ISSN:0975-9646

A Review on Byzantine Attack Detection and Prevention Using Game Theory

Ms.Chetna Guntewar
Department of CSE,
G.H.Raisoni Institute of Engg &Technology for Womens
Nagpur, India

Mrs. Vaishali Sahare
Department of CSE,
G.H.Raisoni Institute of Engg &Technology for Womens
Nagpur,India

***Abstract*— MANET is the collection of various wireless mobile nodes. Security is of high concern in mobile ad hoc network as it has no centralized authority which can oversee the particular node working in the network. The attacks can be preformed from both inside and outside the network. Nodes within surrounding to gain common radio link can be often used to set up ad hoc infrastructure. But the safe communication between mobile nodes needs the secure communication link to interact in network. This paper focus the security and reliability of mobile ad hoc network from Banzantine attack with the help of mean-field Game theory. Game Theory is approach that can allow a single node in mobile ad hoc network to make strategic security defense decision in absence of centralized administration. This paper gives attack defense system in MANET using game theory.**

Keywords—Mobile ad hoc network, Game theory,Banzantine attacks.

I. INTRODUCTION

A. Overview

MANET is infrastructure less network which is used to communicate through independent node with changing topology and conserved bandwidth. In Mobile ad hoc network, a network is conceived changing through the group action of the impulsive set of independent nodes. There is no stable arrangement of nodes playing specific role in network. Each node can be a sender or receiver or lie between the path from sender to receiver. Rather each node makes its own decision severally, without using centralized authority. The characteristics of mobile ad hoc network includes weak physical protection of nodes, dynamically changing topology, no centralized administration, high dependence on inherent node co-operation and limited bandwidth. Each mobile device should be able to detect the instance of any other device in network and work towards facilitating communications and sharing of service and private information. Because of no centralized administration any device can easily connect and disconnect from the network. Establishing a security mechanism in wireless ad hoc network is a tough task specially when there are many attacks performed on network. Mobile ad hoc network has no centralized campus, therefore the system comprise a number of devices or nodes joined via wireless links, forming continues changing wireless network. Vicious nodes cause packet dropping, false routing and etc. Consequences of vicious nodes are shown below:

- Catty node decreases the network property in MANETs.
- The outcome is defragmented networks, sporadic nodes, and drastically degraded network performance.
- No signification for energy-saving.
- Explore all kinds of denial-of-service (DoS) attacks by replaying, reordering.

B. Types of attacks in MANET

Various parameters includes many attacks in mobile ad hoc Network. They are represented in the table given below:

Table 1: Attacks in MANET

Sr. No.	Parameter	Attacks
1	Emission	Passive , Active
2	Location	Insider , Outsider
3	Quality	Single, Multiple
4	Motivation	Confidentiality , Integrity, Selfishness, Privacy, Unauthorized access, DOS
5	Rationality	Native, Rational, Irrational
6	Mobility	Fixed Mobile

C. Byzantine Attacks

Byzantine attacks are such attacks where it expose with the set of intermediate nodes that working individual within the network carry out attacks like forming routing loops, consuming time and bandwidth by forwarding packet from non-optimal paths, selective dropping of packets which disrupt the network. Many byzantine attacks contribute some feature of selfish node, these nodes immediately affects the self-operation of nodes and do not intercept in performance of network. These nodes purposely drop the packet in order to conserve the resources. In ad hoc network byzantine attack has following types concerned with nodes: Selfish Attack, Black Hole attack, Wormhole attack, Gray Hole attack.

- Selfish Node Attack

Selfish node attack is one such attack in which a faulty node performs routing misbehavior in the route discovery packets to advertise itself as having the shortest path to the node whose packets he want to compromise. The attacker aims at modifying the information so that they can control the traffic flow of the network. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find new path to destination.

Malicious nodes quickly respond to the source node as these nodes do not refer the routing table and drop all the routing packets and also flooding the false information of shortest route in network by that the number of nodes that are in radio range directly or indirectly forwarded the routing as well as data packets in the network. The source node assumes that the route discovery process is complete and ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets

- Black hole attack

In this attack, when a vicious node sense some route request packet in the network, it reply the legitimate node by pretending that it has shortest and original route to the destination node even if no such fair route exists. As a result, the vicious nodes easily drops the packet or mislead the routing information in the network which is utilize for forwarding the packets. Figure 1 shows the strategic of black hole attack.

- Gray hole attack

It is peculiar type of black hole attack where gray hole is carried, which drop selective packets such as forwarding packets but not data packet. Figure 2 illustrate the attack.

- Worm hole attack

Worm hole connects two different points in space through shortcut path. In this attack a pair of attacking nodes can intercept the route by short circuiting the network. Worm hole attack can be performed with single node too but generally it is carried out by worm hole link. Figure3 shows the idea of this attack. The dotted line represented RERQ through worm hole. The directed line represents wireless link.

D. Motivation and Problem Formulation

The Game Theory approach explored in recent times addressing security issues in MANET focuses mostly on networks having central administration involving only 2 players i.e. attacker and defender. We propose an attack defense mechanism using game theoretic approach with multiple players for security in MANETs.

In a distributed environment there is no central administration and hence each node has to defend himself from the attacks. We propose a dynamic mean field game theoretic approach to enable an individual node in MANETs to make strategic security defense decisions without centralized administration. In game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET [2], making nodes self-reliable against attacks and enhancing security in mobile ad Hoc network.

II. LITERATURE SURVEY

Author in [1] propose a new approach to automated response called the response and recovery engine (RRE). These engine employs a game-theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game. [2] Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE [2] propose a Mean field Game Theory approach which can be applied to distributed networks having multiple players. The research make the nodes in MANET self reliable in defending the attacks by making strategic decisions depending upon the results obtained from the game theory approach. Xiannuan Liang and Yang Xiao, Senior Member, IEEE [3] have review the existing game-theory based solutions for network security problems, classifying their application scenarios under two categories, attack-defense analysis and security measurement. Moreover, he have presented a brief view of the game models in those solutions and summarize them into two categories, cooperative game models and non-cooperative game models with the latter category consisting of subcategories. Xin Jiang, Chuang Lin, Hao Yin, Zhen Chen [4] present a trust establishment scheme appropriate to the MANET environment. First, they introduce an evaluation model for trust value. Second, analyze the computational methods of the evaluation model. Last, propose the framework of trust establishment for MANET. Xiaofan He , Huaiyu Dai,Peng Ning [5] presents a game-theoretic method to analyze intrusion detection in mobile ad hoc networks. They use game theory to model the interactions between the nodes of an ad hoc network and view the interaction between an attacker and an individual node as a two player non-cooperative game, and construct models for such a game. Priyanks Goyal, Shail Batra,Ajit Singh [6] present an analysis of Byzantine attacks, propose a new algorithm for finding the intentional selective dropping attack by a node in Black Hole and Gray Hole attack. The propose algorithm successfully attempted to detect and prevent Black Hole and Grey Hole attacks using the concept of probability of attacks. Gaurav Soni1 ,Kamlesh Chandrawanshi [8] aims at creating an IDS system to detect selfish behavior of node which is refers to selfish node attacks and blocked the malicious activity carried by faulty node. Network performance is increased due to this IDS system up to 92% and provides 0% infection rate from attack.

III. GAME THEORY APPROACH

Game theory is the functional tool to render mathematical framework for analyzing and modeling decision problems, since it can locate problems where multiple attacks compete with each other. Basically it is study of plan of action for decision making in densely populated network with small interacting singular nodes. Network security management include the interactions of attackers and defenders, and the outcome of a measurement can be modified by their interactions. The actions of both the defenders and the attackers should be forecast by some mechanism.. Since the interoperation between attackers and defenders is a game process, game theory can be practically implement in every possible script to venture the actions of the attackers and then to specify the decisions of the defenders. Consequently, game theory-based solutions have been proposed for network security problems.

Game theory trace a game by declaring the entities or players enclosed in a game, game theory presume every player rational ,means when node reply to other node

action in network, each player focuses to select the response that come up with the greatest benefit. Game include the interoperation between players (nodes) in every situation. There should be atleast two entities participating in game. If entities perform action competitively than the game is said to be non-cooperative and if entities takes action co-operatively the game is said to be co-operative. The basic four elements describing in game theory are state below: Players, Actions, Payoff and Strategies.

- Players : The entities engaged in a game. These node can be institutes or any other connecting thing the role of player is to move around the network and sensing the possibility of prevention
- Actions: While roaming in the network particular player will perform certain action. It is assumed in game theory that the possible action of each player must be known to other player in the network.
- Payoff: Payoff refers to the outcome of action taken by player. The result can be positive or negative that means. we can get negative payoff or positive payoff. These return of every player is his/her payoff.
- Strategic: It is plan of action simply specifying which action to make depending on his/her knowledge of action record.

By choosing proper strategies to increase their payoff when responding to other player's action. This can direct to the concept of Equilibrium in a game that can be tempered as the solution of a game.

When defense-attack interactions in networks are discussed, they are abstracted into the following scenario: attackers discover attacks on network and defenders replied to these attacks. The following descriptions of terms are provided to explain this abstraction[3].

• System: In mobile ad hoc network, a system can be a node, a device, a host, a software entity, a process, or a collection of two or more of these items.

• Attacker: Any entities or thing that tends to attack on a network on his/her behalf for the purpose of affecting the system or carrying negative information for the owner of the system.

• Attack target: The network being attacked or at risk of being attacked.

• IDS: A software or hardware system used to sense the program occurring in a network and then used to analyze these set of program in order to detect whether an attack is occurring or has occurred.

• Virtual sensor: A software agent used to monitor the system and collect data for detection purposes. Virtual sensors can be regarded as a part of the IDS.

• Defender: An entity capable of monitoring the events occurring in the attack target, analyzing these events, determining that an attack has occurred, and responding to attacks. An IDS capable of responding to attacks on behalf of the network administrator is regarded as a defender[3].

IV. PROPOSED SYSTEM

A. Attack Defence System In MANET Using Game Theory

The first player i.e. compromised node will try to behave maliciously by making some moves like not forwarding the packets to the next node in the hop or may forward the packet on non-optimal paths or may change the route of the packet there by ensuring the benefit in terms of own resources saving or gaining incentive by including himself in non-optimal paths or trying to gain benefit to his other attacker. Such moves can be made by the attacker in the networks which can hamper the overall efficiency of the network. The second player i.e. nodes equipped with Game Theory mechanism will make the move in order to defend himself from the consequences of move made by the compromised node. The node has the knowledge about all the other nodes participating in the network.The knowledge like historical paths followed by the nodes, delays encountered etc. So the node checks the behavior for every neighboring node to find whether he is being compromised by using the knowledge about that node. If some misbehavior is encountered for the node in consideration then the decision can be made to either change the path of the communication there by skipping the node from the communication. This move will benefit the node by completing the desired communication. Figure 4 illustrate such type of decision making strategies can be formulated based upon the type of misbehavior exhibited by the compromised nodes. Circle drawn is the range of the MANET.

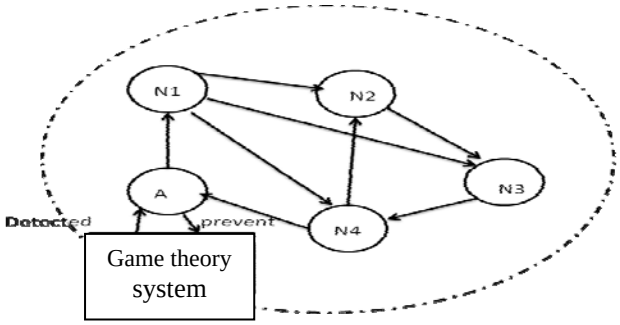

Figure 4:Attack defense system

B. Flowchart for detection and prevention

Game Theory involves players among which the game is to be played. In our proposed system the two players will be the set of Compromised node (attacker) and a set of participating nodes that are willing to communicate.

The application of Game Theory for solving the above depicted attack involves following assumptions:

•Each player is rational i.e. the objective of each player is to maximize his benefit. In our proposed system the benefit for the player who is trying to make an attack will to become selfish by not forwarding the packets to next nodes in order to save its own resources or to include himself in false routing path event though the path through him is not the shortest path etc.

•Players choose their strategy and subsequently each player is allotted some benefit. Depending upon the move made by a player, he is awarded the benefit as per the norms of the Game.

•Players have common knowledge about the game and each other's rationality. The all the players involved in the game monitors the behavior of every other player in the

game. In our proposed system every player i.e. every node monitors the behavior of every other node in the network. The behavior includes the communication history of the nodes, the paths followed by the nodes to route the packets, the delays involved in submission and reception of the packets etc. The work flowchart of the system is given below.

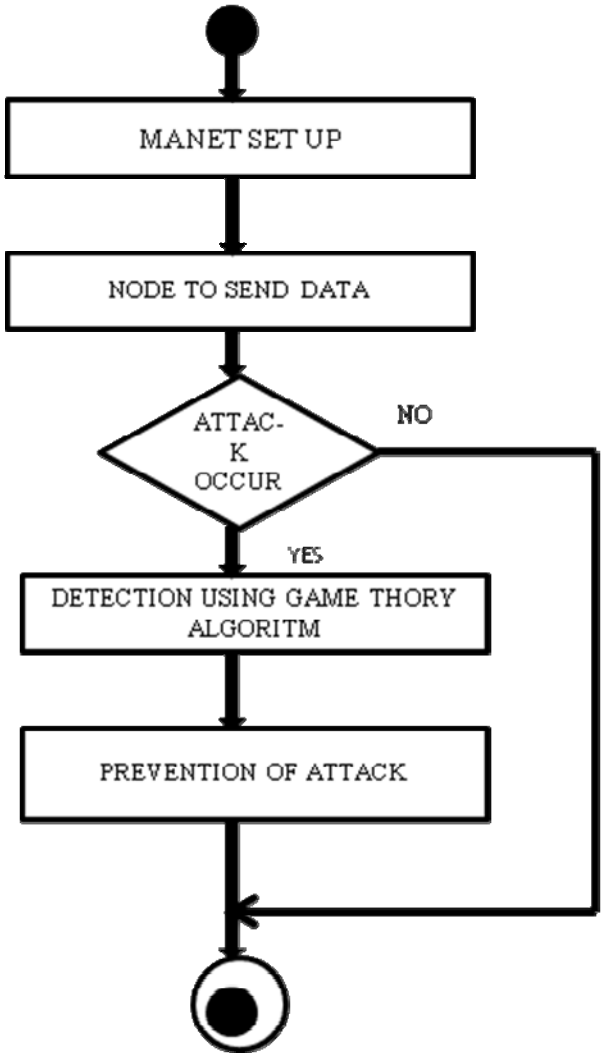

Figure 2: Flowchart of Game Theory system to prevent Attack

V. CONCLUSION

As we have discussed some short come of mobile adhoc network and their security ,the implementation of game theory in distributed MANET's will help in improving the security of MANET. Banzantine attacks are difficult to detect, these attacks are mentioned above. We have proposed the attack defense system, it will strengthen the defense mechanism in MANET which will be the responsibility of individual nodes. The mean field game theory provides a powerful tool for problems with a large number of players. The proposed scheme can enable an individual node in MANETs to make strategic security defense decisions without centralized administration to defend and detect the Byzantine attack**.**

REFERENCES

[1] Saman A. Zonouz, Himanshu Khurana, William H. Sanders, Fellow, IEEE, and Timothy M. Yardley" RRE: A Game-Theoretic Intrusion Response and Recovery Engine" IEEE *Transaction On Parallel And Distributed Systems, Vol. 25, NO. 2,* February 2014.

[2] Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks" *IEEE Transactions On Wireless Communications*, Vol. 13, No. 3, March 2014.

[3] Xiannuan Liang and Yang Xiao, Senior Member, IEEE "Game Theory for Network Security" IEEE *Communications Surveys & Tutorials*, Vol. 15, No. 1, First Quarter 2013.

[4] Xin Jiang, Chuang Lin, Hao Yin, Zhen Chen Department of Computer Science and Technology, Tsinghua University, Beijing, P.R. China, Li Su Engineer Command Collage, CPLA "Game-based Trust Establishment for Mobile Ad Hoc Networks", 2009 International Conference on Communications and Mobile Computing.

[5] Xiaofan He , Huaiyu Dai,Peng Ning, "A Byzantine Attack Defender-the Conditional Frequency Check" *2012 IEEE International Symposium on Information Theory Proceedings.*

[6] Priyanks Goyal, Shail Batra,Ajit Singh," A Literature Review of Security Attack in Mobile Ad-hoc Networks"International Journal of Computer Application(0975-8887)Volume 9-No. 12,November 2010.

[7] Gagandeep, Aashima, Pawan Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[8] Gaurav Soni1 ,Kamlesh Chandrawanshi," A Novel Defence Scheme Against Selfish Node Attack In Manet", International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, June 2013