, A. (2011). A Game Theoretical Approach to Communication Security.

Liu, Y. Comaniciu, C. and Man, H.(2006) A Bayesian game approach for intrusion detection in wireless ad hoc networks. ACM International Conference Proceeding Series; Vol. 199.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A Survey of Game Theory as Applied to Network Security ∗, 1–10.

IEEE Network, 16:13