Open Access Article

GAME THEORY BASED SOLUTION FOR NETWORK SECURITY

Raghad I. Hussein
Faculty of pharmacy university of Kufa, Najaf, Iraq

Nasrullah Pirzada
Department of Telecommunication Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan

Saleem Raza
Quaid-e-Awam University of Engineering, Science and Technology, Larkana, Pakistan

Saif ullah Memon
Department of Information Technology, QUEST, Nawabshah

Sijjad Ali Khuhro
School of Computer Science and Technology, University of Science and Technology of China, Hefei, China

Abstract— Today in this modern age, network security is the hottest and trendy topic of research. Features of network security globally change due to rapid developments in computer networks, mobile applications and wireless computer networks. Open computer system networks do not have any protection and privacy due to fraudulent attacks and the Internet attacks on computer networks or an organization. Network security can be maintained through the firewalls and encryption software's. Many organizations developed intranet to remain connected with network for their business. In this paper, we will try to cover network security issues by applying game theory on network security model. Ongoing occurrences in the Internet, demonstrate that network threats can make huge measures of disaster for governments, private undertakings, and the overall population in wording of cash, information privacy, and authorization. This paper presents the game theories that handle the network security issues by implementing different models and constructs that makes the network more reliable and sufficient. The main focus of the paper is the implementation of game theories to the network security models. The analysis of the game theory in the computer network security helps to find the best and optimal solutions for securing the network. Basic techniques for securing computer networks are anti-virus, data encryption, intrusion detection and firewall techniques but in this paper, gaming theory implemented to network security for securing the network through hackers and protect the system through viruses. Intrusion Detection Systems are used in game theory that will eliminate the danger and threats through the clients' networks.

Received: October 05, 2021 / Revised: October 31, 2021 / Accepted: November 30, 2021 / Published: December 30, 2021

About the authors：Raghad I. Hussein

Corresponding author- *Email:

***Index Terms*— Cyber security, Network security, Intrusion Detection Systems (IDSs), Game theory, Security threats,**

摘要——**在**这个现代时代，网络安全是最热门和最时尚的研究课题。由于计算机网络、移动应用程序和无线计算机网络的快速发展，网络安全特征在全球范围内发生了变化。由于欺诈性攻击和互联网对计算机网络或组织的攻击，开放的计算机系统网络没有任何保护和隐私。网络安全可以通过防火墙和加密软件来维护。许多组织开发了 Intranet **以保持与网**络的业务连接。在本文中，我们将尝试通过将博弈论应用于网络安全模型来解决网络安全问题。互联网上不断发生的事件表明，网络威胁可以在现金、信息隐私和授权等方面对政府、私营企业和全体人民造成巨大的灾难。本文介绍了通过实施不同的模型和结构来处理网络安全问题的博弈论，这些模型和结构使网络更加可靠和充分。本文的主要重点是将博弈论应用于网络安全模型。计算机网络安全中博弈论的分析有助于找到最佳和最优的网络安全解决方案。保护计算机网络的基本技术是反病毒、数据加密、入侵检测和防火墙技术，但在本文中，博弈论应用于网络安全，以通过黑客保护网络并通过病毒保护系统。入侵检测系统用于**博弈**论，通过客户的网络消除危险和威胁。

索引词——**网**络安全、网络安全、入侵检测系统 (IDS)、**博弈**论、安全威胁、

INTRODUCTION

NERWORK security issues are regularly testing in light of the fact that the developing multifaceted nature and unified nature of IT-frameworks leads to restricted capacity for perception and control'. Game theory takes into account displaying circumstances of contention and for foreseeing the conduct of members. Game theory can be utilized as a proficient security system configuration instrument in these networks. Due to development in the Internet technology and computer networks, network security becomes very essential for the network structure and for every organization. From the past few years, the network use in business field is rapidly increasing such as e-commerce, digital marketing. E-commerce application is a business application, many companies and organization use e-commerce for their businesses, they also supply stocks to their customers through the network that is why these applications require job critical networks which provide lodgings of audio, data traffic, video and scalability of the network through the users connected to the sites. Because the business is spread to larger networks that is why there is higher risk of security threats that attack in the network. For detection and prevention of these threats, network security algorithms are playing essential role in this regard. The network is generally made through computer networks with the use of switches, routers, wireless access points, and dial up modems.

Game theory gives mathematical apparatuses and models to examine multi-individual vital basic leadership, where the players go after

constrained and shared assets. Network Security courses of action use ensured gadgets and contraptions like firewall and intrusion recognition framework. Usually, network security game plans use either cautious devices, for instance, firewalls or open devices, for example, Intrusion Detection Systems (IDSs) and those two are used related. An Interruption Recognition Framework (IRF) is an essential protection instrument against an assortment of assaults that can trade off the security of a data framework. It is structured and used to identify the unapproved utilization of frameworks, networks, and related assets. Further, by and large, it is equipped for redirecting or distinguishing network security issues. The interruption identification calculations are either dependent on recognizing an assault mark or distinguishing the bizarre conduct of the framework. When an assault is recognized, the utilized IDS advises the network overseer who at that point makes a move to stop or moderate the assault. Be that as it may, right now IDSs are not exceptionally advanced and they depend on specially appointed plans and test work. The current IDS innovation may demonstrate adequate for shielding against easygoing assailants utilizing surely understood strategies, however there is still a need to configure devices to shield against advanced furthermore, efficient enemies.

Application of game theory in network security includes analysis of network attacks, protections and security, and dependency measurements. Network security analysis includes game modeling and strategic predictions. The strategic predicates outputs predicated defense attacks and defense strategies that becomes input for the security dependency measurements that outputs the values for security dependency measurements. An architecture of game theory applied to network security is defined in the figure1: In which different components of application of game theory in network security are defined and their interactions are also shown.

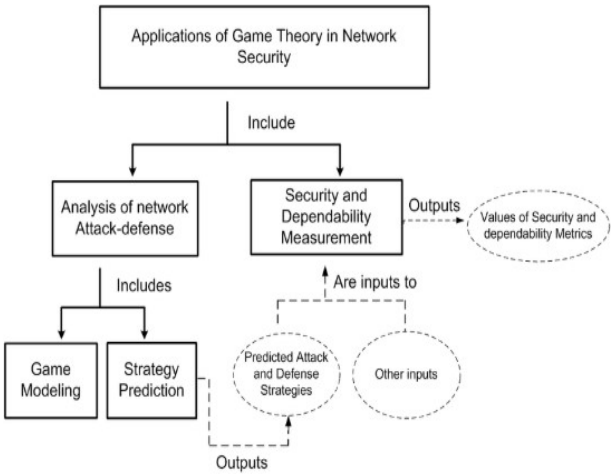

FIGURE 1 GAME-THEORY APPLIED TO NETWORK-SECURITY

The shortcoming of the customary network security arrangements is that they come up short on a quantitative choice structure. To this end, a couple of gatherings of specialists have begun supporting the use of game theoretic methodologies. As game hypothesis manages issues where numerous players with opposing destinations rival one another, it can give us a numerical structure for investigation what's more, demonstrating network security issues. For instance, a network director and an aggressor can be seen as two contending players taking an interest in a game. What's more, game hypothesis has the ability of looking at many a large number of conceivable situations previously making the best move; consequently, it can sophisticate the choice procedure of the network executive to an expansive degree. Accordingly, a few games theoretic methodologies for network security

issues. This paper reviews the current game theoretic arrangements which are intended to upgrade network security and presents a scientific categorization for characterizing them. This paper does not advocate a particular protection game, rather the fundamental design is to furnish the readers and developers with the current arrangement of potential outcomes.

Related Work

Recently the Kevin Mintnick committed major corruption and crime in US history develops interest in the researchers to research more in the network security it opens new ways for searching network security methods for securing the network. Many researchers applied game theory for securing computer networks. This section presents the related work on the game theories and researcher's works. Bursztein et al. [1] presented model for assessing the credibility of effective threats on a given network with related records and administrations. Bursztein et al. [1] showed in his model how the bugs in the computer networks and threats are fixed instead of applying game theoretic models to select whether an attack, or insurance is productive. Sun et al. [2] separated information-security issue in the context of automated exchange-chain. Sun et al. [2] ensured that usage of game theories in the information prosperity relies upon the theory of player's optimal soundness, when the ambiguity created, essential diversity of the information-security simply game theory terms to be only supposition. This is use of transformative game-theories to the hypothesis technique in the network-security to achieve the best advantages and benefits of network security. He applied the game theoretic model inspections and implemented approaches for the proposals for shield relationship to place assets into information-security. Hamilton et al. [3] depicted out the regions of game hypothesis which are fitting to data locks in. His paper isolated a few conditions recommending several potential courses of activities with anticipated results and considers how possible it is that conditions. Alpha-beta, star and beta lopping with min-max look are proposed methodologies. Kjaerland [4] displayed existing combination of research business identified with PC bad behavior profiling and proposed a logical arrangement of advanced interferences, which gives understanding into computerized punks and misused individuals. In this examination, Kjaerland [4] focused on itemized computerized intrusions uncovered from CERT. These dangers were analyzed using highlight theory and multidimensional scaling (MDS) with Method of Operation, Target, Source, and Impact. Each perspective contains different segments, each is in a general sense inconsequential and parts altogether portray the component. Hansman and Hunt [5] proposed a logical arrangement containing four unique estimations that give a thorough request that covers network and PC dangers, giving help with upgrading PC and network security similarly as consistency in lingo with strike depiction. The preeminent estimation is snare vector, which is utilized to amass the assault into a strike class. Hansman and Hunt offered guides for close the proposed coherent order is general to mastermind threats and referenced the need of future work to overhaul organizing mixed perils. Chakrabarti et al. [6] concentrated on the Internet and its foundation just like the clarification behind including threats and security. Chakrabarti et al. portrayed conceivable Internet foundation threats, perceived perils inside each gathering, blueprints inside each class, and demonstrated rules for less

examined zones. In their intelligent course of action of perils they gave four portrayals on Internet framework risks.

Game Theory

Basic techniques for securing computer networks are anti-virus, data encryption, intrusion detection and firewall techniques but the game theory also proved helpful and useful for securing the computer networks. Regular utilization of networked figuring and correspondence frameworks is pervasive in current society. In this manner, security of PCs and networks has transformed into an irrefutably basic concern. Network security issues are routinely trying in light of the fact that the creating interconnected IT structures. Game theory gives logical gadgets, constructs for looking at multi-person essential fundamental authority, where player for obliged and shared-resources. In that capacity, it considers showing conditions of conflict and for foreseeing the lead of individuals. Game speculation delineates multi-singular decision circumstances as games where each player' picks exercises that yields most perfect distinctions for player itself, while picturing adjusted exercises from various players. Basic component of a game is player who settles on decisions and after that performs exercises. Games are a correct delineation of key affiliation that consolidate necessities of changes for exercises that the player can take, nothing characterized with respect to what moves they truly make. The result works associate an outcome with every move boss make. An inclination association is a completed association on the course of action of results which show the tendency of every game player. A technique for players is a finished arrangement to activities in every single conceivable circumstance all through the game. In the event that the methodology determines to take an interesting activity in a circumstance then it is known as an unadulterated system. In the event that the arrangement determines a likelihood conveyance for all conceivable activities in a circumstance then the technique is alluded to as a blended technique. A Nash balance is an answer felt that depicts an undaunted state of games; no players would incline toward to variation his methodology as-that would' chop down settlements given that every single other player is sticking to the recommended system. This approach thought just exhibits persisting state in any case, doesn't indicate how indefatigable states are come to game. Nash synchronization utmost likely comprehended parity, disregarding the route that there are different other game arrangement contemplations utilized once in a while. This data will be utilized to depict games that have applicable highlights for tending to network security issues. Game theory, we can stay away from insufficient terrible balance and plan security instruments that unite to the ideal conceivable arrangement.

Explanation:

Different components are combined together to develop the game theory these components are the Games, players, activities, procedures, results, inconsistent information game, consistent information game, Bayesian Game, Static game, dynamic game and stochastic game.

Game*:* A game is commonly characterized as threesome (P, S, U) segments in which P' characterizes the quantity of player that takes part in a game, U is set of cost capacity and S is an accumulation of techniques.

Player: An essential element of the game that is delegated with making of decisions for various

activities. Players can speak to an individual, machine, or gathering of people that participate in a game.

Activities: The Activities establish moves required in a game.

Procedures: *Activity plans within game defined to the players that given players can proceed aimed game-play.*

Inconsistent Information-Game: The Games in which' every player' knows about the moves' that takes by every other player that has effectively occurred. Instances of immaculate games data are: Chess, tic-tac-toe and go. Games in which players do not know the moves of the other players are known as inconsistent games.

Consistent information game: The Games in which every player knows about the moves that take by every other player that has effectively occurred are known to be consistent games.

Information Warfare as Game

Worldwide networks keep on experiencing emotional changes bringing about regularly expanding network measure, inter connectivity, what's more, availability, and a resulting increment in its defenselessness. A few late Federal strategy reports have stressed the significance of cyber security to the welfare of current society. The President's-National-Strategy to Secure-Cyber-Space portrays needs for reaction, decrease the dangers and susceptibilities, mindfulness what's more, preparing, and national-security and international-participation. Cyber-Security: A Crisis-of-Prioritization depicts requirement aimed at specific advancements for cyber-security. Cyber-Security ought to be a vital piece for the cutting-edge equipment what's more, programming from the earliest starting point, as depicted by Sun-Microsystems, Cisco-Systems, and Microsoft-at-the-2006-RSA Meeting. Cutting edge data foundation should heartily give start to finish network among PCs, cell phones, remote sensors, instruments, and so forth. Cyber security is a fundamental part of data and media communications, which impacts the majority of the other basic US frameworks notwithstanding, conventional cyber-security strategies include an endless cycle's recognition and reaction to new vulnerabilities and dangers. It is perceived that this patches on patches approach is a short-fix and validates disappointment of current cyber security-worldview, what's more, by taking the requirements into account another methodology for Cyber-Security-Division of US-Branch of Homeland-Security used by programming engineers, those needed data and useful direction on delivering safe and trustworthy programming. NSA' has an exertion on the high-confirmation processing stages. The Trusted-Computing-Group has a progressing exertion. Microsoft has an exertion on cutting edge and protected processing. Solution Concepts and Security-Games Circumstances between Attackers and Defender.

	Active	Passive
Active	Nash Equilibrium	Stackelberg Equilibrium
Passive	Stackelberg Equilibrium	Nash Equilibrium

Cyberspace is the warfare of future assume significant trade wherever nobody is ensured having data strength as far as insight and availability. Accordingly, a game-theoretic methodology of joint effort (encouragement) and convincing (counter-) moves (stick) should be played productively. The inquiry at that point turns out to be: How would we develop a model

based on game theory for cyberspace? When all is said in has done, a game-theoretic methodology works within any event two players. A player's accomplishment settling on decisions governed other decisions. In games hypothesis, players are hollowed in contrast to one another alternating consecutively to augment their gain trying to accomplish their definitive objective [7].

Classification of Current Research

Current research presented in this paper is based on network security by applying game theory for securing computer networks. Initial categorization of the game theory presented in the figure below in which game theory comprises of the no cooperative-games and cooperative-games, the non-cooperative game are further divided in to two categories one is static games and other in dynamic games.

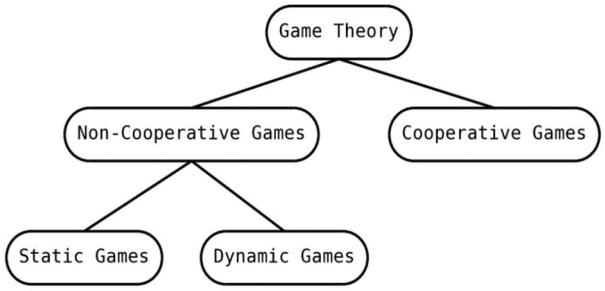

FIGURE 2 GAME THEORY

Static and dynamic Games are briefly described along with complete information and incomplete and inconsistent information.

Static Games

One shot games are the static games and have defective data. As per the culmination of data, static-games arranged in two sub-classes as recorded in ascending order. Now quickly talk about present exploration work on sub-class of static- games

Complete inconsistent data

'Jormokka et, al. [8] presented couple of instances of static-games with comprehensive data where every precedent speaks to a data warfare situation. For every situation the creators establish finest procedure players in quantitative-form. Specifically, he researched if two or three Nash equilibrium-exist and assuming this is the case, at that point one most liable to show up as the result given the players methodologies. Models demonstrate that relying upon situation the player could get the advantage of a strong methodology. Carin et al. exhibited a theoretical way to deal with quantitative hazard evaluation of speculation effective methodologies in cyber-security. Main features of his research the means by which to ensure the basic licensed innovation in private and open divisions accepting the likelihood of figuring out threats. The creators proposed an assault/ensure financial display cast in a game theoretic setting.

Incomplete inconsistent data

Interaction model for the denial of service attacks and network administrator proposed by the Liu et al. [9] in which communication between the attacks and administrators are shown .The ability of this model measured by five elements which are the objects, attackers' intents and the strategies. Fixed number of parameters taken from the bandwidth is used that measures the intensity of the countermeasure and the attack. His works served for the identification of the Intrusion detection systems and the correlation among the attack strategies. His work followed by the Bayesian gaming model.

Dynamic Games

Dynamic games have four subclasses that are shown in the figure below: Existing work on dynamic games are defined below that represents research from different researcher work.

Figure 2: Dynamics games

Complete perfect data

Network security model based on the gaming theory proposed by Lye at, in which he proposed network mode by using four nodes that are the web and file server workstation server and the external world among these nodes relationships created by links. This security model has 2 players, one is the network administrator and other is attacker, this model focused on three attack scenarios that are the denial of service attacks, stealing credential data and defaced web. In this model, Nash equilibrium calculated by MATLAB that is nonlinear program. His research presents the numerical examples in which three nodes are defined how the optimal strategies completed.

Incomplete perfect data

Chen et al, presented game-theoretic models for the reaction of internet-worm attacks, foremost goal his work is that how the protector can be selected for deploying application and the distribution of groups when it is executed on the internet to reduce the speed of the worm. The protector selects optimal strategies for the minimization of the worm attack speed thus here the game is also played between the attacker and protector. Here for minimization or maximization the speed of the worm min-max problem arises. Optimal solution to deal such problem in the network the protector needs to deploy IP address space to each network that is connected to whole enterprise network. His work presented game theoretical model for defining the locations of vulnerable and high-speed values host over the network.

Complete Consistent data

By using stochastic games in the interaction model among the malicious attackers and Intrusion Detection System a model is proposed by the Alpcan et, al [10]. By using the finite states operations of the intrusion detection system are captured by implementing three information constructs. a) These three information structures are the: Attacker have no data about the IDS b) Player has complete information about the system c) Every player of the game has only information about his own costs. On these three cases limited examples are defined by the Alpcan et.

Incomplete Consistent Data

A model is proposed by Alpcan et, [10] in which interaction between the attacker and protector played by the number of states these states can be finite and infinite. In his work sensor systems like Intrusion detection systems are used which detects incomplete and imperfect information attacks by considering the sensor system as a third fictitious player in standard game theories. By considering three attacks Nash Equilibrium is found in repeated games. By computing, the cost function for the player's Algorithm of Nash Equilibrium is computed.

Conclusion

FUTURE WORK

Many game strategies are available for the network security models in which different game theories are applied for securing the network. Dynamic game models have incomplete information and imperfect about the attackers that are faced in reality some of the models that use dynamic games have complete and imperfect information limited to only a wireless network while the other models do not consider the realistic attack scenarios. The limitation of the work proposed in this paper is that statistic games only consider the complete and perfect information that the protector can detect the attacks. And the players of the games attackers and defenders performed synchronous actions. In the future incomplete and imperfect/inconsistent information is considered by the protector for detecting and removing security threats to the network.

ACKNOWLEDGMENT

We are thankful to the anonymous reviewers for their suggestions and encouragement.

REFERENCES

[1] 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.

[2] 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.

[3] 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 (ISW2001/2002), 2002.

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

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

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

[7] A. Alazzawe, A. Nawaz, and M. M. Bayaraktar. Game theory and intrusion detection systems. http://theory.stanford.edu/˜iliano/courses/06 S GMUISA767/project/papers/alazzawe-mehmet-nawaz.pdf, 2006

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

[9] 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.

[10] 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.