International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-2, May 2015
ISSN: 2395-3470
www.ijseas.com

Improvising Routing and Security in MANET with Game Theory

Jeevanantham S
M.Tech., Wireless Communication Systems
Department of ECE, PMU-Vallam
Thanjavur - INDIA

Dr. SPK.Babu
Associate Professor,
Department of ECE, PMU-Vallam
Thanjavur- INDIA

***Abstract*—Data throughput is spectacularly increasing by using MIMO and CR utilizes the existing wireless spectrum opportunistically. The emerging technologies tackle the problem of limited available spectrum. Combination of ad hoc networks with MIMO and cognitive radios greatly ready to merge with the networking and communication technology of decentralized architecture. Adhoc in nature the networks meets many vulnerable security attacks and need existing protocols and security mechanisms must be enhanced through efficient manner. We propose unique scheme to enhance the security for MANET routing protocol under game theoretic approach. In this paper we have to use cooperative mean theoretic game theory is used model the security game between MANET. The overall problem of securing a distributed system comprises the security of the networked environment, and the security of each individual network node. This is a challenging problem and closed-form solution with good localization accuracy has yet to be found. The proposed methodology simulated in MATLAB and the respective results are plotted.**

Keywords—MANET; Adhoc; AODV;Game thoery;TOA;TDOA

I. INTRODUCTION

As ubiquitous wireless networking, security has become one of the key issues in the research field of mobile ad hoc networks (MANETs). In a MANET, mobile nodes can autonomously organize and communicate with each other over bandwidth-constrained wireless links. A wireless mobile node can function both as a network router to route packets from the other nodes and as a network host for transmitting and receiving data. Node mobility makes the MANET topology as dynamic and unpredictable one. Many distributed algorithms have been studied to determine the networking organization, routing, and link scheduling. On the other hand, the unique characteristics of MANETs present some new challenges to security design due to the lack of any central authority and shared wireless medium [1]. There are various security threats that exist in MANETs, such as denial of service, black hole, resource consumption, location disclosure, wormhole, host impersonation, information disclosure, and interference [2]

A number of research have been undergoing about security issues in MANETs. Basically, there are two complementary classes of approaches to secure a MANET: prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection systems (IDSs) [3]. Authentication is an important type of responses initiated by IDS. After an authentication process, only authenticated users can continue using the network resources and compromised users will be excluded. Cognitive radio (CR), with the capability to flexibly adapt its transmission or reception parameters, has been proposed as the means for unlicensed secondary users (SUs) to dynamically access the licensed spectrum held by primary users (PUs) in order to increase the efficiency of spectrum utilization[4].

Game theory can provide a powerful tool for the study of the security problem in wireless networks. However, most of the existing works on applying game theories to security only consider two players in the security game model [5] an attacker and a defender. This assumption may be valid for a network with centralized administration but it is not realistic in MANETs or CR-MANETs, where centralized administration is not available. Consequently, each individual node in MANETs or CR-MANETs should be treated separately in the security game model. This paper can analyze and design a cooperative forwarding game theoretic approach for security enhanced routing protocol in mobile ad-hoc networks, which considers the trade-off both on system security and system resource consumption.

II. RELATED WORKS

Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks, Yu et al. F Richard Yu, Helen Tang, Shengrong Bu and Du Zheng proposed game theoretical approach for security and QoS co-design in MANETs with cooperative communications[6]. With the consideration of system throughput and system security requirement, the proposed game theoretical approach enables the system to strategically select its relay by dynamically updating its belief in the maliciousness of relays according to its record of attacks

A Novel Game Theoretic Approach for Cluster Head Selection in WSN, the authors Sudakshina Dasgupta, Paramartha Dutta modeled a Game theoretic approach for

selecting a cluster head for every cluster in a WSN [7]. This approach is better than the existing LEACH and HEEDS algorithms in terms of network lifetime and optimal selection of cluster heads. The game parameters can be dynamically adjusted to calculate the new payoff matrix which in turn will affect the cluster head selection process.

Security Enhancement in Mobile Adhoc Network using Non-Zero Non-Co operative Game Theory, B. Prabhakara Reddy, Dr. M.N. Giri Prasad, T. Srinivas this paper used non-zero non cooperative game theory is used model the security game between MANET [8], which is defended by Intrusion Detection System (IDS) operating at each node and a group of collaborative malicious nodes called malicious coalition

Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks [9], Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, and Helen Tang presented a distributed scheme of combining user authentication and intrusion detection. In the proposed scheme, the most suitable biosensor (for biometric-based authentication) or IDS is dynamically selected based on the current security posture and energy states in different applications.

Secure Routing for Wireless Mesh Networks International Journal of Network Security, Celia Li, Zhuang Wang, and Cungang Yang described a new algorithm and in this message authentication code (MAC) is attached as the extension to the original AODV routing message to guarantee the message's authenticity and integrity in a hop-by-hop fashion [10]. Security analysis and performance evaluation show that SEAODV is more effective in preventing identified routing attacks and outperforms ARAN and SAODV in terms of computation cost and route acquisition latency.

Game Theoretic Approach in Multipath Routing for Tradeoff between Routing Security and Performance [11]. The authors Siguang Chen & Meng Wu focus the problem of how to select best paths and how to allocate the message shares on these paths in wireless multihop networks. Firstly, established the node disjoint multipath between source and destination node by our routing finding algorithm; next, employed game theory to choice paths and optimize shares allocation on paths; finally, the secret sharing scheme is used to further improve fault tolerance and security.

III. 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 topology creation, 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 which is deployed for routing for on demand.

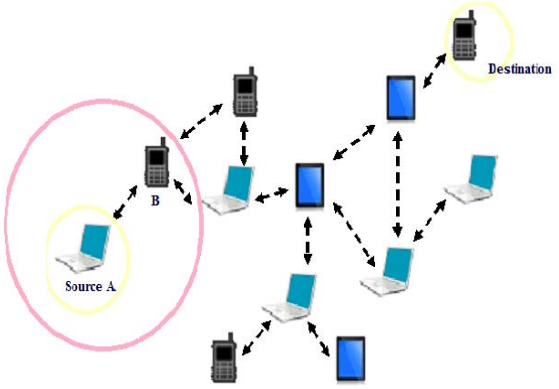

Fig 1. Adhoc Network

In the Ad hoc on demand distance vector protocol, HELLO messages will be periodically broadcasted by nodes and used for link monitoring. In Fig .1 when node A receives a HELLO message from node B, It will discover that node B will be in its wireless transmission range and can be found its neighbor if not getting HELLO message from a node is considered as a broken or dead 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. 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 cooperative 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 be 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 cooperative forwarding Game theory, Time Of Arrival (TOA) and Time Difference Of Arrival (TODA) also taken into account for estimating the position of nodes. If the source node does not receive a RREP from the destination for any reason 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 proposed scheme will show that, under most cases, implementing cooperative forwarding game theory in a Ad hoc wireless network is beneficial by helping reduce the amount of power 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. RESULTS AND DISCUSSION

A. AODV Protocol and Game Theory

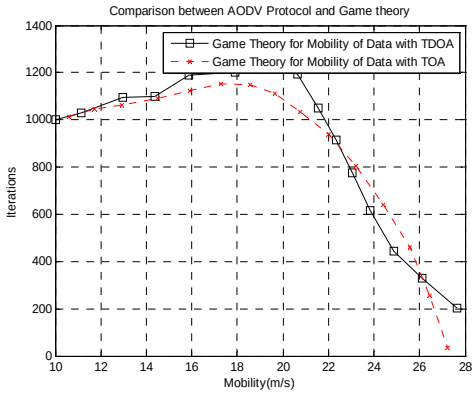

Fig 2. Comparison between AODV protocol and Game theory

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 the clarity and solutions on fixed or stable network topology and each node has full knowledge of the available spectrum.

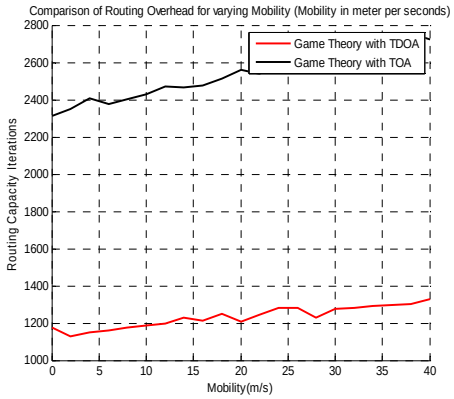

Fig.3 routing overhead for varying mobility

.

C. Compromising Probabilty with nodes

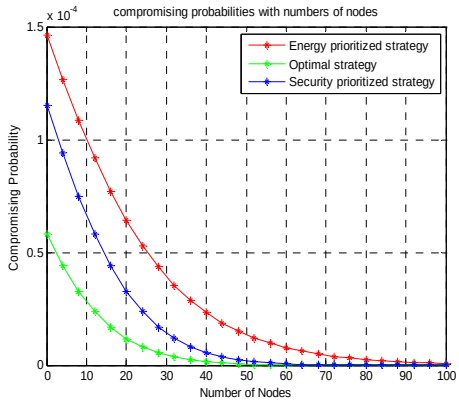

Fig 4: compromising probabilities with numbers of nodes.

In some situations, the nodes in the MANET may be supplied with sufficient energy (e.g., vehicular ad hoc networks). So we only 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 strategy in this situation, our optimal strategy can provide the best performance for the MANET among these three strategies.

V. CONCLUSION

We proposed a novel cooperative forwarding game theoretic approach for security in MANETs to model 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 can enable an individual node in MANETs to make distributed security defense decisions. Game theory algorithms were implemented in order to estimate the TDOA and TOA. Our research showed that there were significant differences in the obtained precession and availability of the location estimates comparing various algorithms. The performance of the algorithms depends on the network topology and the position of the target node. Since security defense mechanisms consume precious system resources, the proposed scheme considers not only the security requirement but also the system resources. Moreover, each node in the proposed scheme only needs to know its own state information and the aggregate effect of the other nodes in MANETs or CR-MANETs. Therefore, the proposed scheme is a fully distributed scheme. Simulation results are presented to illustrate the effectiveness of the proposed scheme.

VI. REFERENCES

[1] S.K. Mahendran "Advanced Security Mechanism for Mobile Ad hoc Networks using Game Theoretic Approach" International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1 Issue 5 (June 2014) ISSN: 2349-2163: online http://ijirae.com

[2] Saravanan T, Mr.P.Rajkumar, "Protection Augmentation in Mobile Ad Hoc Networks Using Game Theory" IOSR Journal of Applied Chemistry (IOSR-JAC), e-ISSN: 2278-5736.Volume 8, Issue 3 Ver. I. (Mar. 2015), PP 16-27

[3] R.Divya, N.Saravanan, "Authentication and Intrusion Detection System for Mobile Ad-Hoc Networks" International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014

[4] Sha Hua , Hang Liu , Mingquan Wu and Shivendra S. Panwar "Exploiting MIMO Antennas in Cooperative Cognitive Radio Networks: infocom, ieee proceedings, 2012

[5] R. Ramamoorthy, F. R. Yu, H. Tang, and P. C. Mason, "Combined authentication and quality of service in cooperative communication networks," in *Proc. Embedded and Ubiquitous Computing (EUC)*, (Hong kong, China), pp. 566–571,Dec 2010.

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

[7] Sudakshina Dasgupta and Paramartha Dutta, "A Novel Game Theoretic Approach for Cluster Head Selection in WSN", International Journal of Innovative Technology and Exploring Engineering (IJITEE), February 2013.

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

[9] 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", IEEE Transactions on wireless communications, vol. 10, no. 9, september 2011

[10] Celia Li, Zhuang Wang, and Cungang Yang, "Secure Routing for Wireless Mesh Networks" International Journal of Network Security, Vol.13, No.2, PP.109–120, Sept. 2011.

[11] Siguang Chen & Meng Wu, "Game Theoretic Approach in Multipath Routing for Tradeoff between Routing Security and Performance". Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design. ©2010 IEEE.