International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-6, June 2015

Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system

Gurbir Singh, Nitin Bhagat

***Abstract*— MANETs are very much prone to internal as well external attacks. Due to frequent change in network topologies and due to less observing .the node misbehave and unable to get possible route path due to malicious node activities .in this paper we studied removal of black hole with alarm system in network by updating detection of malicious node in network and broadcasting to its upstream and downstream nodes. Nodes get avoidance of malicious node and able to get route path for data forwarding.**

***Index Terms*— MANET, Blackhole Attack, DSR, Malicious node.**

I. INTRODUCTION

A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack [1]. Security in MANET is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats [8].

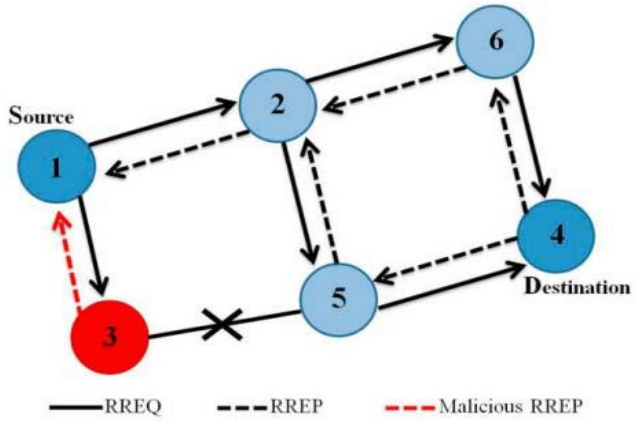

Figure 1 Black Hole Problem [2].

In Figure1, Node 1 is used for defining source node and node 4 denotes the destination node. Node 3 is a mischief node who replies the RREQ packet sent from source node, and makes false results that it has the shortest route to the destination node. Therefore node 1 mistakenly judges the route detection process with accomplishment, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is capable to distract the packets easily, and the network operation is suffered from this problem [2].

The standard security mechanisms such as firewalls, encryption and so on can be used to prevent External attacks. Internal attacks are more serious attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus such malicious insiders work in a group to protect their attacks using standard security measures. These kind of malicious parties are called compromised nodes, as their actions compromise the security of the whole ad hoc. A malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This node advertises its availability of available routes irrespective of checking its routing table. In this way, attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [3].

II. DSR (DYNAMIC SOURCE ROUTING PROTOCOL)

A routing protocol is needed to transfer the packets from source to destination via number of nodes. Number of routing protocols has been proposed for Mobile Ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. Asymmetric link, dynamic topology, interference and routing overhead are the some of the problems in routing in MANET [9].The DSR (Dynamic source routing) protocol is a simple and efficient routing protocol for wireless mesh network which is designed for the use in multi- hop wireless ad hoc network of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need of any predefined infrastructure. This protocol is composed of the two main mechanisms of a) Route discovery and b) Route maintenance. These two work together to allow nodes to discover and maintain routes to arbitrarily destination in the ad hoc network [7].

Gurbir Singh, CSE, Punjab Technical University, Jallandhar, India, 8288845833.

Nitin Bhagat, CSE, Punjab Technical University, Jallandhar, India,

III. Related Work

Ei Ei Khin et al. [4], the performance metrics like average end to end delay, packet delivery ratio and routing overhead has been detected and analyzed with the variable node mobility, pause time and number of transactions. The results show that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. So, the detection and prevention of black hole attack in the network exists as a challenging task.

Arunima Saini et al. [5], a blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. When the packets reach this malicious node, they merely disappear, as a matter of fact, they are said to have been disappeared into a black hole in universe. In fact, the black hole node impersonates the destination node by sending a spoofed route reply packet to the source node that have initiated the route discovery, hence deprive the packets from the source node. Black hole attacks can slow down the network to great extent by dropping out the intended packets to be sent to the destination node. These attacks can be prevented using efficient techniques such as mesh network schemes; AODV based schemes etc. and could be applied to a network ranging from few nodes to larger number of nodes.

K. Selvavinayaki et al. [6], the dynamic changing nature of network topology makes any node in MANET to leave and join the network at any point of time. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. The routing attack addressed in this paper is the black hole attack. The Black hole attack is that where a malicious node advertises itself as it is having the optimal route to the destination. Most of the Routing protocols do not address the issues of the routing attack. This paper describes a solution strategy which will overcome the black hole attacks in MANETs. The proposed solution is that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on DSR protocol .This method is capable of detecting and removing black hole nodes in the MANET.

IV. Proposed System

The proposed routing is based on DSR with modification for detection of black hole attack. In this method the malicious node is detected and the detection of malicious node is transmitted in the upstream and downstream of network with the help alarm system by updating routing table with this method it make route establishment and avoidance of malicious nodes during data forwarding. The striking feature of proposed scheme is its simplicity and effectiveness in finding malicious nodes in scenarios and forwarding frequently in network by updating routing table continuously this algorithm works on the concept that malicious node that drops the packet and modifies the packet. The DSR algorithm is modified to have new system to find malicious node with system the alarm system (AS). During detection process, the nodes initially find the upstream node and downstream nod id's and sends alarm system packet with AS consisting of fake data destination the receiving node update its routing table that it has the route to the invalid destination in its cache, and forward the data packet to it upstream and downstream The information about the black hole is updated in routing table with alarm system in there upstream and downstream. In route finding process, the nodes will verify the routes in its routing table and if the node finds the fake path consists of malicious nodes, the node undermines that route and starts a different direction discovery for escaping the malicious node. Thus, the proposed Schema Removes the black hole attack by a modest method of alarming system (AS) for malicious nodes detection and avoiding it in any of the path during transmitting data packets.

V. Results

The proposed DSR is designed to estimate its performance and compared with traditional DSR. The tests are conducted for changing speed of the mobile hops. The speed is mixed from 10 Kmph to 100 Kmph and calculated for the network performance. The black hole attack mischief is defined as either drop the packets and packet not forwarded in the definite time interval.

Table (130): Values of the end to end delay

Speed	DSR	Proposed DSR
20	0.0512	0.0482
40	0.0625	0.0583
60	0.0675	0.0655
80	0.721	0.680
100	0.0790	0.692

The results in Table (130) shows end to end delay in the proposed DSR is noticeably less.

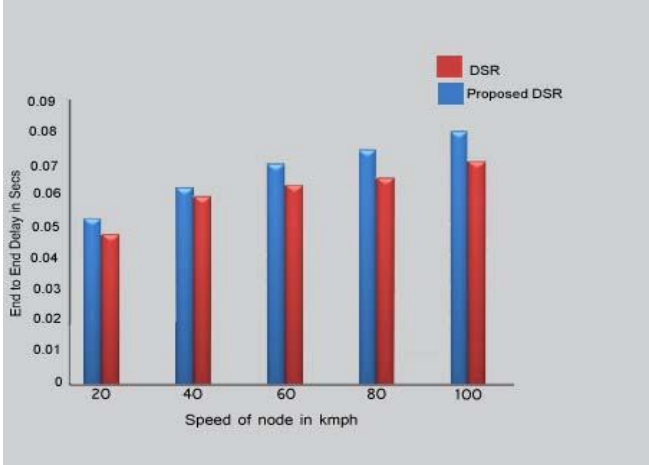

Fig. 2 End to End Delay Ratio

The end to end delay is less in the proposed DSR as shown in Fig. 2.

Table (130): Values of Packet Delivery ratio

Speed	DSR	Proposed DSR

20	**0.9374**	**0.9435**
40	**0.9148**	**0.9326**
60	**0.8842**	**0.9012**
80	**0.8531**	**0.8892**
100	**0.8499**	**0.8846**

The results show the packet delivery ratio improves with the use of Proposed DSR. The results in Table (131) show the proposed DSR performance is better than DSR in the presence of black hole attack. The Fig. 3 shows Comparison results.

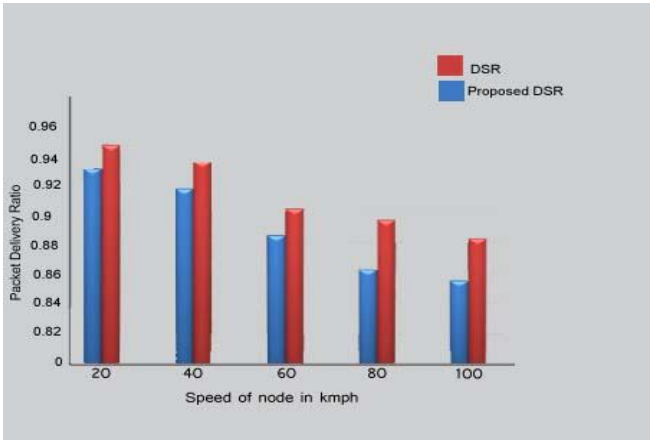

Fig. 3 Packet Delivery Ratio

VI. CONCLUSION

The network system obtained from mobile ad hoc network is called MANET. They are presented self-organized in frequent changing .topologies. Since intruders are sitting inside the network they are Part of network .and they are authorized and they are protected by security system. The DSR routing is improved to include a Alarm system to detect malicious nodes. The result obtained from Experiments shows that the proposed DSR is more efficient than DSR in various conditions.

REFERENCES

[1] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach" IEEE.
[2] Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks" Human-centric Computing and Information Sciences, 2011.
[3] K. Mahamuni, Dr. C. Chandrasekar, "Mitigate Black Hole Attack In Dynamic Source Routing (DSR) Protocol By Trapping" International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013.
[4] Ei Ei Khin, Thandar Phyu, "IMPACT OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOL" International Journal of Information Technology, Modeling and Computing (IJITMC), Vol. 2, No. 2, May 2014.
[5] Arunima Saini, "A Study of Blackhole Attacks, Their Detection and Prevention" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.
[6] K. Selvavinayaki, K. K. Shyam Shankar, Dr. E. Karthikeyan, "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" International Journal of Computer Applications, Volume 7– No.11, October 2010.
[7] Thiyam Romila Devi, Rameswari Biswal, Vikram Kumar, Abhishek Jena, "IMPLEMENTATION OF DYNAMIC SOURCE ROUTING (DSR) IN MOBILE AD HOC NETWORK (MANET)" IJRET, Volume 02, Issue 11, Nov-2013.
[8] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET" International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol. 2, No. 5, October 2012.
[9] Prof. Sunita Sahu, "Impact Of Node Mobility, Pause Time And RREQ Flooding Attack In MANET" International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 6, June 2013.