ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Maximizing Throughput by Isolating Malicious Node in Ad hoc Networks

K.Muthu Gowri [1], A.Kumaravel [2] and R.Kavitha [3]

P.G. Student, Department of ECE, Paavai Engineering College, Pachal, Namakkal, India[1, 3]

Assistant Professor, Department of ECE, Paavai Engineering College, Pachal, Namakkal, India[2]

ABSTRACT: Manets are extensively used these days for communication and there are various communication networks with different standards and computing techniques and as days are passing by the size of manet is increasing day by day and its expansion is unavoidable due to its high penetration and popularity for the usage of mobile application but at the same time it is also prone to many attacks and network failure due to technical vulnerability of the network. Hence security in MANET is a major issue in ad-hoc network. The security framework involves: Detection of malicious node by the destination node, isolating the malicious node by discarding the path and prevention of data packets. In this paper, we proposed a methodology to isolate the malicious nodes that are responsible for packet dropping attack by using MNI-AODV protocol. Due to the isolation of malicious nodes throughput increases.

KEYWORDS: Security, Malicious nodes, MANETS, packet dropping attack, MNI-AODV, and Throughput.

I. INTRODUCTION

A network is a group of nodes connected with each other and node is a device or a mobile terminal connected to the network. An ad hoc network, one of the types of wireless network is a collection of two or more devices equipped with wireless communications and networking capability and MANET has many applications among that two of them are crisis management and military operations.

A mobile ad hoc network (MANET), one of the types of ad hoc network is a collection of mobile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET, each nodes act not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range in the network. Each device in a mobile ad hoc network (MANET) is free to move independently in any direction within the network, and it can also change its links to other devices frequently.

MANETs are much more vulnerable and are susceptible to various kinds of security attacks because of its cooperating environment compared to wired network. In the absence of a fixed infrastructure that establishes a line of defense by identifying and isolating malign nodes, it is possible that the control messages generated by the routing protocols are corrupted or compromised thus affecting the performance of the MANET. Different routing protocols are then evaluated based on measures such as the packet drop rate between nodes, the control overhead introduced by the routing protocol, end-to-end delay and network throughput. The mobile ad hoc network has the following typical features,

- Unreliability in wireless communication links between nodes in the ad hoc network
- Constantly changing topology

The security framework involves: Detection of malicious node by the destination node, isolating the malicious node by discarding the malicious path and prevention of data packets from that malicious node. In this paper, we proposed a MNI-AODV technique to detect and isolate the malicious node in mobile ad hoc environment. Detecting malicious node is the initial process towards protecting the ad hoc network and isolation of these detected nodes is done for smooth and reliable communication between nodes. Isolation means removing the capabilities of nodes which is used in communication process.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Paper is organized as follows. Section II describes AODV reactive routing protocol overview. Related work is shown in Section III then the proposed method consists of flow diagram which represents the step of the algorithm and the detection of malicious node in the network. After the detection, the malicious nodes are isolated by using MNI-AODV protocol that is described in Section III and Section IV presents comparison graph with experimental results showing results of isolation of malicious node and increase in throughput and packet delivery ratio (PDF). Finally, Section V presents conclusion.

II. AODV OVERVIEW

The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. A disadvantage is a possible large delay from the moment the route is needed (a packet is ready to be sent) until the time the route is actually acquired.

The procedure to establish the route in AODV protocol is as follows. Assuming that node S intends to send data to node D but S does not have information to D. Thus, to establish the connection, node S initiates a route discovery process by broadcasting a RREQ packet to the network. The RREQ packet carries a sequence number which will indicate the "freshness" of route information so that intermediate nodes can evaluate the information and reply to the requests with up-to-date route information.

When an intermediate node receives the RREQ packet, and the packet has higher sequence number, the node will update its routing table with new route entry to establish a reverse path, which will be used by route reply. If the information about node D is not available, the node will rebroadcast the request until the RREQ is received either by node D or by an intermediate node that has recently established route to node D otherwise route reply RREP packet will be generated.

The RREP packet also has a sequence number to maintain the up-to-date routing information. After node D receives the RREQ from its neighbours, if the update condition is made, node D updates its routing table with neighbour node address (i.e. next hop node) which is the entry node for node S. Node D generates RREP packet and sends the packet to node S via next hop node in the reverse direction. If the next hop node is not the source node D, the RREP packet is forwarded using reverse path until node S is reached.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches. The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination. The connection setup delay is lower. One disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.

III. RELATED WORK

Enhanced OLSR (Optimized Link State Routing) protocol which is a trust based technique [1] is used to secure OLSR nodes against the node isolation attack which is a specific type of denial-of – service attack. This technique is capable of finding whether a node is advertising correct topology information or not by verifying its HELLO packets [1], thus node isolation attack is detected and this technique is light weight because it doesn't involve high computational complexity for securing the network.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

For the protection [2] of both routing and data forwarding operations, a network layer security solution provided a solution for various security attacks in ad hoc networks. The security framework involves the detection of malicious node by distracting the path and prevention of data packets by using dispersion techniques. Thus Multipath Reliable Routing (MPR) algorithm [2] is proposed to determine the set of node-disjoint reliable paths. The paths are arranged in the descending order of their reliability index.

The reliable path sends the information packet containing the transmission information. If there is any mismatch between the transmission information and the data packets received, a negative feedback is sent back to the source that includes the affected paths. These affected paths are then removed from the list of node-disjoint paths by the source [2]. The destination recovers the data packets using an efficient dispersion algorithm.

The overhead of route discovery in MANET cannot be neglected due to high mobility of nodes which leads to frequent path failures. Thus NCPR (Neighbour Coverage-based Probabilistic Rebroadcast protocol) is used to reduce routing overhead based on neighbour coverage knowledge and rebroadcast probability but there may be a chance of node selfishness which leads to data loss and also reduce packet delivery ratio. To overcome this problem GNDA is used. GNDA [5] (Good Neighbour node Detection Algorithm) identifies the good neighbour nodes based on signal strength and flow capacity thus decreases end –to-end delay and improves good communication, stable route and provides good performance even when the network is in high density.

In MANET, AODV [6] (Ad hoc On-Demand Distance Vector) floods the control packets to discover the route. Generally there is limit in generating and forwarding these packets. Malicious node can disregard this limit and flood the network with fake control packets so that these packets have the limited bandwidth and processing power of genuine nodes in the network while being forwarded. Due to this, genuine nodes suffer and many routes do not get chance. To overcome this problem AODV reactive routing protocol is used in presence of malicious attack under different load.

A trust based Security protocol [7] based on a MAC-layer approach is proposed to attain confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, a trust based packet forwarding scheme is designed for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to forward packets by using trust counter for each node. If trust counter value falls below a trust threshold, then the corresponding node is marked as malicious node. In the next phase [7], link-layer security is provided using CBC-X mode of authentication and encryption that achieves high packet delivery ratio with low delay and high speed and overhead.

Routing protocol [8] calculates the channel non-fading duration for routing which attempts to minimize packet loss due to fading and also reuse the path with some security mechanism to increase the throughput. CA-AOMDV (Channel Aware - Ad hoc On-demand Multipath Distance Vector) is used for channel average non-fading duration as the routing metric. The LBCA-AOMDV [8] (Load Based Channel Aware – Ad hoc On-Demand Multipath Distance Vector) is used for increasing throughput and packet delivery ratio.The genuine node gets isolated from the network due to DOS attack [3] thus a detection mechanism is developed to overcome such scenarios.

The mechanism is divides into 2 parts. The first part is normal flow and other part is attack mode flow. In the normal flow, channel state and time slot is checked. If the channel is free and key matches then continue with communication. In the attack mode flow [3], the illegitimate nodes are identified and it is isolated from the network. Due to this packet delivery ratio and throughput is increased.

IV. PROPOSED METHOD

In packet dropping attack [4], malicious node intentionally drop the data or control packets. For performing routing misbehaviour, a malicious node can intentionally send unnecessary route error message to misguide its neighbour and for also increasing the percentage of congestion in the network. Also, these nodes may reserve resources for their own benefits and can flood the network with query packets and force other nodes to give reply or acknowledgement.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Broadcasting of HELLO messages by source node A is shown in the Figure.1. The node H is the malicious node and it provides miscommunication between source A and destination D. B, C, E, F and G are intermediate nodes. The acknowledgement of path to D by nodes C, B, F, E and D is shown in Figure. 2.

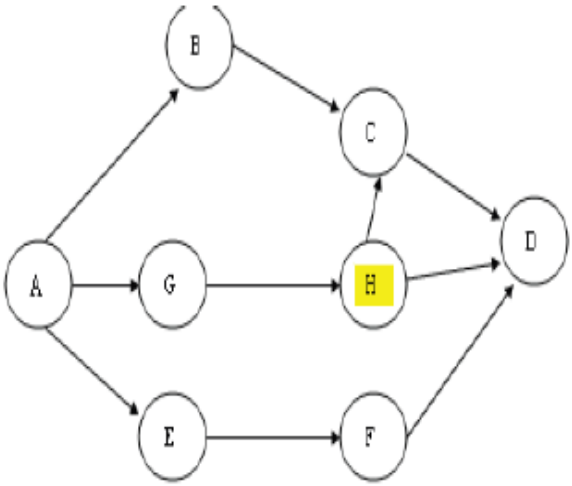


Figure.1: Broadcasting of HELLO message by source node A

If malicious node H declares that it is having greatest destination sequence number than the destination node then other nodes assumes H as a destination node and can divert the traffic towards H. Hence there may be high packet dropping ratio. Format of regular node structure and suspicious node structure is shown in the Figure 3.

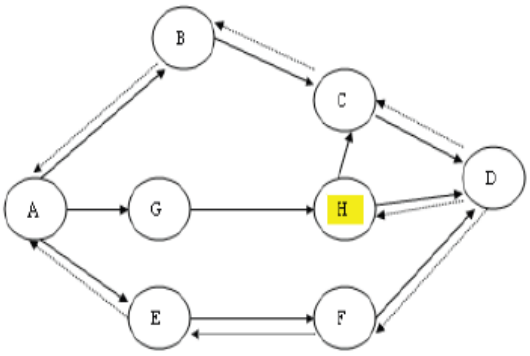


Figure 2: Acknowledgement of path to D by nodes C, B, F, E and D

Profile field consist of 8 sub fields they are Node ID, Action, Confidence evaluated by neighbour, Resource Consumed, Period, Node Type, Threshold and Others. The malicious node is detected and it is isolated from the network by deleting a path in which the malicious node is present. Each intermediate node that wants to remove a link will broadcast this information to all its neighbours. In the same way other nodes will also decided to delete its link from the malicious node. Otherwise, it is not possible or easy to delete the existing path or link among the nodes. If this link remains exist then performance of network may down anytime. Thus source node deletes the malicious node to improve the performance of the network.

Node ID	Node Address	Node Seq. No	Node Type

Figure 3: Format of regular node structure

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Node ID	Node Type	Timestamp	Profile

Figure 4: Malicious node structure

Process flow of MNI-AODV for malicious node isolation is represented in Figure 5. Authentic routes established for secure data transmission and these routes are acknowledged by all neighbor nodes for data transmission. Now source node can choose an optimal path for transmitting data with authentic intermediate nodes and routes.

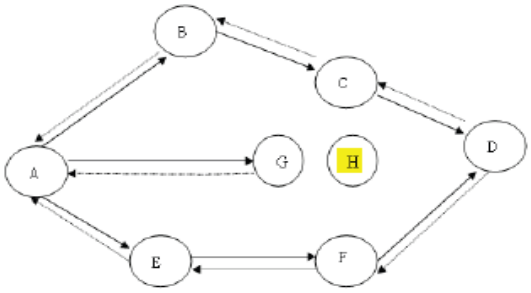


Figure 5: Authentic routes established after malicious node isolation

The flow diagram for malicious node isolation is shown in Figure 6. At first the presence of malicious node H is broadcasted to all the nodes present in the network then all nodes checks the presence of malicious node by calculating one hop and two hop distance. If all nodes recognize the malicious node from the calculation then they identify the path where malicious node exists and they delete that particular malicious path. Thus the malicious node is isolated and it has no link with other nodes n the network. After isolating the malicious node, the source node retransmits the data packets through other genuine path. The isolated malicious node could not be able to take part in the network. For further communication, neighbour node do not include malicious node in routing process and also does not accept request message from malicious node. Thus the malign nodes are isolated from the network graph and rest of network remains connected.

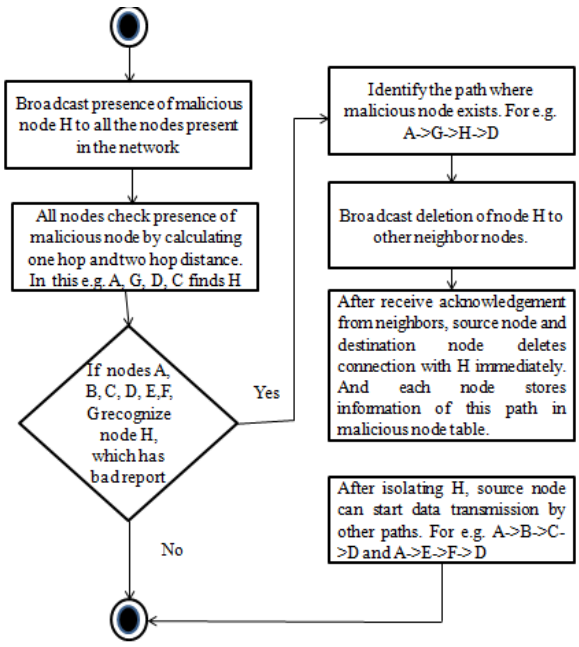


Figure 6: Flowchart for isolation of malicious node using MNI-AODV

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

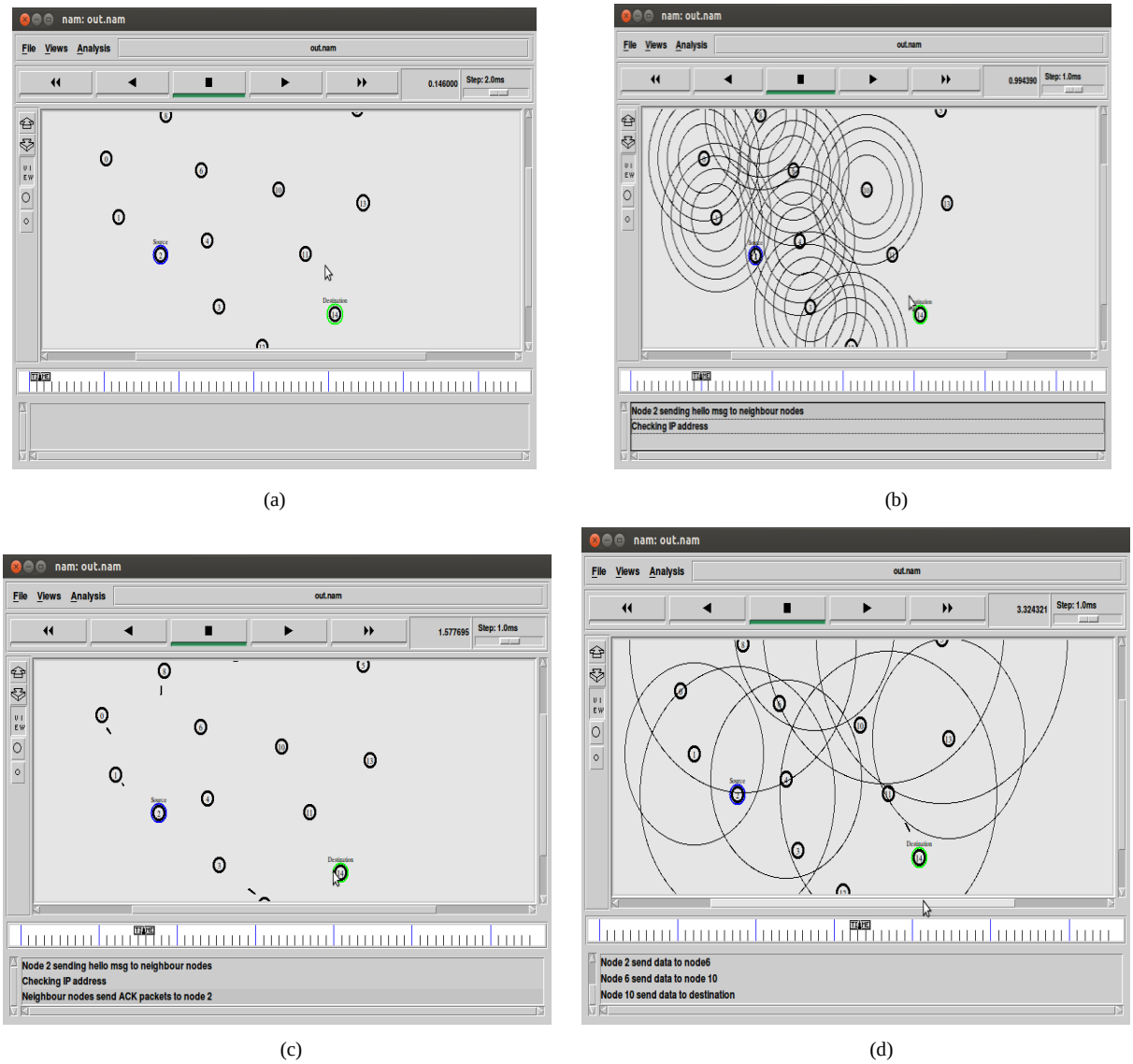
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Hence by isolation of malicious node throughput and packet delivery ratio increases with low end-to-end delay and control overhead.

V. EXPERIMENTAL RESULTS



(a) (b)

(c) (d)

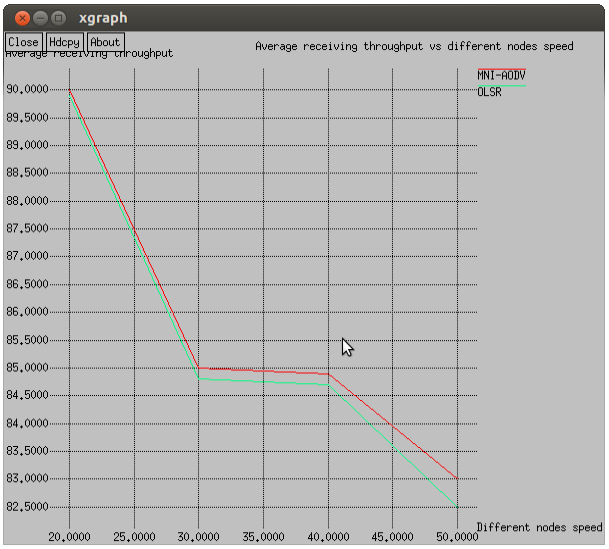
Fig.2. Transfer of data packets between source and destination nodes (a) Source and destination nodes are selected (b) source node 2 sends hello msg to neighbour nodes (c) Neighbour nodes sends acknowledgement packets to source node 2 (d) Data packet sent to destination node

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

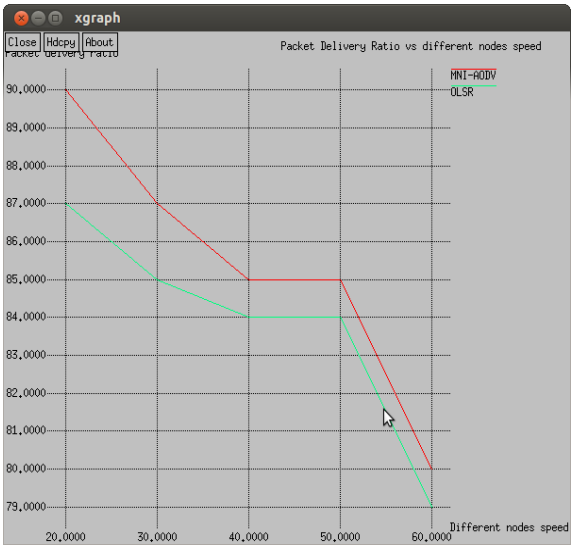
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

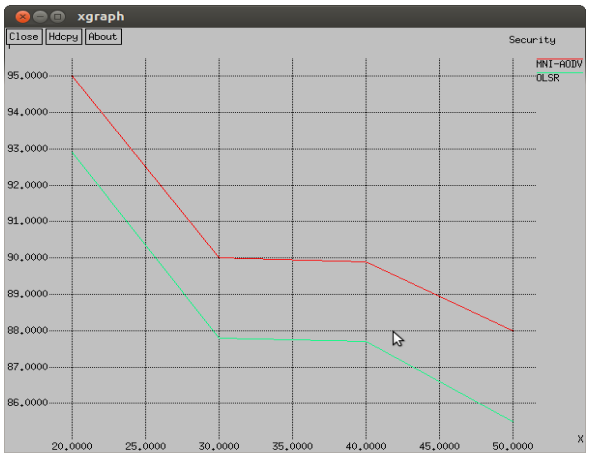
Vol. 4, Special Issue 6, May 2015



(a)



(b)



(c)

Fig. 3 Comparison graph between MNI-AODV protocol and existing EOLSR protocol [1] a) Throughput vs different node speed (b) Packet delivery ratio vs node speed (c) Security using MNI-AODV

Above Figures shows the results of data packet transfer between the source node and destination node by using MNI-AODV protocol. Fig. 2 (a) shows the selection of source and destination nodes (b) and (c) shows the communication between source nodes and neighbour nodes by sending HELLO packet and the necessary acknowledgement. Fig. 3 (a), (b), and (c) show the comparison graph for throughput, packet delivery ratio and security.

VII. CONCLUSION

In this paper, we proposed a solution for packet dropping attack in mobile ad hoc networks based on the detection and isolation of the malicious node using MNI-AODV technique. This technique detects the misbehaviour node in network and broadcast the information about the misbehaviour node detected to all the nodes present in the network. Thus each and every node in the network removes its link with that malicious node hence the malicious node is isolated and it can't take part in the data transmission anymore. Simulation result shows that the proposed method increases the

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

throughput and packet delivery ratio with less control overhead. The simulation also shows that the performance of the network is good even when the network is in high density.

REFERENCES

[1] Mohanapriya, Marimuthu, and Krishnamurthi," Enhanced OLSR for Defense against DOS Attack in Ad hoc Networks," *IEEE Trans. commun.and networks*, vol. 15, No. 1, pp. 31- 37, June 2013

[2] Dhanalakshmi Somasundaram, and Dr. Rajaram Marimuthu," A multipath reliable routing for detection and isolation of malicious node in MANET," *IEEE conference on computing on commun and networking*, vol. 2013, pp. 188–190, 2008.

[3] Pooja, and Er. Deepika Khokhar," Isolation of malicious node in DOS scenario in MANET," *International Journal. Computer. Tech.*, vol 3(4), *ISS7-IS63*, July-August 2012.

[4] Umang, Dr. B. V. R. Reddy, and Dr. M. N. Hoda, " MNI-AODV: Analytical model for attack mitigation using AODV routing in ad hoc networks," *IEEE conference on computing for sustainable Global Development*, pp. 719 –723, 2014.

[5] T. Suganya, R.Abirami, L. Anuprabha, and J. Anupriya, " GNDA: Good neighbour node detection for selfish node identification," *International Journal. computer Science and Information*, vol. 5(2), pp. 1648–1651, 2014.

[6] Priyambada Sahu, Sukant Kishoro Bisoy, and Soumya Sahoo," Detecting and isolating malicious node in AODV routing algorithm," *International Journal of Computer Application, vol. 66, No. 16*, Mar. 2013.

[7] A. Rajaram, and Dr. S. Palaniswami," Malicious node detection system for mobile ad hoc networks," *International Journal of computer science and information Technology, vol.1(2), pp. 77-85*, 2010.

[8] A. Ayyasamy and K. Venkatachalapathy," Increased throughput for load based channel aware routing in MANETs with reusable paths," *International Journal of computer science*, vol. 40, no. 2, pp. 20-23, Feb. 2012.

[9] Aravindh S, Vinoth R S, and Vijayan R,"A trust based approach for detection and isolation of malicious nodes in MANET," *International Journal of Engineering and Technology, vol. 5, No. 1*, Feb-Mar 2013.

[10] Ze LI, and Haiying Shen," A QOS-oriented distributed routing protocol for hybrid wireless networks," *IEEE trans. Mobile computing, vol. 13, No. 3, pp. 693-708*, March 2014.

[11] Zhexiong Wei, Helen Tang, F. Richard Yu, MAoyu Wang, and peter Mason," Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Trans. Vehicular Technology*, pp. 1-12, 2013.

[12] Zaid Ahmad, Jamalul-lail Ab Manan, and Kamarularifin Abd Jalil," Performance evaluation on modified AODV protocols," *IEEE Asia-Pacific conference on Applied Electromagnetics*, pp. 158-163, Dec. 11-13, 2012.

[13] Ahmed M. Abdulla, Imane A. Saroit, Amira Kotb, and Ali H. Afsari," Misbehavior nodes detection and isolation for MANETs OLSR protocol," *World Conference on Information Technology*, 2010.

[14] Dr. Nasib Sinngh Gill, and Ekta, "Detection and isolation of malicious and hostile nodes in MANETs," international Journal of Advanced research in Computer science and software Engineering, vol. 4, Issues 4, pp.853-856, Apr. 2014.

[15] Syed S. Rizvi, and Khaled M. Elleithy, "A New scheme for minimizing malicious behaviour of mobile nodes in mobile ad hoc networks," *International Journal of computer science and Information Security, vol. 3, No. 1, pp. 45-54, 2009.*

[16] Gaurav Sonil, and Kamalesh Chandrawanshi, "A Novel defence scheme against selfish node attack in MANET," *Internationsl Journal on Computational Sciences & Applications (IJCSA), vol. 3, No. 3, pp. 51-63*, June 2013.

[17] S. Manatha, and A. Damodaram, "Enhanced intrusion detection system for malicious node detection in mobile ad hoc networks using data transmission quality of nodes," *I. J. Computer Network and Information Security, vol. 10, pp. 32-39*, 2014.

[18] Reshmi T. R, and Murugan. K, "Application of fuzzy sets for isolating selfish nodes by trust evaluation during auto-configuration and service establishment in MANETs," *Journal of Network and Innovative Computing ISSN, Dynamic Publishers, Inc, USA, vol.1, pp. 65-73*, 2013.

[19] R. Shanthakumari, "Intrusion detection systems for malicious node detection in DYMO protocol," International Journal of Advanced Research in Information and Communication Engineering, vol. 1, Issues 1,pp. 32-38, July 2013.

[20] Chaitas Shah, and Prof. Manoj Patel, "Improving ZPR protocol against blackhole attack," *International Journal of Engineering Development and Research, vol. 2, Issues 2, pp. 1939-1943*, 2014.