Improving Reliability against Security Attacks by Identifying Reliance Node in MANET

G. Arulkumaran and R. K. Gnanamurthy

***Abstract*—Mobile Ad Hoc Network (MANET) has unstructured infrastructure and form arbitrary topologies. All nodes are capable of movement and can be connected dynamically in arbitrary manner. Although the user want wireless connectivity irrespective of their geographic positions. Mobile Ad hoc Network (MANET) is one among them. Due to the mobility connection these networks reduce its throughput and increases mitigate effect of attacks. Improve reliability by identifying reliance node is one of the intrusion detection technique (IDT). The monitor based intrusion detection technique is only monitoring the packet transmission. The objective of proposed technique is to find the malicious node and select the better route and detect the security attacks. Our main objective is to reduce the total number of lost message and improve the reliability of the MANET transmission.**

***Index Terms*—MANET, throughput, intrusion detection technique, reliability.**

I. Introduction

This MANET has unstructured infrastructure and form arbitrary topologies. These networks have no fixed routers. All nodes in the networks are capable of free movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobility, and the individual nodes are allowed to move freely anywhere in the network. In this type of network, the terminals may not be able to communicate directly with each other and depend on third party message is required to reach its destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks (See Fig. 1).

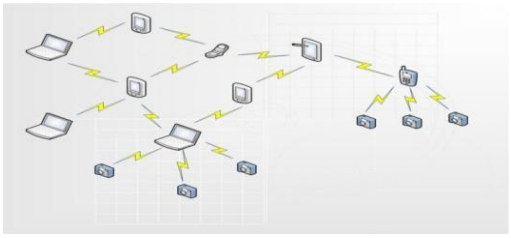

Fig. 1. Mobile Ad hoc network.

The Characteristics of MANETs are Dynamic Topologies, Bandwidth constrains, limited physical security [1]. Dynamic topologies means the nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times [2]. The links may be unidirectional or bidirectional. Bandwidth constrains means wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput. Limited physical security means mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats [3]. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.

A. Routing Protocols

Routing is the act of moving information from a source to destination. Basically routing involves two activities First, Determining the optimal routing path to reach the data from a source to destination, Second, Transferring the information as a group also called as a packets from source to destination[4]. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another. Routing tables are filled with a variety of information like number of hops, source and destination hop address, routing MAC address which is generated by the routing algorithms. Static and dynamic routing are the two types of routing, in static routing the administrator has to give the values manually whereas in dynamic routing the router itself announce their routes.

The various types of routing protocols are given below (see Fig. 2):

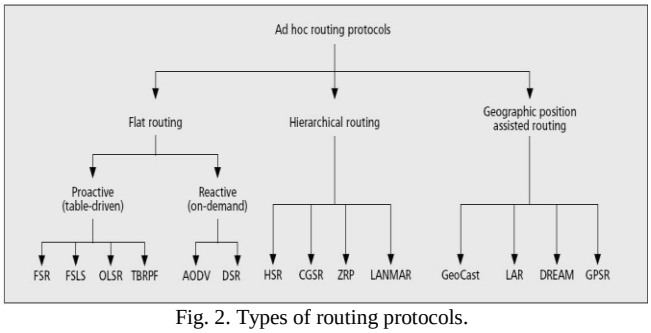

Fig. 2. Types of routing protocols.

In proactive (Table – Driven) routing protocols each and every node in the network maintains routing information to every other node in the network [5]. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Depend on the

Manuscript received September 13, 2013; revised December 11, 2013.

G. Arulkumaran is with Department of IT, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India (e-mail: erarulkumaran@gmail.com).

R. K. Gnanamurthy is with SKP Engineering College, Tiruvannamalai, Tamilnadu, India (e-mail: rkgnanam@yahoo.co.in).

routing information there exist some differences between the protocols. Each routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth. In reactive (On Demand) routing protocols they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. In hierarchical routing protocol is the combination of both proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attribution for respective levels. The main drawback of this routing protocols are, it depend on meshing parameters and nesting addressing scheme. The examples of hierarchical routing algorithms are CBRP(Cluster Based Routing Protocol) and FSR (Fisheye State Routing protocol). The process of geographic routing is the source node sends a packet to the geographic location of the destination node instead of using the network address. Geographic routing defines that each node can determine its own location and that the source node is aware of the location of the destination node. With this information a message can be routed to the destination without knowledge of the network topology or a prior route discovery. The various approaches used in geographic routings protocols are single path, multi path, and flooding.

B. Security Attacks in MANET

There are two ways of attack in MANET one is External attack means the attackers aims to cause congestion, fake routing information, disturb nodes from providing services, second one is internal attack means the attack adversary wants to gain normal access to the network and participate in network activities[5]. The security attacks in MANET classified in two broad categories first is passive attacks and second one is active attacks [6]. Passive attack means the attackers do not disturb the normal operation of the network, instead the attackers sneak the data in the network without alter it. Detection of passive attack is difficult because it will not affect the network operation [7]. The two types of passive attacks are eavesdropping and Traffic Analysis & Monitoring. Active attacks disrupt the normal operation of the network by alter or destroy the data to be communicated [8]. It involves the action like as fabrication, modification, impersonation and replication. The active attacks are carried out in OSI Layers, In MAC Layer Attacks the attack called jamming attack. In network layer the attacks are named as Wormhole attack, Black hole attack, Resource consumption attack, State Pollution attack, Byzantine attack, Fabrication, IP Spoofing attack, Modification, Routing Attacks and Sybil attack,. Again the routing attacks are classified as Routing Table Overflow, Routing Table Poisoning, Packet Replication, Route Cache Poisoning and Rushing Attack [9]. In transport layer attacks are named as flooding attack and Session Hi jacking attack. In application layer there is only one attack named as repudiation attack [10]. Apart from this there are some of other active attacks also possible named as Denial of Service attack, flooding attack, Spoofing attack, Jellyfish attack, location disclosure attack, Device tampering attack, Gray hole attack, Colluding misrelay attack, Packet dropping attacks and Sleep deprivation torture [11].

II. Improving Reliability and Identifying Reliance Node

This process carried out the following phases.

A. Intrusion in MANET Communication

Mobile Ad hoc Network (MANET) means every single node can make establish the connection and communicate with other nodes. The radio waves only the carries the signal between the mobile nodes. Due to a lack of infrastructure support, each node acts as a router and forwarding data packets for other nodes. Intrusion detection systems detect and mitigate an attack after detected. Assume three nodes in a route namely A, B, C. When node A want to communicate to node C via node B, so node A sends data packet to node B and expects to know the transmission packets of node B within allocated time. If fraction of packets not overheard by node A exceeds certain threshold, then node A concludes, node B is dropping too many data packets, suspects it as a malicious node.

B. Monitor Based Intrusion Detection

The MANET characteristics there are varying in signal propagation and noise. To overcome this any one node is act as a monitor node. If any node found as malicious node then this intrusion detection technique fix reliance value before considering as node. Simulation carries no noise and signal propagation in monitor based technique but this technique unable to identify false positive quantification of effective monitoring. Every node acts as a monitoring node and verifies the behavior of its neighboring node before forwarding data packets. The node allowed monitoring only its next hop within the route. The recently send packets are tracked by both sliding window and fixed window.

C. Significant Evaluation Technique

The best way to evaluate the intrusion detection technique is watchdog and path rater. The watchdog used to monitor any malicious node and path rater used to identify a better path to traverse the packets from source to destination. When there is a malicious node in the specified path every node forward packets to its next hop. If the next hop node is a susceptible node then it sends ALARM message to source node. By using both fixed and sliding window the source node assign rating of source value to susceptible nodes. If the rating value is negative value then the source discover new route to reach its destination else if the rating value is positive value and having multiple path to the same destination, the source node chooses the highest rated path.

D. Node Identifier against Collusion Attack

To improve the reliability of data transmission in MANET

these monitoring technique detect collusion and malicious node. These nodes are classified as New, Normal, Prioritized, Suspect, Instable and Banned. According to the reliance node rating value each node carry out its transmission. Each node to allow comparing the transmitted data with source node data before forwarding the packets to other node. Separate list to be maintained by each node individually for the banned nodes. The suspected nodes are temporary inaccessible from network, and some periodic of time these nodes are unable to send and receive any message.

E. Reliance Node Valuation

Intrusion detection system select most reliable path by gathering the next node information based on quality and quantity. Initially the nodes are not allowed to migrate to other state. All gathered information are validated and ensure with direct observation. The reliance node only allowed choosing the transmission route. When the rating value is less than minimum threshold then it indicate the message from unreliable source and discard it. When the rating value is above threshold value then prevent against the attack by sending ALARM message to the source node.

III. Experimental Setup and Result Scrutiny

In this section by using NS2 simulation the performance of reliance node is evaluated. The main objective of this evaluation is to improve the reliability against security attacks by identifying reliance node. We consider the following factors to evaluate the reliance node and improve the reliability of the MANET operation, Throughput Gain defined as average successful packet delivery over a communication channel. Throughput can be measured either in Bits per Second (BPS), Data Packets per Second and Data Packets per Timeslot. Route reliability explains to select the best path when there are two (or) more different routes to the same destination from two different routing protocols. Each routing protocol is prioritized in order of most to least reliable using an administrative distance value. Collusion attack rate is the agreement between two or more nodes by defrauding others data or gaining an unfair advantages.

TABLE I: Throughput Gain

Number of Nodes	Existing Technique	Proposed Technique
10	4.4	5.5
20	3.8	5.1
30	3.4	4.6
40	2.7	3.9
50	2.6	3.6

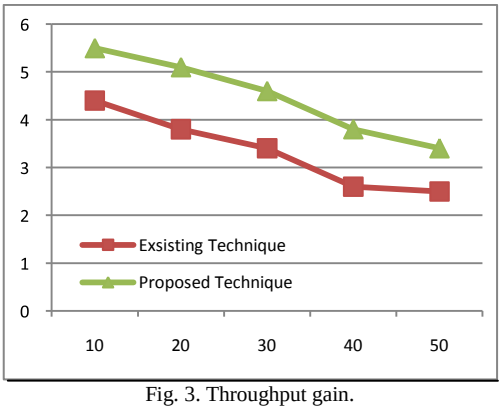

Fig. 3. Throughput gain.

Fig. 3 and Table I explain the throughput gain. In the above Fig. 3 X axis represent the number of nodes and Y axis represents the throughput gain. The existing technique is the Monitor based Intrusion detection and the proposed technique is to improve reliability and reliance node technique. When number of nodes increase then the curve shows throughput gain is steadily descendant. But compare to existing technique the proposed technique achieve 10% to 20% throughput gain.

TABLE II: Route Reliability

Number of Mobility	Existing Technique	Proposed Technique
20	5	7
40	4	6
60	3	5
80	2	4
100	1	3

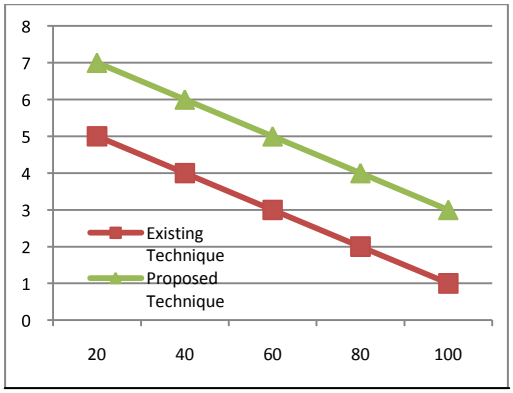

Fig. 4. Route reliability.

Fig. 4 and Table II explain the route reliability. In the above Fig. 4 X axis represent the number of mobility and Y axis represents the route reliability. The existing technique is the Monitor based Intrusion detection and the proposed technique is to improve reliability and reliance node technique. When number of mobility increase then the curve shows route reliability is steadily descendant. Fig. 4 shows improved reliability and compare to existing technique the proposed technique achieve 20% to 30% route reliability.

TABLE III: Collusion Attack Rate

Number of Mobility	Existing Technique	Proposed Technique
10	43	12
20	54	21
30	68	32
40	74	41
50	82	50

Fig. 5 and Table III explain the collusion attack rate. In the above Fig. 5 X axis represent the number of nodes and Y axis represents collusion attack rate. The existing technique is the Monitor based Intrusion detection and the proposed technique is to improve reliability and reliance node technique. When number of nodes increase then the curve shows the collusion attack rate get increased. Fig. 5 shows

less collusion rate attack and compare to existing technique the proposed technique achieve 40% to 50% less collusion attacks.

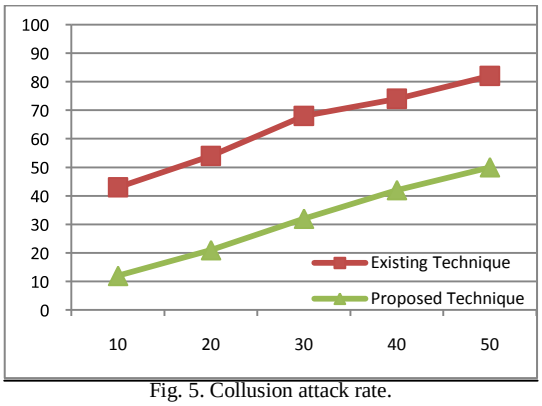

Fig. 5. Collusion attack rate.

IV. Conclusion

In this paper, when compare to existing monitor based intrusion detection technique, the improving reliability against security attacks by identifying the reliance node in MANET, we concluded the throughput gain is high, route reliability is high and collision attack rate is less. If any node is found as malicious node then with the help of reliance node, the source will avoid the transmission of packets through malicious node and identify the alternate path to reach its destination. Hence this technique provides reliable and efficient data transmission.

References

[1] S. Agrawal, S. Jain, and S. Sharma, "A survey of routing attacks and security measures in mobile ad – hoc networks," *Journal of Computing*, vol. 3, issue 1, pp. 41 – 48, Jan. 2011.

[2] P. M. Jawandhiya and M. M. Ghonge, "A survey of mobile ad – hoc network attacks," *International Journal of Engineering Science and Technology*, vol. 2, no. 9, 2010.

[3] H. Yang, J. Shu, and X. Meng, "SCAN: self – organized network layer security in mobile ad – hoc netowrks," *IEEE Journal on Selected Areas in Communication*, vol. 24, issue 2, pp. 261 – 273, Feb. 2006.

[4] G. S. Sharvani, N. K. Cauvery, and T. Rangaswamy, "Adaptive routing algorithm for MANET: TERMITE," *International Journal of Next – Generation Networks*, vol. 1, issue 1, Dec. 2009.

[5] M. Ghonge and S. U. Nimbhorkr, "Simulation of AODV under black hole attack in MANET," *International Journal of Advance Research in Computer Science and Software Engineering*, vol. 2, issue 2, Feb. 2012.

[6] L. Tamilselvan and V. Sankaranarayanan, "Prevention of black hole attack in MANET," *Journal of Network*, vol. 3, issue 5, May 2008.

[7] L. P. Rajeswari, R. A. X. Annie, and A. Kannan, "Enhanced intrusion detection techniques for mobile ad – hoc networks," in *Proc. IET – UK International Conference on Information and Communication Technology in Electrical Science*, Dec 20 – 22, 2007, pp. 1008 – 1101.

[8] A.Vani and S. D. Rao, "Removal of black hole attack in ad – hoc networks to provide confidentiality security service," *International Journal of Engineering Science and Technology*, vol. 3, issue 3, Mar. 2012.

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgement based approach for the detection of routing misbehaviour in MANETs," *IEEE Transaction on Mobile Computing*, vol. 6, no. 5, pp. 488 – 502, May 2007.

[10] H. Lee, A. Cerpa, and P. Levis, "Improving wireless simulation through noise modeling," in *Proc. 6th International Symposium on Information Processing in Sensor Networks*, Apr, 2007, pp 21 – 30.

[11] A. Clementi, F. Pasquale, and R. Silvestri, "Opportunistic MANETs: mobility can make up for low transmission power," *IEEE / ACM Transactions on Networking*, vol. 21, no. 2, April 2013.

G. Arulkumaran has completed his bachelor of engineering in the field of computer science and engineering from Arunai Engineering College of Madras University. He also had finished his master of engineering in the field of computer science and engineering from Anna University of Technology, Trichy. He is pursuing his Ph. D in the field of information and communication engineering in Anna University, Chennai.

He has more than 7 years experience in the field of teaching. Currently he is working as an assistant professor in the Department of Information Technology, Vivekanandha College of Engineering for Women, Tiruchengode, Tamil nadu, India.

R. K. Gnanamurthy has completed his bachelor of engineering in the field of electronics and communication engineering from Bharathiar University, Coimbatore. He also had finished his master of engineering in the field of microwave and optical engineering from Madurai Kamaraj University, Madurai. Received his Ph. D in the field of information and communication engineering from Anna University, Chennai.

He has more than 25 years experience in the field of Teaching; He worked in several institutions in the various designations like senior lecturer, assistant professor, professor and head of the department and principal. Now He is working as a principal of SKP Engineering College, Tiruvannamalai, Tamil nadu, India.

He is a life member of Indian Society for Technical Education and Computer Society of India Member of IIIE, India. And he also is a students member of Institute of Electrical and Electronics (IEEE) (USA). He is the chairman and member of board of studies in various universities. His Area of specialization is wireless sensor networks and mobile computing. He guided 27 PG students and under his guide ship more than 13 students are doing their research.