ISSN:0975-9646

# A Survey on Forwarding Game Theory in Mobile Ad hoc Network

Ashwini Chandrashekhar Maske
*Department of Computer Science and Engineering*
*G.H Raisoni Institute of Engineering and Technology for Women*
*Nagpur, India*

***Abstract*— Game theory is mainly used to study security problems in mobile ad hoc networks (MANETs). Only two players: an attacker and defender is considered in security game model in existing works on game theory approaches for security purposes. In MANETs, the assumption is not efficient because of absence of centralized administration. In proposed system, using advances in mean field game theory, we will propose a novel game theory called Forwarding Game theory for multiple players to enhance security in MANETs. The mean field game theory gives a efficacious mathematical tool for security enhancement in MANETs. The proposed scheme will enable an individual node to make strategic security defense decision in MANETs without centralized administration. The proposed scheme merely needs to know its own state of information and the total effect of other nodes in MANET. At the same time System resources are also considered with security. So that system resources will be conserved. Ad hoc on demand distance vector routing (AODV) protocol is used for routing on demand. and Neighbor discovery protocol(NDP) is used for neighbor node discovery.**

***Keywords*— Mobile Ad hoc Network (MANET), Game theory, NDP(Neighbour discovery Protocol), AODV(Ad hoc on demand distance vector) protocol**

## I. INTRODUCTION

Mobile ad hoc network (MANET) is a network of mobile nodes connected by wireless link. It is one of the main type of ad hoc network where every node in MANET is mobile. The nature of nodes mobility changes dynamically. MANET has no fixed infrastructure. Each node functions as network router for routing packets from other nodes and for transmitting and receiving data node act as network host . The Mobile ad hoc network can be illustrated in Fig.1. One of the important issues of MANET is security. There are various attack occur in MANET due to lack of centralized administration. Attacks occur are denial of services, black hole, resource consumption, location disclosure, wormhole, host impersonation, information disclosure and interference. On security issue in MANET number of researches take place. There are two approaches exist to secure a MANET. These two approaches are prevention based approach and detection based approach. Security of MANET will be enhanced by reducing the probability of attack. Game theory is powerful mathematical tool for enhancing the security of MANET. In MANET, for route discovery routing protocol (AODV) is used. As MANET is dynamic in nature, Ad hoc on demand distance vector routing protocol is used. Ad hoc on demand distance vector protocol is used on demand. Neighbor discovery protocol (NDP) is mainly used for neighboring nodes discovery.

Game theory is used to enhance security in mobile ad hoc networks (MANETs). In existing work only two players are taken in the game model which provides security: an attacker and a defender. This assumption may be efficient for a network with centralized administration, In MANETs it is not realistic, because lack of centralized Authority. In this paper, using advances in mean field game theory, Forwarding game theory with multiple players for security in MANETs will be used. The mean field game theory gives a efficacious mathematical tool for problems with a large number of players. The proposed scheme will enable an individual node without centralized administration to make strategic security defense decisions. Also, security defense mechanisms consume precious system resources the proposed scheme considers the security requirement of MANETs as well as the system resources. Nodes in a Mobile Ad hoc network do this by optimizing their decision making based on a framework using game theory. Malicious nodes are detected and data will not send to nodes. Data will be send to the nodes which are not malicious. Also the Malicious nodes information is broadcasted to other nodes in network so that further data will not send to malicious nodes.

## II. PREVIOUS WORK

Yanwei Wang F. Richard Yu, Helen Tang and Minyi Huang [1], proposed the Mean Field Game Theoretic approach for enhancing the security in Mobile Ad hoc Network. Mean Field game Theory furnishes a mathematical tool to solve the problem of security in MANET. By using Mean Field Game theoretic approach, the nodes can be empowered to make strategic security defense decision without centralized administration.

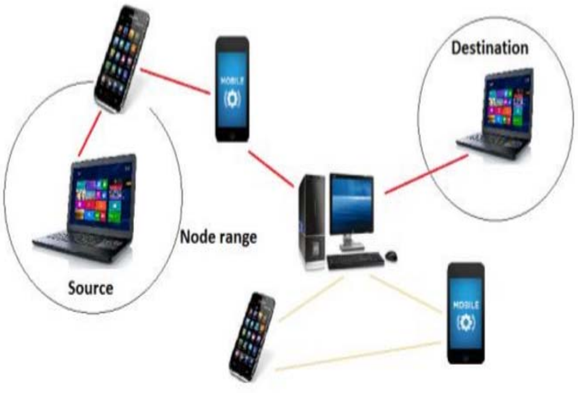

Fig. 1. Mobile Ad hoc Network

Wei Sun, Zheng Yang, Xinglin Zhang, Yunhao Liu[2], have proposed Energy Efficient Neighbor Discovery in Mobile Ad hoc and Wireless sensor Network. In that Authors mainly focused on Neighbour Discovery protocols along with minimum power consumption. Neighbour discovery is takes place even in worst case.

Q. Guan, F. R. Yu, S. Jiang, and V. Leung [3], proposed Joint Authentication and topology control scheme to improve throughput. Authors main objective is to solve authentication and topology control issues. Authors has focused on Security in Mobile Ad hoc Network with cooperative communication. They worked over a discrete stochastic optimization problem which does not need prior perfect channel status but merely channel estimate.

S. Bu, F. R. Yu, X. P. Liu, and H. Tang [4], proposed a scheme in which two approaches i.e combined continuous user authentication and intrusion detection system are combined in distributed manner. Authors considered, optimal security design with account system security requirements and resource constraints in MANETs. Authors formulated the problem as a partially observable Markov decision process (POMDP) multi-armed bandit problem.

F. Li, Y. Yang and J. Wu [5], proposed a model in which interaction among nodes in Mobile Ad hoc network is studied by using Game theory. Dynamic Bayesian signaling game is used to resolve and present the underlining connection between nodes and its better combination of actions and the cost and gain of the individual strategy. The nodes consistently update their beliefs based on the opponent nodes nature, while malicious nodes evaluate their risk of being caught to decide when to flee.

J. Liu, F. R. Yu, C. H. Lung and Tang [6], have proposed a framework that combines intrusion detection and continuous authentication in Mobile Ad hoc networks. In this proposed scheme, multimodal biometrics deployed for continuous authentication and intrusion detection is modeled to resolve system security state. Author formulated the whole system as a partially observed Markov decision process and also considered both system security requirements and resource constraints. Dynamic programming based hidden Markov model scheduling algorithms is deployed to receive the optimal schemes for intrusion detection as well as continuous authentication.

E. A. Panaousis and C. Politis[7], proposed a game theoretic approach to secure Ad hoc on demand distance vector protocol which is for routing on demand in emergency mobile ad hoc network. Game theoretic approach known as AODV-GT (AODV-Game Theoretic) is deployed and Ad hoc On-demand Distance Vector routing protocol is used to provide defense against black hole attacks along with game theory. AODV-GT is based on the non-cooperative game theory. AODV- GT is deployed as AODV in terms of malicious dropped packets when blackhole nodes occur in the eMANET.

J. Omic, A. Orda, and P. Van Mieghem [8], a has proposed unified framework that combines the N-intertwined SIS epidemic model with a non cooperative game model. Author resoveled the existence of a Nash equilibrium of the relative game and its properties are also characterized.. Author showed overall network security as its quality, which depends on the underlying topology.

A. Mishra, K. Nadkarni, and A. Patcha [9], proposed Intrusion Detection System for Wireless Ad hoc network. Intrusion detection system is detection based approach for securing a MANET. Due to lack of centralized authority, wireless ad hoc network is prone to attacks. Various techniques for intrusion detection were proposed.

## III. Proposed Work

In proposed work first step is creation of topology. After topology creation, Neighboring node discovery will take place by using Neighbor Discovery Protocol. For Routing, Ad hoc on demand distance vector protocol will be used. Forwarding game theory will be implemented in Ad hoc on demand distance vector protocol which is deployed for routing for on demand. In the Ad hoc on demand distance vector protocol, HELLO messages will be periodically broadcasted by nodes and used for link monitoring. When node A receives a HELLO message from node B, It will discover that node B will be in its wireless transmission range and therefore its neighbor. On the other hand, not getting a HELLO message from a node is considered as a broken link.

In order to use Ad hoc on demand distance vector protocol, HELLO messages to obtain neighbor information a neighbor discovery protocol (NDP) will be introduced. Neighbor discovery protocol will assume that the links are symmetric. The source ID of the sender is deciphered from the header of the HELLO messages. Every node generates a time-stamped list of its neighbors (i.e. the source ID of the HELLO message that it has received). The neighbor list will be updated periodically and outdated entries will be removed. The number of neighbors of a node is the number of entries in the updated neighbor list.

For implementation of the Forwarding Game Theory, the route discovery process and the structure of RREQ packets in Ad hoc on demand distance vector protocol will be modified. An extra field is given to the RREQ (route request) to carry the number of neighbors of the source node. When a source node generates a RREQ packet, in addition to its ID, it also inserts the number of its neighbors N , into the RREQ packet. This must done at the intermediate nodes also. When the RREQ packet is forwarded by an inter-mediate node, the number of neighbors of the intermediate node as well as its ID is inserted into the related fields of the RREQ packet. When the RREQ is received by other nodes, the number of neighbors N of the originator (forwarder) of the RREQ will be discovered. Using N in Equation, the receiver of the RREQ can calculate the probability of forwarding for that

RREQ. Then, the forwarding probability is compared to a generated uniform random number to make the forwarding decision. In the Forwarding Game theory, if the source node does not receive a RREP from the destination for any reason (e.g. link quality), it initiates another RREQ. Nodes that may not forward the RREQ in the previous round increase their forwarding capacity by 20% each time. It will give guarantee of arrival of the RREQ at the destination.

The outcome of propose scheme will show that, under most cases, implementing Forwarding game theory in a Ad hoc wireless network is beneficial by helping reduce the amount of voltage consumption throughout the network. By adding a decision making process of when to send and not to send packets, the sensors conserve energy while maintaining the throughput. The propose scheme will include experimenting with different strategies in order to save power, as well as improving the accuracy of our malicious node detection procedure.

## IV. Proposed Solution

From the idea of the proposed system we are clear with two outcomes.

1. *Detection of Malicious Nodes*

   The first step after route establishment and neighboring node discovery is to detect Malicious node using Forwarding Game Theory.

2. *Enable a node to make strategic Security defense decision*

   After Detection of Malicious nodes, the nodes can be enabled to make strategic security defense decision.

## V. Conclusion

The proposed system will used for enhancing security in MANETs by modeling the interactions among a malicious node and a large number of legitimate MANET nodes. Unlike the existing works on security game modeling, the proposed scheme will be enabled an individual node in MANETs to make distributed security defense decisions. Both security requirement and system resources will be considered in the proposed scheme. Multiple attacker and defenders will be considered in Propose system.

## References

[1] Yanwei Wang F. Richard Yu, Helen Tang and Minyi Huang, “Mean Field Game Theoretic Approach for Security Enhancements in Mobile Adhoc Network,” IEEE Transaction on Wireless Communication. Vol. 13, No.3,March 2014.

[2] Wei Sun, Zheng Yang, Xinglin Zhang, Yunhao Liu, “Energy Efficient Neighbor Discovery in Mobile Ad hoc and Wireless sensor Network,”IEEE Communication survey , vol. 16 No. 3, 2014-10-18

[3] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, “Joint topology control and authentication design in mobile ad hoc networks with cooperative communications,” *IEEE Trans. Veh. Technol., vol. 61, no. 6, pp. 2674*–2685, July 2012.

[4] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks,” *IEEE Trans. Wireless Commun., vol. 10, no. 9,* pp. 3064–3073, Sept. 2011.

[5] F. Li, Y. Yang and J. Wu, “ Attack and flee: game theory based analysis on interactions among nodes in Mobile Adhoc networks,” IEEE Trans Syst., Man, Cyber (B) , vol. 40, pp. 612-633, June 2010.

[6] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, “Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks,” *IEEE Trans. Wireless Commun., vol. 8, no. 2,*pp. 806–815, Feb. 2009.

[7] E. A. Panaousis and C. Politis, “A game theoretic approach for securing AODV in emergency mobile ad hoc networks,” in Proc. 2009 IEEE Conf. Local Comput. Netw., vol. 53, pp. 985–992.

[8] J. Omic, A. Orda, and P. Van Mieghem, “Protecting against network infections: a game theoretic perspective,” in Proc. 2009 IEEE INFOCOM, pp. 1485–1493.

[9] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–60, Feb. 2004.