ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A New Cryptographic Puzzle with Effective Counter Measure

M.Suganya[1], M.A.Gopisaran[2], R. Reshma Sony[3]

M.E Student, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, India[1]

Asst. Professor, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, India [2]

M.E Student, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, India [3]

ABSTRACT: Internet is the booming and promising domain in the current scenario, where enabling a single computer to serve many users globally using their geographical information's. Due to this widespread nature, the system affects by several security threads. In this study, we propose an optimal game theory to Internet security systems (ISSs) against different types of security threads. In order to manage internet with secure features, the proposed system creates a novel game theory driven approach named as TRAP. In specific, TRAP prevents ISs from intrusion and unauthenticated behavior. The main process of the proposal is the detection and prevention of intruders using game theory and another motive is to propose a solution to provide response for intruders. Honey_trap also improves the performance of the proposed scheme using the C#.net Platform and this pinned with existing server features, and a set of performance metrics such as: false alarm reduction, control communication overhead and improvement in accuracy along with other QOS metrics. This study proposes a new pattern for intrusion detection in ISs using fusion based paradigms, which are adaptive low interaction honey pots and game theory concepts. This approach performs the interaction between the game theory and honey pot. This effectively applies the production honey pot technique along with the new game theory approach; here the game theory is a non cooperative game theory concept.

KEYWORDS: Game theory, security, Puzzle, DOS attacks

I. INTRODUCTION

Denial and Distributed denial of services (DOS, DDoS) attacks attempt to exhaust internet server resources such as computation power, memory and network bandwidth by spreading fake requests, this will affect the server performance. These types of fake requests drain the resource of the server. As the server has to spend a lot of CPU time in completing the requests, it may not have sufficient resources left to handle service requests from the legitimate users. This will result in poor throughput. DoS and DDoS are effective if attackers spend much less resources than the victim server or are much more powerful than normal users [1]. The attacker spends insignificant effort in producing a request, but more computational overhead consumed at the server side due to this enormous requests. In this situation, traditional tools do not enhance the availability of the services; besides, they may degrade service quality due to expensive operations [2].

The seriousness of the DoS and DDoS problem and their increased frequency has led to the advent of numerous defense mechanisms. In this paper, we are concentrated on the countermeasures to DoS and DDoS attacks with optimal feature selection. Client puzzle is a well-known approach to increase the cost of clients as it forces the clients to carry out heavy operations before being granted services. In general, a client puzzle scheme consists of several process: puzzle generation, puzzle solving by the client and puzzle verification by the server. Using this puzzle mechanism, we proposed a new game theory with optimal counter measure against different attacks in the network structure.

1.1 Game Theory;

This chapter discusses about the game theory. In general, game theory can be separated into two branches; named as non-cooperative and Cooperative game theory [3].

Non-cooperative game theory: This studies the strategic choices resulting from the interactions among competing group of actors, where each actor chooses its strategy independently for improving its own performance or reducing its losses. For solving non-cooperative games, several concepts exist under the non-cooperative game theory

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

such as the celebrated Nash equilibrium. The main applications of non operative game theory are many, such as distributed resource allocation, congestion control, power control and Spectrum sharing in cognitive radio [4].

Cooperative game theory: this provides analytical tools to study the behavior of rational players when they work together. The main branch of cooperative games describes the formation of cooperating groups of players, referred to as coalitions [2] that can strengthen the players' positions in a game [5].

1.3 Game Theory and Its Security

Game theory (GT) is a domain under applied mathematics that deals with multi-person decision-making situations. GT is devised for the purpose of accounting for interactions among strategies of rational decision makers and it is essential for determining a preferred strategy where such interactions are in play. GT contains a game which generally consists of a set of players, a set of strategies for each player, and a set of corresponding utility functions for every game. A strategy for a player is a complete plan of actions in all possible situations throughout the game. In any games, the players try to act selfishly to maximize their consequences according to their preferences. These preferences are expressed by a utility function, which maps every consequence to a real number [6].

Nash equilibrium is a solution concept that describes a steady state condition of the game; no player would like to change his strategy unless there is a better strategy that can result in more utility that is favorable for the player current.

Honeypots can be classified based on their deployment (use/action) and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. production honeypots
2. research honeypots

Production honeypots (PH) are easy to use, capture only limited information, and are used primarily by companies or corporations. PH is placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do[7].

Research honeypots (RH) are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats. RH are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations[8].

II. PROPOSED SYSTEM

2.1 Proposed system

In the field of Internet, there is a course to acquire methods for detecting intrusions and private access by an attacker against the stability of Internet, by using game theory based intrusion detection schemes. In literature there are few exploration has been done in the development of optimal game theory in ISs for intrusion detection over ISs.

This paper implements an optimal game theory to Internet (ISs) against intruders. In specific, the study of intrusion and unauthenticated behavior has been implemented in Internet. The main process of the proposal is the detection and prevention of intruders using game theory and another motive is to propose a solution to provide response for intruders. The last objective is the performance evaluation of the proposed scheme using the C#.net Platform and this pinned with existing sensor features, and a set of performance metrics such as: false alarm reduction, control communication overhead and improvement in accuracy along with other QOS metrics.

This study proposes a new pattern for intrusion detection in ISs using fusion based paradigms, which are adaptive low interaction honeypots and game theory concepts. This approach performs the interaction between the game theory and honeypot. This effectively applies the production honeypot technique along with the new game theory approach; here the game theory is a non cooperative game theory concept.

This analyzed numerous existing game theory models and uses a new game theoretical model optimal for ISs, where the new approach analyzes the past behaviors and performs iterative learning from the log.

Advantages of the proposed framework:

- The proposed method expands the security of ISs and also reduces the cost caused by IDS and monitoring sensor nodes.
- The method also considers the detection of selfish nodes in the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- Improves the accuracy and reduces the false alarm.
- With the use of new chronological data, the behavior of intruder can be easily identified.
- Detection of multiple attacks
- Energy efficient framework
- Reducing false alarm
- Tracking of attackers and broadcasting the attacker details
- Robust and optimal

2.2 CONTRIBUTIONS:

The contribution of this study consists of a game theoretic framework against Intruders over ISs. This proposes and analyzes an interactive learning game model driven from honeypot mechanism. This influences the equilibrium solutions for the proposed model and analyzes the resultant strategies of the attacker and the defender. This also proposes the use of chronological behavior of client nodes to reduce the communication overhead. This also performs intrusion response system in ISs to reduce and schedule the resource utility issues. So this is a mixed strategy equilibrium solutions which is a non-cooperative game theory.

- Proposes a new scheme named as TRAP, which is a honeypot technique driven game theory with interactive learning mechanism.
- Utilizes the production honeypot technique, which helps to gather information about the the intruder community targeting from different clusters.
- Introduces a new game theory with the fusion mechanism which is named as honey_trap which is an extension of stochastic game model.
- This also finds the selfish node in the network.
- And also finds flooding, spoofing attacks in ISs using the Honey_Trap strategies.
- Produces a chronological equilibrium instead of existing nash equilibrium.

III. METHODOLOGIES

Honey_Trap games where the uncertain data are only known to belong to a given set can arise when the data are subject to random measurement errors these conditions are well applicable to the intrusion detection problem of interest in this research. In this chapter consider a two-player, nonzero-sum version of the Honey_Trap game to model the interactions between an Intruder (player 1) and the defender (player 2) in a typical ISs.

Honeypot are used to monitor the attacker's behavior. It is an information system that allows the intruders to interact with it. The value of Honey_Trap lies in unauthorized use of that resource which finds the intruder in ISs. Honey_Trap appeals attackers by providing some false or fake information at the time of detection. Honey_Trap require very less resources to run, therefore they are easy to use. Through Honey_Trap events and activities of the attacker on the network are captured. This will be helpful in learning new malicious activities, methods and evidence can be collected against an attack for legal use and network security.

In this study the interaction between an attacker and the defender system as a basic signaling game which falls under the dynamic non-cooperative game with incomplete information. This is also associated with the above information gathering process by honey_Trap. In a non-cooperative game with incomplete information these model situations in which some players have some private information before the beginning of a game. This initial private information is called the type of a player and it fully describes any information the player has which is not common knowledge. A player may have several types one for each possible state of their private information. It is also assumed that each player knows their own type with complete certainty.

In Honey_Trap model of the dynamic game, a sensor node is the sender and the server (Cluster Head) attached with IDS is the receiver to which the data is transmitted. The client nodes private information is identified as their sensed data. The sensor node divided into two types: the node could be a regular node or that could be a intruder or attacker.

The type space of a given sender is therefore given by Θ = [Attacker, RegularNode]. The IDS prior beliefs concerning the probability that any other node in the system is either an attacker or a regular node can be described by a single number $q \in [0, 1]$. The malicious node's (attacker) decision is a choice between exhibiting malicious behavior or exhibiting normal behavior. Let the probability of a particular malicious node exhibiting malicious activity be s and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

the probability of the same node exhibiting normal behavior be 1 − s. The particular choice that the attacker makes is his "message". The IDS "detects" this decision with a probability t and misses it with a probability 1 − t depending on his beliefs.

Scheme design not only provides the right incentives but also to ensure the participants tell the truth. It can balance individual behavior and common behaviors. The following terms related to procedure:

Definition 1: Procedure can be expressed as M = (λ, P), where M means some kind of procedure, λ is the output function, λ = λ (λ1, λ2, ...,λn) P is the reputation function, P = P (P1 (λ), P2 (λ), ..., Pn (λ)).

Definition 2: (Strategy proof Procedure) In the procedure M any sensor node i, its true value ti, the access vector b−i, agent i in order to obtain maximum points only by submitting a real access and behavior (i.e., bi = ti), the procedure is strategy proof.

Definition 3: (Voluntary participation condition) In the procedure M, any agent i, as long as it honestly access, it cannot get negative points, then this procedure to meet the voluntary participation condition.

In a Procedure a sensor node is called an agent, there are usually n sensor nodes, each sensor node i (i = 1,2,...,n) has some private information which is known as the type of the agent or called the true value ti, the private value is only known by sensor node, and is confidential for the other sensor nodes. In a mechanism design strategy proof condition will make all participants report their true value and voluntary participation condition can ensure that all participants are willing to participate

3.1 Honey_trap:

In Honey_Trap framework intrusion detection is looked at in the form of a non-cooperative nonzero-sum game without have the interaction between sensor nodes. Here the players are the intrusion detection system (IDS) of the ISs which is named as Honey_Trap and the attacker. The Honey_Trap IDS wants to preserve functionality of the network by preventing those intrusion and malicious attacks. The model for the ISs is a large network of nodes sorted into clusters. The existing IDS defend a cluster. Due to system limitations the exisitng IDS can only defend one cluster at a time. The existing game formulation is rather unproductive. The honey_trap increases the complexity of attacking choice over ISs. The HT (Honey_Trap) defends attacks in almost all clusters at a time.

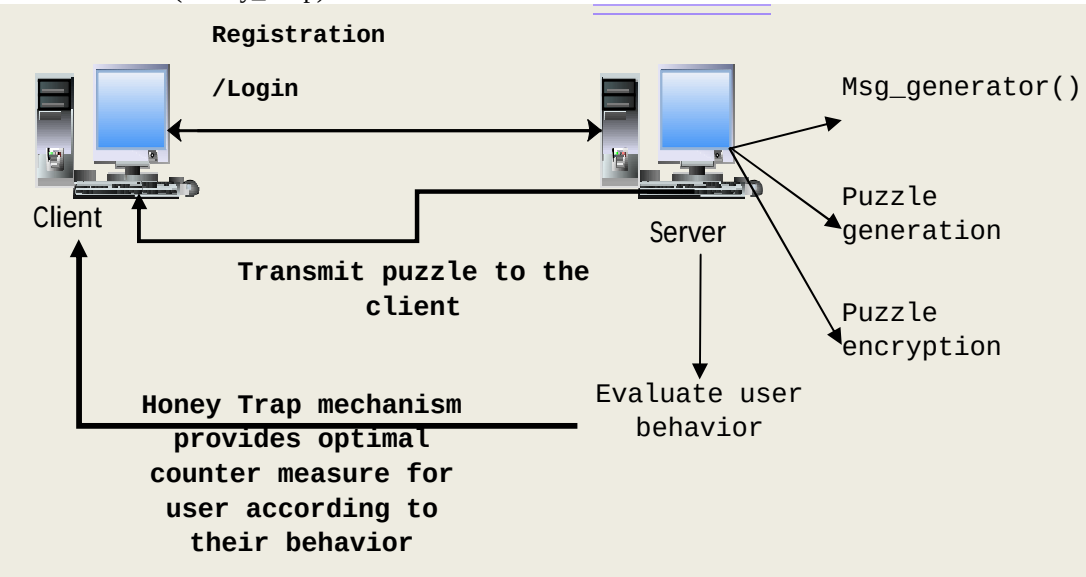

Fig 1.0 honey-trap working mechanism

In the HT framework each node and cluster will have to act independently of the others. This HT limits the playing strategy which has decided by the ID. The current framework facilitates the intrusion prevention, detection and response schemes in a quicker way. For effective prevention the HT provides different strategies and for detection HT provides chronological equilibrium and finally for response, the HT provides effective payoffs and honeypot techniques.

1. HT monitors every client nodes and their usage log.
2. Finds the attacker by verifying the usage log

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

a. When an attacker investigates an unused IP, HT detects the system and limits the resources.
b. For prevention and detection, the HT refers different strategies.

3. Provide different strategies for prevention and detection of intruders.
4. In certain cases it uses effective payoff for intrusion response system.
   a. Honeypot based payoff function finds and tracks the intruder details.
5. Broadcasts the intruder details to other server.

Intrusion Prevention System is a network module which monitors the radio spectrum to detect the existence of un-authorized access points, and can do automatically intrusion prevention by generating alerts accurately using the game theory. The main purpose of an intrusion prevention system is to prevent un-authorized network access to Internet and other information resources by wireless devices. IPS which is an extension of IDS not only detects wireless intrusions also prevents them.

This section examines the Honey_trap game theoretic framework to analyze and model the response of IDS. Here IDS response actions include broadcasting attacker details, watching suspicious activity before broadcasting, and a total system reconfiguration and data collection from attacker. This model the interaction between an attacker and a honey_trap as a non-cooperative zero sum game with chronological equilibrium for effective intruder tracking. In the honey_trap game, the aim of the system is to send a fake report to the attacker, in order to find their details. The attacker is believed successful when the fake message reaches the attacker machine. Honey_trap also identifies the selfish activity in ISs.

The following table describes the strategies involved in the Honey_Trap.

Playing strategy	Type of attack
Position, identity verification Authentication, monitoring, redundancy	Spoofer node/ Sybil attack
Authentication, packet leashes by using geographic and temporal info, threshold	Flood attack
Traffic details and other statistics are different ex time	Intrusion
maximum value of average retransmission numbers in the period threshold verification	Selfish attack

Table 1.0: playing strategies

From the above table, the honey_trap mechanism finds the attack by applying various strategies. To find the spoofer node in ISs, the techniques gets the position, redundancy and authentication details. Like the same above flood attack can be identified. The overall interruption will be identified by applying Gaussian driven verification with above parameters. Finally based on the same Gaussian model the system identifies the selfish attack also. After the successful detection, the system performs broadcasting attack information process. The honey_trap creates a fake node to cheat the intruder. As like the above playing strategy, the following table describes the defense strategies involved with honey_trap.

Intrusion	Defense strategy
Misdirection	Source authorization
Flooding	Limit the connections
Spoof	Find the spoofer- eliminate the spoofer Broadcast spoofer details
Selfish	Calculate credit score and limit resources
Black holes	Multiple routing paths
Overall intrusion	Fake reply to the attacker

Table 2.0: defense strategies

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Different strategies and chronological equilibrium in ISs can provide differentiated detection capabilities at different constraints and locations. This proposal analyzes the problem of intrusion detection in a heterogeneous cluster based ISs, by characterizing intrusion detection probability with respect to playing and defense strategies.

IV. RESULTS AND ANALYSIS

The first set of experiments is to compare the performance of different combinations of existing game theory schemes, node verification strategies. All strategies are tested under two request patterns: attack detection accuracy and verification delay.In more specific the chapter particularly interested in the total number of data's and verification delay during a secure data transmission and the average processing time of a verification process since they are the dominant factors affecting service quality experienced by the users.

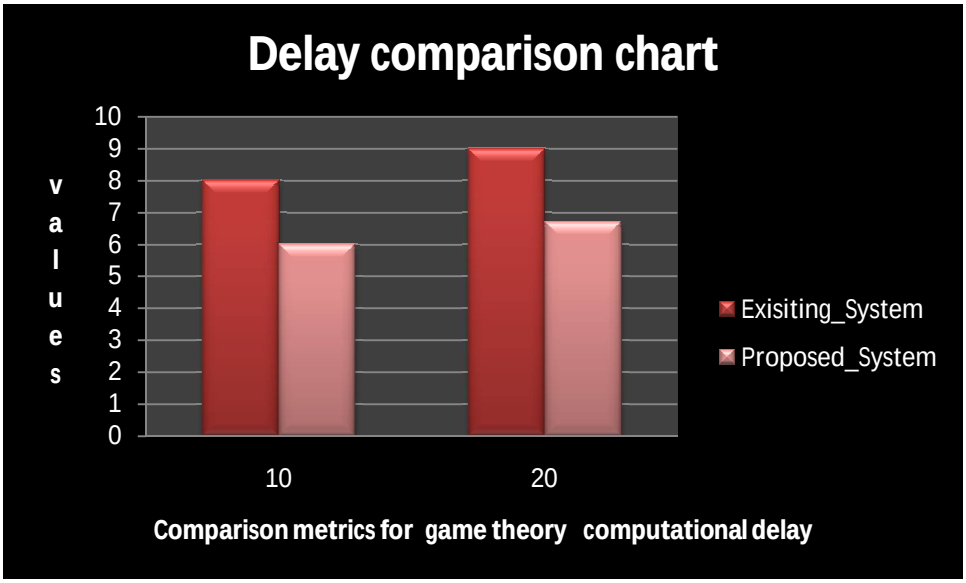

Figure 2.0 shows that all strategies perform significantly better than traditional game theory schemes. Since the enclosure of the later makes others hard to compare, this exclude the strategy for all subsequent figures.

V. CONCLUSION AND FUTURE WORK

The paper considered the intrusion detection problem on distributed network and designing a new game theory driven approach named as Honey_Trap, a honeypot and game theory approach for secure distributed networks. In this study the interaction between an attacker and the defender system as a basic signaling game which falls under the dynamic non-cooperative game with incomplete information. This is also associated with the data gathering process by honey_Trap. In a non-cooperative game with incomplete information these model situations in which some players have some private information before the beginning of a game. This initial private information is called the type of a player and it fully describes any information the player has which is not common knowledge. The experiments and results show the proposed honey_trap mechanism can effectively identify the intruder at the time of data transaction.

As future work, the system leaves the co-operative game theory framework with honey-trap for further implementation. The system can also include other type of intrusion detection schemes rather than game theory.

REFERENCES

1. Wu, Yongdong, et al. "Software puzzle: A countermeasure to resource-inflated denial-of-service attacks." *Information Forensics and Security, IEEE Transactions on* 10.1 (2015): 168-177.
2. Kohli, Rajeev, and Heungsoo Park. "A cooperative game theory model of quantity discounts." *Management Science* 35.6 (1989): 693-707.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

3. 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.
4. Suris, Juan E., et al. "Cooperative game theory for distributed spectrum sharing." *Communications, 2007. ICC'07. IEEE International Conference on*. Ieee, 2007.
5. Agah, Afrand, et al. "Intrusion detection in sensor networks: A non-cooperative game approach." *Network Computing and Applications, 2004.(NCA 2004). Proceedings. Third IEEE International Symposium on*. IEEE, 2004.
6. Chapman, Archie C., et al. "Decentralised dynamic task allocation: a practical game: theoretic approach." *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*. International Foundation for Autonomous Agents and Multiagent Systems, 2009.
7. Manshaei, Mohammad Hossein, et al. "Game theory meets network security and privacy." *ACM Computing Surveys (CSUR)* 45.3 (2013): 25.