Technique for Detection and Isolation of Black Hole Attack in MANETs

Ramneet Kaur
Punjab Technical University,
Sri Sukhmani Institute of Engineering and Technoogy, Derabassi, Punjab

Amandeep Kaur
Sri Sukhmani Institute of Engineering and Technoogy, Derabassi, Punjab,
Punjab Technical University

ABSTRACT
The infrastructure less property in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In AODV route request, route reply and route error are the control messages. When source node wants to establish route to the destination nodes, source node first sends route request control packets to their adjacent nodes. When adjacent node receives route request packets if node has the route to the destination node it will reply back to source node with route reply message. Source node select best route on the basis of hop counts and on the basis of sequence number. The black hole attack is the active type of attack in which malicious node commit that it has path to destination but it does not have path to destination. In this work, technique of blacklist and clustering is proposed which detect and isolate malicious nodes from the network.

Keywords
MANETs, AODV, Black Hole Attack, Security

1. INTRODUCTION
MANET stands for Mobile Ad hoc Network. It is a vigorous infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are arbitrarily linked with each other and forming arbitrary topology. It can act as routers and hosts both. MANET has skill to self-configure makes this technology suitable for provisioning communication. In MANET no infrastructure is required. The routing protocols are those which are responsible for routing data from source to destination [1]. There are various types of routing protocols. In reactive routing protocols the route from the source to destination is established when required. Source flood the network with the route request packets and intermediate nodes which is having path to the destination will reply back with the route reply packets. In Proactive routing protocols, the route between the source and destination is predefined [2]. In the network, each node maintains a routing table. Hybrid routing Protocol is the combination of both proactive and reactive routing protocols. The whole network is divided into zones. The inter Zone routing is done with the use of Proactive routing protocols and Intra Zone routing is done with the use of reactive routing Protocols. ZRP is the Hybrid type of routing Protocols. Mobile ad hoc networks are vulnerable to security attacks. Attack is the mechanism which disrupts the normal behavior of the network [3]. The security attacks are triggered from the internal as well as external nodes.

2. BLACK HOLE ATTACK IN AODV PROTOCOL
AODV is an important on-demand routing protocol that creates routes only when desired by the source node. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination [4]. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred.

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number [5]. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination [6]. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

3. LITERATURE REVIEW
M. Jhansi et.al [2012], proposed [7] a new method of detecting cooperative black hole attack in MANET. This method uses extra bits of information to store the information regarding the number of packets received by a node and the number of packets further transferred by it. The DRI entry is checked by source node and data is routed depending on a positive match. Otherwise FRq (Further request) message is send to NHN (Next Hop Node) to check the reliability of the intermediate node. This method can be applied to identify multiple black hole nodes cooperating with each other and to discover secure paths from source to destination.

Vaishali Mohite et.al [2012], implemented [8] a novel method to find a secure route from source to destination by avoiding cooperative malicious nodes. This method uses data routing information and two additional tables namely RRT (Receiving Record Table) & SRT (Self Record Table). These additional tables hold information regarding the node that sent the reply packet and the information about the current node to be sent to the node that sent the packet respectively. These tables are helpful in keeping the history of the packets sent/received at each node so as to make detection of an inside attacker easier.

This method proves out to be effective against cooperative attacks.

Meenakshi Patel et.al [2013], projected [9] a novel automatic security mechanism using SVM (Support Vector Machine) to defend against malicious attack occurring in AODV (Ad hoc On Demand Distance Vector). This method uses three metrics viz. Packet Delivery Rate (PDR), Packet Modification Rate (PMR) and Packet Misroute Rate (PMISR), to decide the behavior of a node. The information required by the metrics is gathered from all the nodes in the network. These metrics are checked against a threshold, below which the node is considered malicious. The projected scheme is simple and provides fast and quick response to suspicious or compromised node.

Jaspal Kumar et.al [2013] analyzed [10] the effect of black hole attack on the routing protocols and have used AODV (Ad hoc On Demand Distance Vector) and Improved AODV (Ad hoc On Demand Distance Vector) protocol. Experimental results show that IAODV (Improved Ad hoc On Demand Distance Vector) is less affected by black hole attack than AODV (Ad hoc On Demand Distance Vector). Moreover packet delivery ratio of IAODV (Improved Ad hoc On Demand Distance Vector) is improved at an increased routing overhead which can be avoided considering that tackling black hole attack in the network, is a challenging task.

Rutvij H. Jhaveri [2013] presented in [11], a method to avoid malicious nodes from participating in the information exchange between two nodes and also reducing the network load. This method works on R-AODV (Reverse AODV), which states that a PEAK value is calculated by intermediate node using parameters viz. routing table sequence number, RREP sequence number and number of replies during a time interval. Maximum possible value acceptable as a sequence number is the PEAK value and if a RREP packet received has a sequence number higher than the PEAK value, the packet is simply discarded. In this way, only genuine RREP are received at the source. Thus it reduces the network traffic. This method increases the packet delivery ratio with acceptable routing overhead.

Nidhi Sharma et.al [2012], presented [12] a couple of solutions that can be used as a strategy against the black hole attack in MANET (Mobile Ad hoc Network). Two extra tables are maintained to record sequence number of the forwarded packets and sequence number of the received packets. If there is a mismatch between sequence number of received RREP (Route Reply) and the sequence number of the table, the route discovery process is started while alarming the whole network about the node. The scheme does not add overhead as sequence number itself is included in every packet in base protocol.

4. RESEARCH METHODOLOGY

The mobile ad hoc network is the decentralized type of network due to which malicious nodes enter the network which trigger various type of active and passive attacks. The black hole attack is the active type of attack which is triggered by the malicious nodes. The proposed technique is based on to detect malicious nodes which are responsible to trigger black hole attack in the network. The proposed technique consists of following steps for the detection of malicious nodes:-

(i) In the first step, the source node will flood the route request packets in the network. The source node will start the timer to check the time for receiving route reply packets.

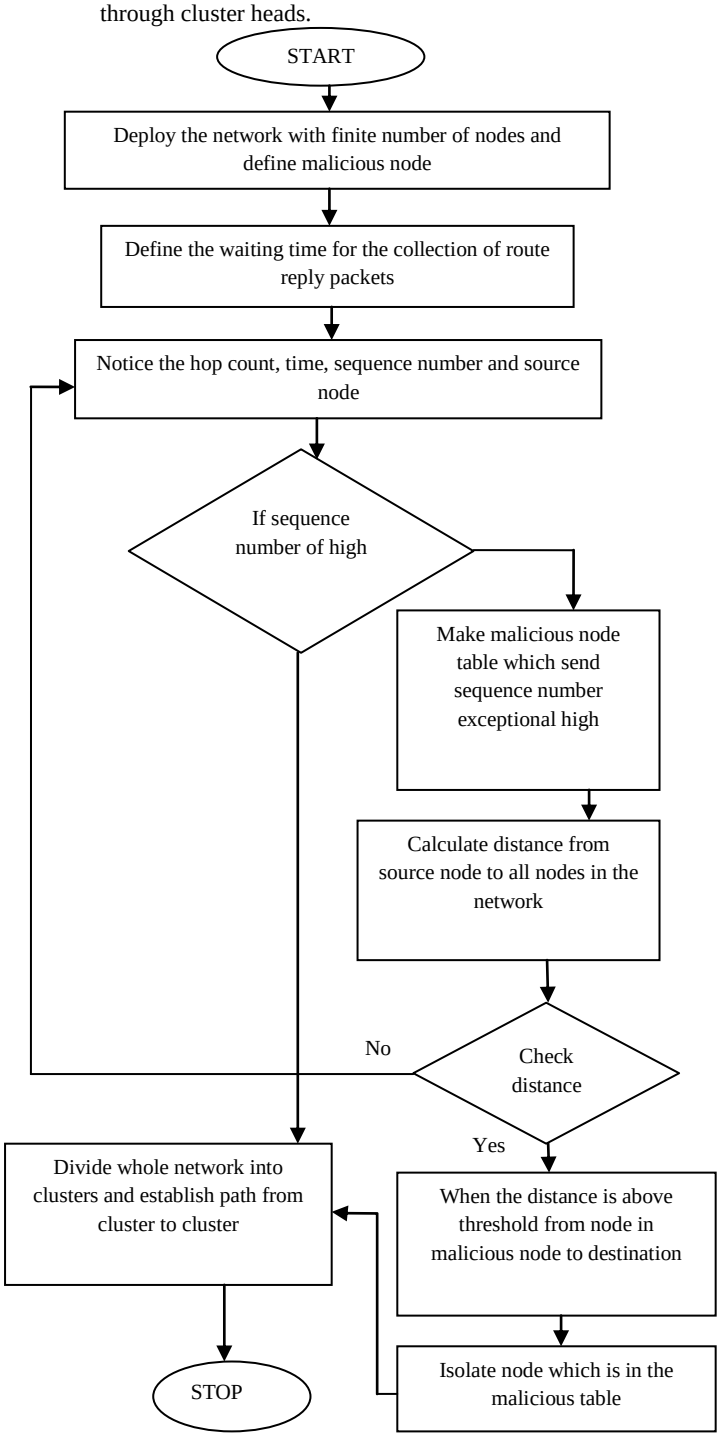
(ii) The source checks each route reply packet and check which node revert in minimum time with the exceptional high sequence number.

(iii) The node which replies back with the exception high sequence number in minimum amount of time will be put into the blacklist.

(iv) The source will check each node that how many numbers of packets are re-transmitted by the each node in the network.

(v) The rating is assigned to each node in the network and node which has maximum trust values will be the most trusted or legitimate node.

(vi) The cluster are formed in the network and node which has maximum trust value will be selected as cluster head and all network data will be transmitted through cluster heads.



5. EXPERIMENTAL RESULTS

The proposed algorithm has been implemented in NS-2 and the results are analyzed in terms of packetloss, delay and throughput.

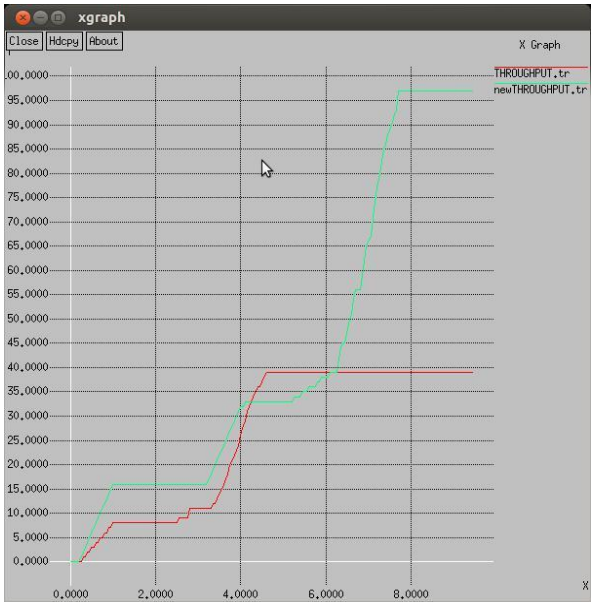


Fig. 1 Throughput graph

In above figure 1, red line shows old throughput and green line show new throughput. X-axis show time and y axis shows packets. It concluded that new technique has more throughput as compare to old technique.

Fig. 2 Delay Graph

In above figure 2, red line shows old delay and green line show new delay. X-axis show time and y axis shows packets. It concluded that new technique has less delay as compare to new technique. It proves that new technique is better than old technique.

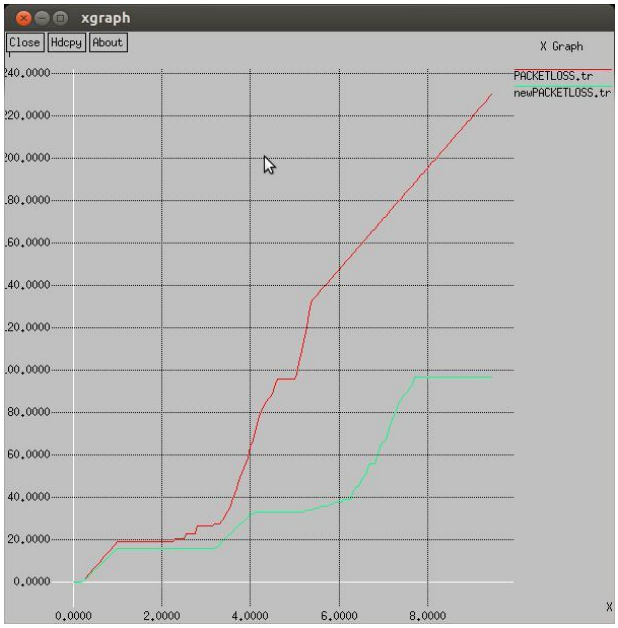


Fig. 3 Packet loss

In above figure 3, red line shows packet loss and green line show new packet loss. X-axis show time and y axis shows packets. It concluded that new technique has less packet loss as compare to new technique. It proves that new technique is better than old technique.

6. CONCLUSION

The mobile ad hoc network is the decentralized type of network in which mobile nodes can join or leave the network when they want. Due to de-centralized type of network mobile malicious nodes join the network which is responsible to trigger various types of active and passive attacks. The black hole attack is the active type of attack which is triggered by the malicious node in the network. The malicious node commit that it has path to destination but it does not have path to destination. This leads to increase network throughput, delay and packet loss in the network. In this work, technique is been proposed which is based on blacklist technique and clustering technique. The proposed technique leads to increase network throughput, reduce packet loss and delay.

7. REFERENCES

[1] Caimu Tang, Dapeng Oilver, "An Efficient Mobile Authentication Scheme for Wireless Networks", 2011, IEEE

[2] Durgesh Wadbude, Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET", 2012, International Journal of Engineering and Innovative Technology (IJEIT) ISSN: 2277-3754 Volume 1, Issue 4

[3] Jacek Cicho,Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada"On Alarm Protocol in Wireless Sensor Networks", 2010, IEEE

[4] S. Sharmila and G. Umamaheswari, "Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", 2012, International Journal of Computer Applications (0975 – 8887) Volume 39– No.4

[5] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", 2005, IJSER

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", 2006, Springer

[7] M. Jhansi, K. R. Devi and B. M. Chandra, "Effective Measure to Prevent Cooperative Blackhole attack in Mobile adhoc Wireless Network," 2012, International Journal of Engineering Research and Applications, vol. 2, no. 4, pp. 204-209

[8] H. L. Nguyen and U. T. Nguyen, "A Study of Different Types of Attacks in Mobile Adhoc Network," 2012, 25th IEEE Canadian Conference on Electrical and Computer Engineering, no. 2, pp. 1-6

[9] M. Patel and S. Sharma, "Detection of Malicious Attacks in MANET: a Behavioural Approach," IEEE International Advance Computing Conference, pp. 388-393, 2013

[10] J. Kumar, M. Kulkarni and D. Gupta, "Effect of Black Hole Attack on MANET Routing Protocols," 2013, International Journal of Computer Network and Information Security, vol. 5, pp. 64-72

[11] R. H. Jhaveri, S. J. Patel and D. C. Jinwala, "A Novel Approach for Gray Hole and Black Hole Attacks in Mobile Adhoc Nework," 2012, IEEE 2nd International conference on Advanced Computing and Communication Technologies, pp. 556-560,

[12] N. Sharma and A. Sharma, "The Black Hole Node Attack in MANET," 2012, IEEE Second International conference on Advanced Computing and Communication Technologies, pp. 546-550