ISSN NO: 9726-001X
Volume 04 Issue4 December2016

JOURNAL OF CURRENT SCIENCE

Using Game Theory to Improve MANET Routing and Security

Dhanaji Bhosale
Research Student, Energy Technology, Shivaji University, Maharashtra, India

Abstract

Using MIMO and CR, data throughput is dramatically increased while simultaneously making optimal use of the available wireless spectrum. The new technologies aim to solve the issue of few radio frequencies. Integrating ad hoc networks, MIMO, and cognitive radios into a decentralized network design is well within reach. The inherent instability of ad hoc networks necessitates the effective improvement of preexisting protocols and security procedures. Using a game-theoretic approach, we present a novel strategy to enhance the safety of MANET routing protocols. The security game between MANETs is modeled in this study using cooperative mean theoretic game theory. The security of the networked environment and the security of each network node are both parts of the larger challenge of protecting a distributed system. A closed-form solution that guarantees precise localization has yet to be discovered, notwithstanding the difficulty of the challenge. MATLAB simulations of the suggested approach are run, and the results are shown.

Terms Like "Game Theory," "TOA," "TDOA," and "MANET"

INTRODUCTION

Due to the increasing prevalence of wireless networks, security in mobile ad hoc networks (MANETs) has emerged as a central topic of study. Over limited bandwidth, mobile nodes in a MANET may self-organize and interact with one another. A wireless mobile node may act as both a router, forwarding packets from other nodes, and a host, sending and receiving data from the network. The mobility of nodes in a MANET creates a topology that is both dynamic and unexpected. In order to establish the routing and scheduling of links in a network, researchers have examined a wide variety of distributed algorithms. However, the decentralized nature of MANETs and the use of a common wireless channel provide novel security design considerations. Denial of service, black hole, resource consumption, location disclosure, wormhole, host impersonation, information exposure, and interference are just some of the security challenges that MANETs face. [2]Concerning the safety of MANETs, several studies have been conducted. Authentication and intrusion detection systems (IDSs) are two examples of preventative measures that may be used to increase a MANET's security [3]. Authentication is a crucial category of IDS-initiated replies. After authentication, only authorized users will be able to access the network, while unauthorized or hacked users would be locked out. Cognitive radio (CR), which can dynamically access the licensed spectrum held by primary users (PUs) by adjusting its transmission or reception parameters, has been proposed as a means for unlicensed secondary users (SUs) to increase the efficiency of spectrum utilization[4].

The study of the security issue in wireless networks may benefit greatly from the use of game theory. The security game model [5] often only includes an attacker and a defender in the current literature on applying game theory to security. While this may be true in a network with centralized management, it is unrealistic in decentralized networks such as MANETs and CR-MANETs. Therefore, in the security game model, each node in MANETs or CR-MANETs should be considered independently. This research can investigate and build a security improved routing protocol in mobile ad hoc networks using a cooperative forwarding game theoretic method, taking into account the trade-off between system security and resource consumption.

I. RELATED WORKS

Cooperative mobile ad hoc network security and quality of service (QoS) co-design, As Yu et al. F Security and quality of service (QoS) co-design for cooperative communications in MANETs was suggested by Richard Yu, Helen Tang, Shengrong Bu, and Du Zheng[6]. The suggested game-theoretic technique allows the system to strategically pick its relay, taking into account system throughput and system security need, by dynamically updating its confidence in the maliciousness of relays based on its record of assaults.

In their paper, "A Novel Game Theoretic Approach for Cluster Head Selection in WSN," Sudakshina Dasgupta and Paramartha Dutta modeled such an approach.

choosing a leader of each WSN cluster [7]. In terms of network lifespan and best-case cluster head selection, this method excels above the state-of-the-art LEACH and HEEDS algorithms. The cluster head selection procedure may be modified in real time by recalculating the payout matrix using the updated game parameters.

Using Non-Zero Non-Cooperative Game Theory to Strengthen Mobile Ad Hoc Network Security, T. Srinivas, M.N. Giri Prasad, B. Prabhakara Reddy, and Dr. This study models the security game between a MANET [8] protected by individual Intrusion Detection Systems (IDSs) and a malevolent coalition made up of a group of nodes working together to commit attacks.

Structured Outcomes for High-Security Mobile Ad-Hoc Networks Integrating Continuous User Authentication and Intrusion Detection [9], User authentication and intrusion detection were provided in a unified fashion by Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, and Helen Tang in their distributed approach. Based on the current security posture and energy states, the proposed approach dynamically selects the most appropriate biosensor (for biometric-based authentication) or IDS.

A message authentication code (MAC) is attached as an extension to the original AODV routing message to guarantee its authenticity and integrity on a hop-by-hop basis [10]. This new algorithm was described by Celia Li, Zhuang Wang, and Cungang Yang in the International Journal of Network Security. Evaluations of security and performance reveal that SEAODV is superior than ARAN and SAODV in terms of computing cost and route acquisition delay, and that it is also superior at blocking detected routing threats.

Multipath Routing with a Game Theoretical Approach [11] for Balancing Safety and Performance. down their study, Siguang Chen and Meng Wu zero down on the challenge of selecting optimal pathways in wireless multihop networks and equitably distributing messages across them. First, using our routing discovery technique, we constructed a set of disjoint multipaths between the source and destination nodes; second, we utilized game theory to choose pathways and optimize the distribution of shares along those paths; third, we added an extra layer of security and fault tolerance by using a secret sharing system.

II. PROPOESD WORK

Game theory has been satisfactorily employed in the design of routing protocols that it is able to account for difficulties in node behavior, energy balance, dynamic route allocation and many others. Game theory can also be applied in the control of ad-hoc network management, random access MAC and other communication architectures. After topologycreation, neighboring node discovery will take place by using Neighbor Discovery Protocol. Ad hoc on demand distance vector protocol will be used for routing. Cooperative forwarding game theory will be implemented in AODV whichis deployed for routing for on demand.

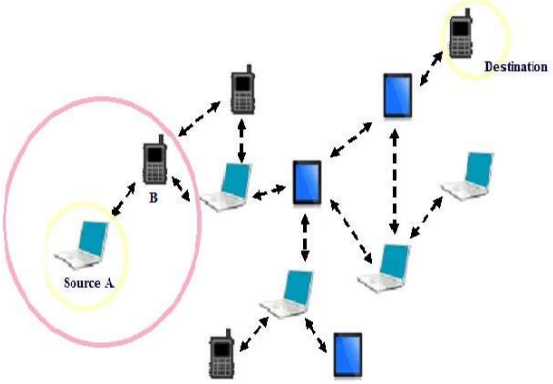


Fig 1. Adhoc Network

Nodes will regularly broadcast HELLO messages as part of the connection monitoring process in the Ad hoc on demand distance vector protocol. Not receiving a HELLO message from a node is seen as a dead connection, therefore if node A in Fig. 1 gets a HELLO message from node B, it will learn that node B is within its wireless transmission range and may be located as its neighbor. To facilitate the exchange of HELLO messages between nodes in an Ad hoc on demand distance vector network, a neighbor discovery protocol (NDP) is being developed. A symmetric connection is assumed by the neighbor finding technique. The header of the HELLO messages is decoded to provide the source ID of the sender. Each node creates a list of its neighbors with timestamps. At regular intervals, the list of nearby neighbors will be refreshed and old names eliminated. The total number of a node's neighbors is the sum of its most recent neighbor list entries. Cooperative forwarding Game Theory requires changes to the Ad hoc on demand distance vector protocol's route discovery procedure and the format of RREQ packets. The number of the source node's neighbors is included in the RREQ (route request) as an additional field. A source node will provide its ID and the total number of its neighbors, N, in the RREQ packet it sends out. This also has to be completed at the nodes in between. The ID and number of neighbors of the intermediary node are placed into the appropriate RREQ packet fields before the packet is transmitted. Other nodes will learn the number of the RREQ's forwarder's neighbors, N, after they get the RREQ. The probability of forwarding for a given RREQ may be calculated by the RREQ's receiver using N in Equation. The forwarding choice is then made by comparing the forwarding probability to a uniformly random value.

For more accurate node location estimation, the cooperative forwarding Game theory additionally takes into consideration the Time of Arrival (TOA) and Time Difference of Arrival (TODA). A second RREQ is sent out by the sending node if it does not receive an RREP from the receiving node. Each iteration, the forwarding capacity of nodes that did not convey the RREQ in the previous iteration grows by 20%. It will ensure that the RREQ gets where it needs to go. The results of the suggested method will demonstrate that using cooperative forwarding game theory in an Ad hoc wireless network is useful in minimizing the overall network's power consumption. The sensors are able to preserve energy without sacrificing throughput thanks to a decision-making algorithm that determines when to deliver packets. The proposed plan will include trying out new methods of reducing power consumption and refining our method of identifying rogue nodes.

III. RESULTS AND DISCUSSION

*A. AODV Protocol and Game Theory*clarity and solutions on fixed or stable network topology andeach node has full knowledge of the available spectrum.

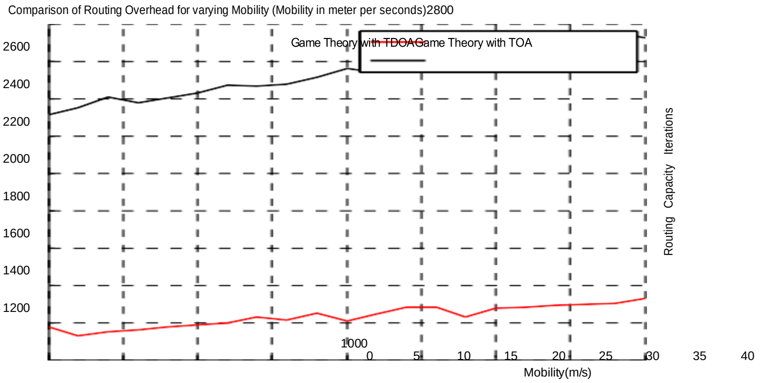
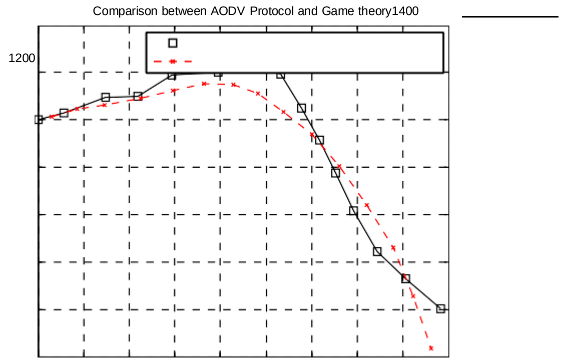


Fig.3 routing overhead for varying mobility

.

C. Compromising Probabilty with nodes



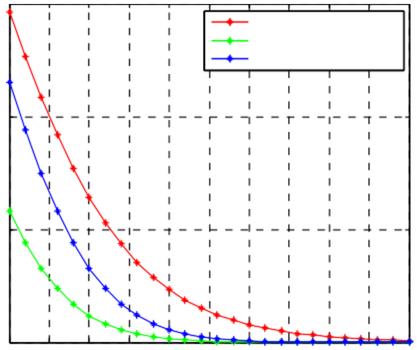


Fig 2. Comparison between AODV protocol and Game theory

The mobility of MANET with high data rate is plotted in the Fig 2. The reduction in TDOA and TOA gives high mobility ratio.

B. Routing overhead with game theory

The less TOA and TDOA provide the high routing data capacity which is shown in the Fig 3. The compared the output with routing capacity iterations and mobility gives theFig 4: compromising probabilities with numbers of nodes.

In some situations, the nodes in the MANET may be supplied with sufficient energy (e.g., vehicular ad hoc networks). So weonly consider the security value loss as the criterion to determine the lifetime. The result in Fig.4 indicate security- prioritized strategy can bring longer lifetime and lower compromising probability than the energy-prioritized strategyin this situation, our optimal strategy can provide the best performance for the MANET among these three strategies.

IV. CONCLUSION

To describe the interactions between a malicious node and a large number of legal MANET nodes, we suggested a unique cooperative forwarding game theoretic technique for security in MANETs. Unlike previous research on security game modeling, the proposed technique allows each node in MANETs to independently decide how to defend the network from known threats. In order to calculate the TDOA and TOA, game theory methods were constructed. Our study revealed that while comparing different methods, there were substantial variations in the acquired precession and availability of the location estimations. The effectiveness of the algorithms varies with the layout of the network and the location of the intended node. The suggested approach takes into account both the security need and the system resources, which is important since security defensive mechanisms use up scarce system resources. Each node in a MANET or CR-MANET simply has to be aware of its own state and the collective influence of the other nodes in order to participate in the proposed scheme. This means the suggested approach is really decentralized. The efficiency of the suggested method is shown via simulation results.

V. References

[1] Security in Mobile Ad Hoc Networks: A Game-Theoretic Approach, by S.K. Mahendran[1]. Volume 1 Issue 5 (June 2014) of the International Journal of Innovation and Research in Advanced Engineering (IJIRAE). Online ISSN: 2349-2163 http://ijirae.com

[2] Protection Augmentation in Mobile Ad Hoc Networks with the Help of Game Theory, by Saravanan T. and Mr.P.Rajkumar. Volume 8, Issue 3, Version I (March 2015), Pages 16–27 IOSR Journal of Applied Chemistry (IOSR-JAC), e-ISSN: 2278–5736

[3] Authentication and Intrusion Detection System for Mobile Ad-Hoc Networks, R.Divya and N.Saravanan [3]. The Second Volume of the International Journal of Innovation in Computer and Communication Engineering

[4] March 2014's Special Number One Issue

[5] In 2012, researchers Sha Hua, Hang Liu, Mingquan Wu, and Shivendra S. Panwar published "Exploiting MIMO Antennas in Cooperative Cognitive Radio Networks" in the proceedings of the conference infocom.

[6] "Combined authentication and quality of service in cooperative communication networks," by R. Ramamoorthy, F. R. Yu, H. Tang, and P. C. Mason, was published in the proceedings of the 2010 conference on embedded and ubiquitous computing held in Hong Kong, China.

[7] [6] F Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks, Richard Yu1*, Helen Tang2, Shengrong Bu1, and Du Zheng. 2013:2013:188 EURASIP Journal on Wireless Communications and Networking

[8] The following is an excerpt from "A Novel Game Theoretic Approach for Cluster Head Selection in WSN" by Sudakshina Dasgupta and Paramartha Dutta, published in the International Journal of Innovative Technology and Exploring Engineering (IJITEE) in February 2013.

[9] According to [8] "Security Enhancement in Mobile Adhoc Network using Non-Zero Non-Co operative Game Theory," published in the International Journal of Research in Computer and Communication Technology, Volume 2, Issue 8, August -2013, by B. Prabhakara Reddy, Dr. M.N. Giri Prasad, and T. Srinivas.

[10] IEEE Transactions on Wireless Communications, Volume 10 Issue 9 September 2011 Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, and Helen Tang "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks"

[11] "Secure Routing for Wireless Mesh Networks," by Celia Li, Zhuang Wang, and Cungang Yang, appeared in the September 2011 issue of the International Journal of Network Security (Vol.13, No.2).

[12] Game theoretic approach in multipath routing for tradeoff between routing security and performance [11], Siguang Chen & Meng Wu. Computer Supported Cooperative Work in Design: Proceedings of the 14th International Conference, 2010. ©2010 IEEE.