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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

Optimal Game Theory for Network Security using IPDRS Engine

Shyam Chandran P, Resmi .A.M[2]

Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu[1]

Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu[2]

Abstract: With the tremendous growth of network technology, network attackers are also rationally increased to disrupt the activities and hacking the data from the network users by the intruder. To provide the security from the intruder is most important one. Many researchers were proposed a different approach for providing security they does not tackle the problem, it leads an untruthful in the network. In existing system they propose a game based intrusion request and response process by game play of header node to access the data by their correct play, from this if the real header play it in wrong method means all the client user under the header also suffer from the access of the data. To tackle this issue we enhanced the game theory based on the individual play in the network to avoid the suffering of misplayed game played by the header using the IPDRS Engine.

Keywords: Network Security**,** Intrusion Response System, Game Theory, Optimal Game and IPDRS Engine.

1. INTRODUCTION

In Today's environment distributed system is network plays a major role for sharing the data among the network. To provide the security to those network users from the intruder is one of the major issues, for this issue they were lot of security providing techniques like intrusion prevention, detection and intrusion response system were implemented in existing level, and those techniques were does not satisfy the network user from the security issues [1]. It gives a major problem among the network users who share the resources in distributed network. For this issue most of the researchers were focused on intrusion prevention and detection technique but does not concentrate on the response technique. Hence Intrusion response is based on three types they were Notification, Manual response and Automatic response [2]. Most of researchers concentrate on manual level and are no longer adequate. In Notification level system provides reports and alarms. Reporting is not a feasible means of intrusion response by itself and Alarms produce instant messages to alert the network administrator. But in Automatic response, it permits the system administrator to intimate the response automatically, it does not remain for the system administrator it place automatic respond to intrusive behavior. And hence response technique provides a better one after intruder had found in the network. For this response system, 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. In addition, through the constancy analysis of the security game, the protector can gain a deeper considerate of the attacker's strategy, as well as the potential attack risks. In previous work they present a game based intrusion response and recovery techniques were proposed. In that existing work it is based on the game play method of finding the intruder and provides a response through their play of the game. Here it is present the game in the distributed network and the game is played by the network header, if the real header play the correct method means we can allow the data to that network user, incase they were played the method in wrong manner means we provide the response and recover the data from the intruder, here the real header contains the method of play through the hind which they already have [4, 5]. From this if the real header play it in wrong method means all the client user under the header also suffer from the access of the data, so it will be the great drawback from the existing work. To overcome this issue we enhanced the game theory based on the individual play in the network to avoid the suffering of misplayed game played by the header. Here proposed a series of optimal game-based strategies for handling increasingly sophisticated flooding attack scenarios. The proposed system presents a game-theoretic study of the problem of routing, resource allocation and security based issues. The problem is formulated as a non-cooperative game, in which each user aims to maximize its own bandwidth by selecting its routing path.

2. LITERATURE REVIEW

In paper [6] they considered the problem of providing anonymity to network communication when adversaries compromise an unknown subset of nodes in the network. They invent a game-theoretic equivalent, and proved the survival of Nash equilibrium. While the numerical simulation was based on a simple switching network, the solutions indicate that this approach can provide a significant insight into optimal design of anonymizing strategies as well as the optimal adversarial behavior. The difficulty of computing the Nash equilibria has not been dealt with in this work, but it is an efficient algorithm for this purpose would fortify the results here, and is part of ongoing research. In this work, they have used a specific network model, and assumed knowledge of topology and sessions. A similar approach for random networks with random connections could shed valuable insights on scaling behavior of anonymous communication

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

The work [7, 8] presented a framework to classify DoS attacks into single- and multi-source attacks. In addition to using packet headers to classify the attacks, they develop two new approaches: initial ramp-up transients and spectral analysis. These approaches based only on information in the attack packet stream, and they believe the spectral characteristics of attacks cannot be altered without reducing attack rates. They estimate their framework on 80 attacks captured from two peering links at a moderate-size, regional ISP. They validated their framework with attacks captured at a second monitoring site, and during experiments with unreal attacks on a wide-area network, and real attack tools on an isolated testbed. They obtained experiments and simulations to clarify the underlying reasons for the difference in attack characteristics.

In this work [9] they presented a new protocol that protects against malicious bandwidth consumption by using adaptive client puzzles and pushing their generation to the intermediate routers (rather than destination servers). The routers adaptively modify the complexity level of the puzzles depending on the global measurement of flows directed to a particular destination. As in the case of other adversarial protocols such as fair exchange, alternating-time temporal logic provides a concise and powerful formal language for expressing the properties of interest. Their case studies include two client puzzle protocols and a state-of-the-art key establishment protocol.

In this paper [10] Network puzzles are an elegant mechanism for mitigating the effects of undesirable network communication. This paper has described the design and implementation of a network layer puzzle protocol and algorithm that can be used to effectively slow down flooding attacks and port scanning activity [11]. The system allows for high-speed implementations in the fast path of modern network devices, can be elastic deployed, and is resistant against replay and spoofing attacks.

This article [12, 13] they showed how the robustness of authentication protocols against denial of service attacks can be improved by asking the client to commit its computational resources to the protocol run before the server allocates its memory and processing time. The difficulties of the puzzle are parameterized depending to the server load. Here server stores the protocol state and computes classy public-key operations only after it has verified the client's solution. The puzzles protect servers that authenticate their clients against resource exhaustion attacks during the first messages of the connection opening before the client has been reliably authenticated. It should be noticed, nevertheless, other techniques are needed to protect individual clients against Dos and to prevent exhaustion of communications bandwidth.

In this research paper [14, 15] they presented a game theoretic model as a defense mechanism against a classic bandwidth consuming DoS/DDoS attack. Validation of their analytical results was performed utilizing the NS-3 network simulation tool. In their future work, we will consider the existence of multiple equilibria in some scenarios. The TCP congestion window is one example of such possibilities. Furthermore, we plan to simulate a dynamic game where both the attacker and the defender can alter their strategies during the attack event [16]. They also plan to contribute their NetHook module to the NS-3 codebases in order to make it available to other researchers interested in packet manipulation within the simulator.

3. PROBLEM DEFINITION

Network security problems are often challenging because the growing complexity and interconnected nature of Distributed systems lead to limited capability of observation and control. They are also multi-dimensional in that they entail issues at different layers of the system; for example, higher level privacy and cryptography problems, physical layer security problems, and issues on information security management. Theoretical models at the system level play an increasingly important role in network security and provide a scientific basis for high-level security-related decision making. In these models, the agents or decision makers (DMs) in network security problems play the role of either the attacker or the defender. An attacker attempts to breach security of the system to disrupt or cause damage to network services, whereas a defender obtains appropriate measures to enhance the system security design or response. In this case intrusion response systems (IRS) are necessary because intrusion prevention systems are unfeasible [17, 18]. In previous work [19] game play method of finding the intruder were proposed based on the response and recovery method. The problem in that existing work is if the real header is misplayed the game in wrong method means the entire client under the network cannot access the data, so they can suffer the access of data, so it will be the great drawback from the existing work and study the various work from [20].

4. PROPOSED WORK

To resolve the abovementioned problems, our system has constructed with the client server based approach. The server has the monitoring and puzzle providing process. In this proposed system, a client node sends out a request message to server. The server will receive all details of the client. The system presents two methods to generate puzzles according to the network behavior purposes. An important characteristic of a client puzzle is that the amount of computation needed to resolve it can be estimated fairly well. Note that the puzzles used in the defense against flooding attacks need not require naturally sequential operations. It is significant which a data cannot be accessed by anyone until a pre-determined game is solved. In recent years, a number of game-based defense mechanisms have been proposed against network attacks. Nonetheless, these mechanisms have not been designed through formal approaches and thereby some important design issues such as effectiveness and optimality have remained unresolved. This paper exploits game theory to propose a series of optimal game-based strategies for handling increasingly sophisticated flooding attack scenarios. The proposed system presents a game-theoretic study of the problem of routing, resource allocation and security based issues. The problem is formulated as a non-

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

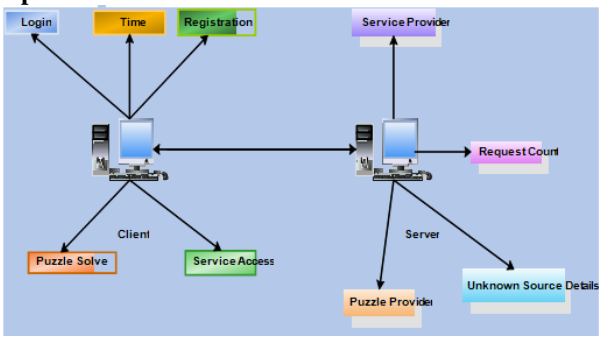
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

cooperative game, in which each user aims to maximize its own bandwidth by selecting its routing path. The proposed system deals with the following problems.

1. Resource allocation and selfish detection
2. Sybil users
3. Unknown source detection.

If the flooding attacks arises means; the amount of resources may increase. The system should overcome the above drawback by providing proper puzzle. The client should solve the given puzzle within the time is more important.

Proposed Architecture:



This proposed system ensures a view on which nodes will try irrelevant or malicious activities due to their compromised nature, as they want to increase their reputation in the network. The defending system also wants to recognize the malicious nodes and block them from participating in network functions, but it would desire not to risk it and have the least amount of false discovering, to maximize its own utility. The benefits of using a framework based on repeated games is that, the base station has a history of the previous games and when a node is malicious it gets a negative reputation when the total reputation accumulates, a path consisting of less number of malicious nodes is chosen to be the server. This results in blocking of malicious nodes.

4.1 PROPOSED METHODOLOGY:

Our proposed system handling below said modules to achieve the security in the network.

(i) Handling Client:

Clients are the users who will send the data to the receiver and they also can get the responses of their request from the server. Mainly clients are connected the data with their puzzle. The client phase contains three steps,

- Connect the server
- Registration with the puzzle
- Login

So that client can access the data by playing the correct method.

(ii) Server Responses:

Admin is the main controller of the network communication. Admin is just like the puzzle authority. Server is the databases which will responses to the client's request. According to the following rules the server will send response.

- Puzzle selection
- Request processing
- Unknown host management
- Repeated count
- User behavior

The puzzle based service provider is used to provide the resource to the requested client. The client information detail is checked before providing resource to the requested client.

(iii) User wardrop Equilibrium:

After the completion of user gain level access the server will provide the service for based on the client request. It has the three label parameter it providing the service is the directory. When the user select the file and double click on the file that time the file is downloaded successfully for user access the service from the distributed network. The network has separated by workgroups.

This module will help us to connect and access server in the network. After connected the server, the module will get the requested machine details such as protocol, IP, time and request service. For a unchanging routing policy of the traffic engineer, there exists a simple characterization of equilibrium among infinitesimal users that generalizes the well-known Wardrop equilibrium.

(iv) Game Theoretic settings:

The puzzle generation module is used to display the puzzle game. The puzzle game is displayed only when the user enters the details and clicks the puzzle button. Then the instructions are displayed to user for rearranging the puzzle. Similar the same operation about the previous function but in order to added the user register page. It has information about the registered user information.

It also contains the same function of the listen () function and its verified the user is validated user or new user to have an access in distributed network. When the user connects the server, the server will provide a puzzle with default instructions. The users have to register with their personal data and selected puzzle. To answer such questions, this paper begins by modeling the interaction between users of a content distribution network (CDN) and the ISP's traffic engineering in a game-theoretic setting.

(v) Monitoring Client ad defending attacker

In this module, the server has to monitor the client requests, which are sent to the server with certain data's. The server will present different kinds of puzzle for unregistered users and known puzzle for registered users. Based on the repeated count and playing strategy the server will identify the attacker.

After the identification of the attacker the server will send a mail about the attacking. Identify unknown resource module is used to display the sever page. All the registered user information is stored in server. The client movement of the puzzle is displayed in the server page.

DOI 10.17148/IJARCCE.2015.4108

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

4.2 PROPOSED IPDRS ENGINE:

Input: IDS, AART
Steps:

1. Read the IDS alert
2. Read the Attack response tree and its Subconsequence
3. Local Engine Process:
   a. State space generator (SG)
   b. Perform decision making process by the local engine L using the ART.
   c. Return R from ART.
4. Transmit R to the RRE agent.
5. Global Engine Process:
   a. Read Local RRE engine report R.
   b. Analyze the network topology.
   c. Perform the state space alert in Global engine
   d. Perform decision making process by the global engine L using the R.
6. Perform the result fusion for final decision making.

GAME THEORY: WARDROP EQUILIBRIUM

GAME THEORY:
WARDROP EQUILIBRIUM

The game being played each period

- A_i the action of player i taken in period t
- $a_t = (a_1^t, \ldots, a_n^t)$ the list of what each player played at t

History:

a list of what has happened in every login period up to the present

- $h^t = (a^1, \ldots, a^t)$ the list of what happened in each of the first t periods
- H^t the set of all possible histories of length t.
- $H = \mathbf{U}_t H^t$ the set of all possible finite histories.
- $S_i : H \rightarrow (A_{iA})$ a strategy of i
- $S_i (h^t)$ specifies what i will do after a history h^t

So, $S_i (h^t)$ is a choice of a play in period t+1 after observing what happened in all previous periods.

5. EXPERIMENTAL RESULT

The experimental results shows the improvement of our proposed system, our system has constructed with the client server based approach. Our modules contain the above said methodologies to overcome the existing problems. By our system the server has the monitoring and puzzle providing processes to the client when it wants to access the data from the server. A client node sends out a request message to server. The server will receive all details of the client. The system carries two methods to produce puzzles according to the network behavior purposes. An important characteristic of a client puzzle is that the amount of computation needed to resolve it can be estimated fairly well. Note that the puzzles used in the defense against flooding attacks need not require naturally sequential operations. It is significant that a data cannot be accessed by anyone until a pre-determined game is solved.

Evaluation Results: For our evaluation result here we recognize the node by its number of unique properties. Such as IP address, port and client id with the date and time. The following are the evaluation results of performance measures:

Client Details

IPAddress	Protocol	Message	Received Time
127.0.0.1	Tcp	RequestService	2:16 PM
192.168.1.104	Tcp	RequestService	2:17 PM
192.168.1.104	Tcp	RequestService	2:18 PM

Table 1: Client Details

For our proposed system we have taken the Client Details like their IP address, port and client id with the date and time to find out the attackers and the normal user among the network.

Metrics: We taken the metrics as a Number of client's requests: Malicious behavior affects performance in a number of ways. The system considers different puzzles, and sees the effect of random puzzle selection based on multi-hop flows and requests.

Throughput: we achieve the throughput from the following chart. This measure characterizes the total number of forwarded packets over the total number of received packets.

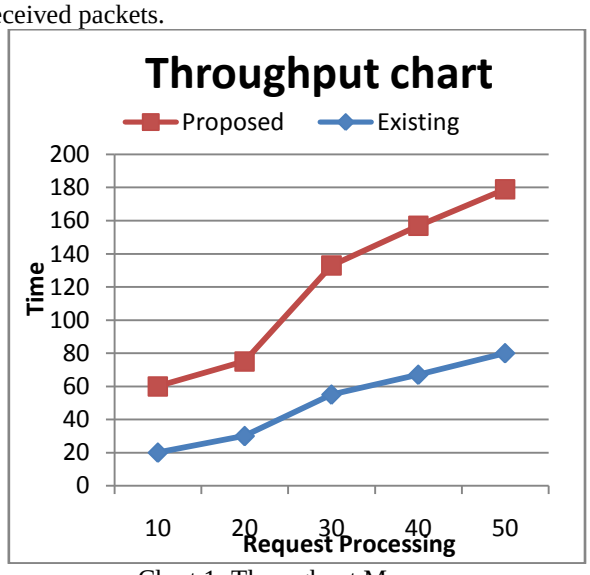


Chart 1: Throughput Measure

The above chart illustrates throughput as a function of the percentage of attackers. The figure indicates that without any attacking node, legitimate nodes spend 60% of their

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

time successfully access, and the remaining 40% having broken by flooding and trying to re-establish the request.

Attacking identification: The Chart 2 represents the time variance between the normal user and the attackers. If the attacker attempt to solve the game by taking more counts and time. The system will find out the time variance in order to detect the attacker.

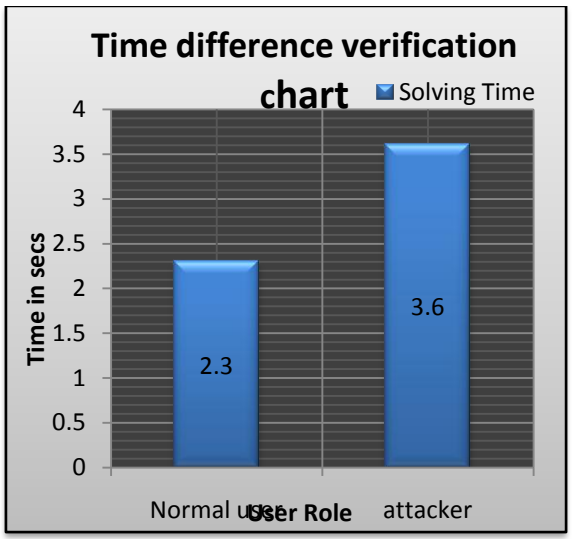


Chart 2: Time variance between the normal user and the attackers

The server will maintain the time and clicks of the given puzzle. The time and clicks may vary based on the user and attacker. The system will effectively find the attack with minimum time span. A number of puzzle-based defense mechanisms have been proposed against flooding denial-of-service (DoS) attacks in networks. Nevertheless, these approaches have not been designed through formal approaches and thereby some important design issues such as effectiveness and optimality have remained unresolved. This utilizes game theory to propose a series of optimal puzzle-based strategies for handling increasingly sophisticated flooding attack scenarios.

Behavioral identification: This identification is based on the type of click when playing the game and repeated count of their play occurred in the game.

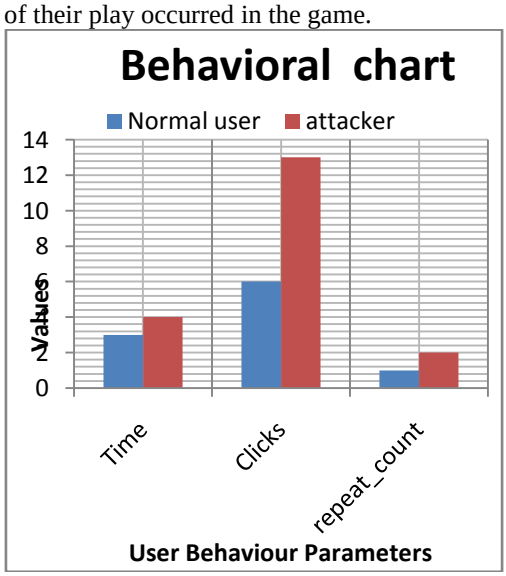


Chart 3: User behavior Performance

The above chart represents the main parameters to the proposed method. The system verifies the above parameters with the attacker behavior based on the attacker by the count of puzzle request. And the system will find the frequent request.

Our experimental results achieve the problem of network security. The DOS flooding attacks have been identified by monitoring the request flow from the client node in every particular time interval. If the flow is too random, the system will find the node sends and tried to send traffic based attacks. This kind of monitoring enables the server to detect the malicious node rapidly.

6. CONCLUSION & FUTURE WORK

Current intrusion detection systems (IDS) have limited response mechanisms that are inadequate given the current threat. Our proposed system based on the 3 techniques of prevention, detection and when attackers attack our network we use the response technique by using the game theory based response technique. It achieves the better security among the network. And also our system proposed a game based defending system against intrusions. The system has implemented with the user wardrop method. In future work will expanded with some other game theory. Along with the came the system may use additional security like graphical passwords based authentication. This section discusses some aspects of the puzzle-based defense mechanisms proposed in this paper and outlines future researches in the game-theoretic study of the client- puzzle approach. It also compares these mechanisms with some of the earlier puzzle-based defenses against flooding attacks. If the game continues at each period with a probability less than the unity, it is also of discounted payoffs, where the future payoffs are lowered using a discount factor.

REFERENCES

[1]. Liang, B. (2000), How To Guide-Implementing a Network Based Intrusion Detection System. Available at:http://www.inguardians.com/research/docs/switched.pdf Last accessed: 15.07.2011

[2]. Debar, H. (2000). An Introduction to Intrusion-Detection Systems. Available at: http://www.syros.aegean.gr/users/tsp/citations_dnl/Debar00a.pdf Last accessed:17.07.2011

[3]. Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.6603

[4]. Holz, T., Meier, M., and Koenig, H. (2002). An Efficient Intrusion Detection System Design. Available at: http://icsa.cs.up.ac.za/issa/2002/proceedings/A014.pdf

[5]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proc. Information Systems Security Conf., pp. 353-65, 1997.

[6]. D. Ragsdale, C. Carver, J. Humphries, and U. Pooch, "Adaptation Techniques for Intrusion Detection and Intrusion Response System," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 2344-2349, 2000.

[7]. Curtis A., Carver Jr. - "Intrusion response systems a survey".

[8]. Manshaei, Mohammad Hossein, et al. "Game theory meets network security and privacy." *ACM Computing Surveys (CSUR)* 45.3 (2013): 25.

[9]. Jackson, Matthew O. "A Brief Introduction to the Basics of Game Theory." (2011).

[10]. Alpcan, Tansu, and Tamer Basar. "A game theoretic approach to decision and analysis in network intrusion detection". *Decision and Control, 2003. Proceeding. 42nd IEEE Conference on*. Vol. 3. IEEE, 2003.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

[11]. 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.
[12]. O.P. Kreidl and T.M. Frazier, "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System," IEEE Trans. Reliability, vol. 53, no. 1, pp. 148-166, Mar. 2004.
[13]. I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using Specification- Based Intrusion Detection for Automated Response," Proc. Int'l Symp. Recent Advances in Intrusion Detection, pp. 136-154, 2003.
[14]. K. Lye and J. Wing, "Game Strategies in Network Security," Int'l J. Information Security, vol. 4, pp. 71-86, 2005.
[15]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proc. Information Systems Security, Conf., pp. 353-65, 1997.
[16]. 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.
[17]. 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.
[18]. Anuvarsha.G and RajeshKumar.J, "Survey On Automated Intrusion Response System Using Game Theory", IJARCCE-2014.
[19]. 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, 2014.
[20]. 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.

DOI 10.17148/IJARCCE.2015.4108