ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

SURVEY ON AUTOMATED INTRUSION RESPONSE SYSTEM USING GAME THEORY

Anuvarsha.G[1], RajeshKumar.J[2]

PG scholar, Department of Information Technology, SNS College of Technology, Coimbatore, India[1]

Assistant Professor, Department of Information Technology, SNS College of Technology, Coimbatore, India[2]

Abstract: With the increasing number of network technology, intruders are also rationally increased. To provide the security to the network from the intruders is one of the vital one, this survey presents Intrusion Response System to handle the intruders by request and response process by using Game theory. This survey provides a better understanding of the different research approaches by applying game theory for the Automated Intrusion Response System (AIRS). It focuses on fictitious play, fuzzy game, and zero-sum game for automatic response system to the intruders. This survey helps to the researchers in various fields to develop game-theoretic solutions in current and emerging security problems in network security.

Keywords: Network Security**,** Decision Making, Automatic Intrusion Response System and Game Theory.

1. INTRODUCTION

The number of intrusions on computer networks is hastily increasing in today's network communication. Intruder handling techniques are labeled into three classes such as intrusion prevention, intrusion detection and intrusion response system. Most researchers focused only on intrusion prevention and detection techniques but failed to concentrate on the intrusion response process. Incase, the process includes in response system means, then it may be a manual process which is performed by network administrators and are no longer adequate [1, 2]. This survey provides a better understanding of Automated Intrusion Response System (AIRS) using Game theory. It provides games to find the intruder and their activity. It consist fictitious play, fuzzy game, and zero-sum game for finding the intruder and provides automatic response to the intruder. It provides game to two persons Actual person and the intruder. Actual person play the game by using their hint and the intruder play the game without any hint, so we easily analyze the intruder and can raise the automatic response technique.

Game theory has become one of the systematic tools that improve researchers design security protocols in network security [3]. It can be used as a rich mathematical tool to evaluate and model a new security problem. Moreover, through the stability analysis of the security game, the protector can gain a deeper understanding of the attacker's strategy, as well as the potential attack risks [4, 5]. In this survey, we presented an impression of security and privacy problems that are analyzed within a game-theoretic framework. We have reviewed and evaluate security games in computer network in terms of game models and game-theoretic approaches. The general objective is to identify and address the attacker's activity where game theory helps to schedule the intruder's game and also finding the attacker by playing their game. Also applied to model and evaluate security problems and consequently used to design efficient protocols.

2. INTRUSION RESPONSE TYPES

There are three types of intrusion response, they are

- Notification
- Manual response
- Automatic response

2.1 Notification

The notification system is one of the popular mechanisms in intrusion detection and response systems. This system provides reports and alarms. Periodic reports were the earliest form of intrusion response. Reporting is not a feasible means of intrusion response by itself. Alarms produce instant messages to alert the network administrator to potential intrusive actions. Alarms present in a various formats including email messages, calm alerts, and/or pager activity [6].

2.2 Manual Response

Through manual response, regularly the systems guide the user through correct response which is allowed by the network administrator. It allows a system administrator to react more hastily to intrusions. This system is more helpful than notification one; by this manual system there is a time gap between detected intrusion and the response arise from the system administrator. Hence time gap is the main problem in manual system.

2.3 Automatic Intrusion Response

An Automatic Intrusion Response (AIR) system is one which allows the system administrator to intimate the response automatically; it does not wait for the system administrator it place automatic respond to intrusive behavior. It provides two approaches for intrusion response: Decision tables and Rule-based systems. Decision table is used to the particular response is associated with a particular attack. Rule-based is used to determine the appropriate response to intrusive behavior [7].

3. RESPONSE SYSTEMS TECHNIQUES

Intrusion responses have numerous techniques in Automatic Intrusion Response (AIR). The automated

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

response focuses on many techniques, such as attack method, target attack (either in host or network), etc [8]. The techniques and their intrusion response mechanisms is listed

3.1 ARMD

ARMD is an Adaptable Real-Time Misuse Detection. It is a network-based intrusion detection system. ARMD utilize a high-level language to map the system events into a conceptual misuse signature [8]. It monitors the detection strategies of intruder's activity and it provides the pattern in sequence events of their activity. It uses an optimization technique to speed up the processing of audit events of the attackers. ARMD shows the auditing estimation of performance misuse detection. It is a manual response through global directives.

3.2 Intruder Alert and NetProwler

Intruder Alert (IA) and NetProwler are common Intrusion Detection Systems (IDS). Intruder alert was an alert status in services which were sounded when an intruder was detected. It is a host-based misuse detection system. It uses a centralized specialist system to find attack signatures in audit logs. It provides reports, alarms, and automated responses. Alarms may be an email, a pager message, etc. IA activated automatically based on predefined standards, such as entering a restricted area, malicious activity, etc.. Hence intruder alert mechanism announces it to the administrator. NetProwler provide response to major security developments. It provides dynamic intrusion detection by evidently explorative network traffic to identify, identity log, and conclude unauthorized use or misuse of network systems.

3.3 NetSTAT

NetSTAT is a Network Statistical Analysis Tool; it shows the details about the misuse behavior of the intruders. It provide attack signature at state transition level. It captures the network traffic and it checks the activity of the attackers. If an attack is detected then the decision engine is responsible for the intrusion response. The response is in the form of reports, alarms, and implication for network administrator or an automatic response may arise.

3.4 NSM

Network Security Monitor (NSM) is used to monitor the anomaly intruder which is in the intrusion detection process. It captures the misuse behavior which is carried in host and network for anomaly intrusion detection. It reports the disturbing or distrustful behavior to the system administrator instantly through an administrator interface. It includes network monitoring model of network intrusion detection to enlarge performance and introduced a hierarchical model for tracking the attacker's activity. This system is carrier by automatic response system of network monitoring mechanisms.

3.5 SAINT

SAINT is a Security Administrator's Integrated Network Tool. It is computer software used for scanning computer networks for security vulnerabilities, and uses establish vulnerabilities. It Detect and fix possible fault in network's security before they can be exploited by intruders. It is an information examination tool that present cross examination of reports generated by several security tools. It provides the response by generating report.

3.6 GAME THEORY

Game theory is the mathematical study of decision-making which is associated to conflict and cooperation. Game theoretic model concern whenever the actions of several players are interdependent. These players may be individuals, groups or any combination of these. This concept of game theory provides a language to invent structure, examine, and understand strategic scenarios of the player (attackers) in network. It is automatic response to the intruder by providing the game to each and every player (attacker) and catches their activity and notices their every action. For Automatic intrusion response technique Game theory is most effective one. In this survey we focus on Game Theory for the intrusion response mechanism [9].

4. GAME THEORY- AN OVERVIEW

Game theory: It is an attempt to mathematically confine behavior in strategic state, in which an individual's success in providing choices based on the choices of others.

The aim of the game theory is to assist the consideration of the games. Game theory depicts multi-person decision situation where each player chooses their own actions, which results in the best attainable rewards for self, while expecting the rational actions from other players. A player is the main objective of a game that he/she makes decisions and then performs their own actions [10, 11]. A game is a specific explanation of the strategic interface that includes the restriction of every player, and payoffs for, actions that the players can take their action, but they says nothing about what actions they he/she actually takes.

A *solution concept* is a systematic explanation of how the game will be played by utilizing the best potential strategies and what the outputs might be.

The *consequence function* describes a *consequence* of each action the player and the decision maker's takes.

A *preference relation* is an entire relation on the set of consequences model, which give the preference to the each player in the game.

A *strategy* for a player is an absolute plan of events in all potential situations throughout the game.

A *pure strategy* is if the strategy identifies to obtain a unique action in a situation then it is called a *pure strategy*.

A *mixed strategy* is if the plan identifies a possibility allotment for all possible actions in a state then the strategy is called a *mixed strategy*.

Strategy:

Plan of the action taken by the player during the game play by them.

Perfect Information Game:

In game theory a perfect information game is an extensive-form game, a game in which each player is attentive of their action and all other players that have previously take's place of their actions. Examples of perfect information games are: tictac-toe, chess and go. A game where at least one player is not attentive of the actions of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

at least one other player which have taken place is called an imperfect information game.

Complete Information Game:

Complete and perfect information games are significantly different. In this game, each player knows both the strategies and payoffs of all players in the game, but not necessarily the actions. This often puzzled with that of perfect information games but it is separate in the fact that it does not take into account of the actions of each player which have already taken. Where incomplete information games are those in which at least one player is unaware of the probable strategies and payoffs for at least one of the other players [12].

Bayesian Game:

In game theory Bayesian Game is a game in which information about the strategies and payoff for other players is incomplete and a player allocate a 'type' to other players at the beginning of the game. In this game the players have initial beliefs about the type of each player. Such games are called Bayesian games due to the use of Bayesian analysis in predicting the output.

Stochastic Game:

Stochastic game is one of the games in game theory; this game progresses as a sequence of stages. This game may entail *probabilistic transitions* during several states of the systems. The game begins with a start state; the players chooses their actions and receives a payoff that relate on the current state of the game, and then the game moves into a new state with a probability based on players' actions and the current state of the player [13].

5. INTRUSION RESPONSE SYSTEM (IRS) USING GAME THEORY

In this survey we focus on security problems at intrusion response system by using Game Theory. Here we use Decision-Making approach for automatic intrusion response System to reduce the cruelty of attack damage resulting from delayed response in Manual Response [14, 15]. In this survey, we evaluate various game-theoretical formulations of network security issues. We address Security Game for Intrusion Response; here we present *fictitious Play, fuzzy game and zero-sum game*. These games can effectively defending approach for homogeneous attackers represented by a single player or multi player.

(a) IRS using fictitious play

This game model, called fictitious play (FP), used to learn opponent's motivations. In a FP process, each player observes all the actions and makes estimates of the mixed strategy of the opponent. At each stage owner update their estimate and plays the pure strategy that is the best response to the current estimate of the other's mixed strategy. It Formulate the repeated security games where players make random decision errors as a fictitious play process [16]. The convergence of plays with random number of action is taken by the intruder then game establishes the convergence property for several classes of games with decision errors where both players are restricted to two actions (either to play/quit). We examine the fictitious play process where the players' observations are imperfect and the players try to compensate for the inspection errors. We point out a no of scenarios that can be considered as special cases of result of the intruder [17]. This fictitious play studied the impact of the error probabilities associated with the intruder's action while playing the game— (a) each player is aware of these error probabilities, and (b) neither player knows these error probabilities. Fictitious play consists the fake play the intruder may hack the fake data. While playing the game the can get the fake data in each and every play they get a chance to get the data, if data loosed in any time means they cannot get the same data by perfectly catch the step of their action play in their game, hence it is a repeated game via simulation considering of a simple scenario. Hence, Fictitious play leads to more randomized mixed strategies for Intrusion Response System (IRS).

(b) IRS using Fuzzy game

Another approach is by using Fuzzy Game for Intrusion Response System, the system could determine the most probable attack made by the intruder, on the basis of the generated alerts by automatic response to the intruders, using conditional probabilities or fuzzy model, and hence a single response is generated as the most appropriate one. The owner assumes that the (attackers) players know only their own payoff of accessing the data [18]. Furthermore, to be more efficient in responding to the noticing intrusion, it should be essential to trace down the attack source to avoid the denial of service to authorized users. As the players of the game often have limited information about the preferences of the opponent, they also evaluate a fuzzy game in which players attempt to maximize their utility using an imprecise payoff matrix of the intruder. Fuzzy logic is blending with decision making to better enhance the detection capability and reduces false alarms. And also used to calculating the on-going attack with linguistic values and calculate the relevant attributes of attack and automatically generate the response to intruder by playing this game in network. While playing a game by intruder a variation of fuzzy multi-attribute decision theory is applied to select the desired response to the multi attackers. The complexity of this response system depends on the detected attacks because the generated play depends on multi attacker. Furthermore, it depends on the fuzzy multi criteria decision method applied to choose the best response to the intruder. In this method, best responses are selected and ranked according to their degree of preference over other responses by playing the game by the intruders. By playing the game by the multi intruder, we can easily schedule the response to each and every intruder by which the action is taken by them. By using fuzzy Game it gives moderate defense strategy for Intrusion Response System (IRS).

(c) IRS using Zero Sum Game

Zero-sum games are generally used to form conflicting goals of a detector and an attacker and suspicions in the decision making. It is commonly modeled between malicious attackers and transmitter-receiver pairs in Network. By using this Zero-Sum, it has been stretched to treat a wide class of communications, which are classified

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

according to numerous strategies, one of these being cooperative versus non-cooperative communications [19]. Typical classical games are used to model and predict the outcome of a wide variety of scenarios involving a finite number of attacker (player) that seek to optimize some individual objective. Non-cooperative game studies the strategic interaction among self-interested attackers (players). Zero-sum game is shared information game on multi attackers (players), the effectiveness of the communication is measured by the mutual information of I(x, y), where x is the input of the intruder from the output of the encoder; y is the output of the intruder that follows a response model of

$$y = Zx + n + u; \quad (1)$$

Where Z is the Intruder gain matrix of appropriate dimensions, u is the disrupted input and n is the additive noise [20]. By allowing the game to intruder we can capture the variance goals of intruders then the utility is often expressed in terms of consumed data or achievable throughput on a link or end-to-end basis. In this Zero-Sum game, the intruders maximize the mutual information while playing the game in network and minimize data disrupted problem. So we can easily response to the intruder by this game. Hence Zero-sum game is an optimal defense strategy for Intrusion Response System (IRS).

RESPONSE SYSTEM	SECURITY MATRIX
IRS using fictitious play	Losses of data due to action play
IRS using Fuzzy game	Moderate defense strategy for response system
IRS using Zero Sum Game	Optimize defense strategy for response system

Table 1: Comparison for security in various Games

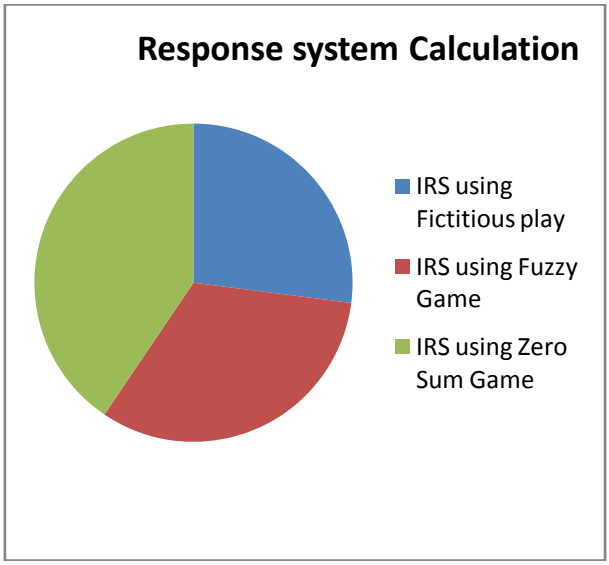

Chart 1: Response System Calculation

6. CONCLUSION

In this survey, we have presented an overview of automated Intrusion Response System using game theory for security and privacy issues in network. We have compared an existing security games in computer networks in terms of players, game forms, game-theoretic method, and equilibrium analysis. It does so by applying game theory and seeking responses that gives on long-term gains. Moreover, they do not have entire information about each others' payrolls and strategies of their play. By using this we get a better response from fuzzy and zero sum game in form conflicting goals of a detector and an attacker and suspicions in the decision making.

REFERENCES

[1] Zonouz, Saman A., et al. "RRE: A game-theoretic intrusion Response and Recovery Engine." *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*. IEEE, 2009.
[2] Kabiri, Peyman, and Ali A. Ghorbani. "Research on Intrusion Detection and Response: A Survey." *IJ Network Security* 1.2 (2005): 84-102.
[3] Anis alazzawe,Asad nawaz and Murad Mehmet Bayraktar, "Game theory and Intrusion Detection system", 2006.
[4] Roy, Sankardas, et al. "A survey of game theory as applied to network security." *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010.
[5] Chen, Fu-Wen, and Jung-Chun Kao. "Game-based broadcast over reliable and unreliable wireless links in wireless multihop networks." *Mobile Computing, IEEE Transactions on* 12.8 (2013): 1613-1624.
[6] Weller-Fahy, D., Brett J. Borghetti, and Angela A. Sodemann. "A Survey of Distance and Similarity Measures used within Network Intrusion Anomaly Detection."
[7] Hwang, Kai, et al. "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes." *Dependable and Secure Computing, IEEE Transactions on* 4.1 (2007): 41-55.
[8] Curtis A., Carver Jr. - "Intrusion response systems a survey".
[9] Jackson, Matthew O. "A Brief Introduction to the Basics of Game Theory." (2011).
[10] Nguyen, Kien C. *Game theoretic analysis and design for network security*. Diss. University of Illinois at Urbana-Champaign, 2011.
[11] Nguyen, Kien C., Tansu Alpcan, and Tamer Basar. "Security games with decision and observation errors." *American Control Conference (ACC), 2010*. IEEE, 2010.
[12] Manshaei, Mohammad Hossein, et al. "Game theory meets network security and privacy." *ACM Computing Surveys (CSUR)* 45.3 (2013): 25.
[13] Gao, Xing, Weijun Zhong, and Shue Mei. "A game-theory approach to configuration of detection software with decision errors." *Reliability Engineering & System Safety* 119 (2013): 35-43.
[14] Alpcan, Tansu, and Tamer Basar. "A game theoretic approach to decision and analysis in network intrusion detection." *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*. Vol. 3. IEEE, 2003.
[15] Alpcan, Tansu, and Tamer Basar. "A game theoretic analysis of intrusion detection in access control systems" *Decision and Control, 2004. CDC. 43rd IEEE Conference on*. Vol. 2. IEEE, 2004.
[16] Nguyen, K., Alpcan, T., and Bas_ar, T. 2008. Fictitious Play with Imperfect Observations for Network Intrusion Detection. the 13th International Symposium Dynamic Games and Applications.
[17] Nguyen, Kien C., Tansu Alpcan, and Tamer Basar. "Fictitious play with time-invariant frequency update for network security." *Control Applications (CCA), 2010 IEEE International Conference on*. IEEE, 2010.
[18] Shamshirband, Shahaboddin, et al. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." *Engineering Applications of Artificial Intelligence* 32 (2014): 228-241.
[19] Washburn, Alan, and Kevin Wood. "Two-person zero-sum games for network interdiction." *Operations Research* 43.2 (1995): 243-251.
[20] Theodore L. Turocy and Bernhard von Stenge, "Game Theory." October 8, 2001.