Performance Analysis of Black Hole Attack in MANET NETWORK

Prashant Kumar Varma[1], Rajesh Upadhyay[2], Gulshan Katara[3]

Mangalayatan University, Aligarh

***Abstract*— MANET is sovereign and decentralized wireless systems. Mobile nodes in a MANETs are free in moving in and out in the network. Due to their self configuration ability these nodes have property to configure themselves.MANETs are not working properly against many types of attack, and black hole attack is one of them. Malicious node shows itself having a valid route to the destination in a black hole attack. An attacker can generate fake information by modifying the packet and, this cause the network traffic diverted or dropped. The performance of MANET's under black hole attack using AODV and OLSR as a routing protocol with Http traffic load will be examined in this research. The performance analysis of AODV and OLSR reactive protocol is evaluated with respect to throughput, end-to-end delay and Packet delivery ratio using OPNET modeler.**

Keywords—MANET, AODV, OLSR, HTTP, OPNET.

I. INTRODUCTION

MANET is sovereign and decentralized wireless systems. MANETs having mobile nodes that are free to move in and out in the network. These nodes can act as host/router or both at same time. According to connectivity with eachother they can create many arbitrary topologies in the network.Because of nodes self-configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) having MANET working group that is dedicated for developing IP routing protocols. Routing protocol has great scope in research area for researchers. Many routing protocols are already there for MANETS.

MANETs need a secure technique for transmission and communication and it is not easy task at all, and vital issue as there is increasing threats of attack on the Mobile Network. Security is the prime requirement of the day. To prevent different attacks those may create unsecure communication and transmission engineer must be careful about different types of security issues of the MANETs. MANET is more open to these kinds of attacks because communication is based on mutual agreement among the nodes, there is no central network management point and no authentication facility, vigorously changing topology and limited resources. Routing protocols in MANETs is a challenging task that is why the researchers are giving their attention to this area [1].

II. ROUTING PROTOCOLS IN MANET

Routing protocols in MANETs is a challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area. According to the function of protocol the routing protocols are categorised in two different classes.

- *Reactive protocols:* they are also called as on demand driven reactive protocols. Only they act on the request of source route hence called reactive protocols. These protocols setup routes when demand.
- *Proactive protocols:* They are different from reactive protocols because. They maintain constant topology of the network. Every node has the information in the networkabout the other node in previous keeping it simple, the whole network is open to all the constituent nodes of that network.The routing information is generally saved in the form of different tables.

2.1. AODV Routing Protocol

AODV is described in RFC 3561 [4]. It's reactive protocol, when a node wishes to data to a node, to which wishes to transmit data to a node to which it has no route, AODV will provide topology information for the node. There is description given below about three different control messages.

Route Request Message (RREQ) —Source node which wants to establish communication link with another node in the network transmits RREQ message. By using expanding ring technique AODV floods RREQ message,in every RREQ message There is a time to live (TTL) value, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP) —A node having a requested identity or any intermediate node having direct route to the requested node generates a route reply RREP message again back to the originator node.

Route Error Message (RERR) —Each node in the network always keep monitoring the linking status to its neighbour's nodes during active routes. When the node detects a link crack

in an active route, Route error (RERR) message is generated by the node for informing other nodes that the link is down.

2.1.1. Route Discovery Mechanism in AODV

When a node "A" wants to initiate transmission with another node "G", it will generate a route request message (RREQ). This message will get travelled to other nodes through a limited flooding. This control message is forward to the neighbours, and those node forward the control message to their neighbours' nodes. This process is repeated until a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP message reaches to the source node, a route is established between the source node "A" and destination node "G". Once the route is establish betweennode "A" and "G" then they can communicate with each other. The following diagram show exchange of control messages between source node and destination node [7].

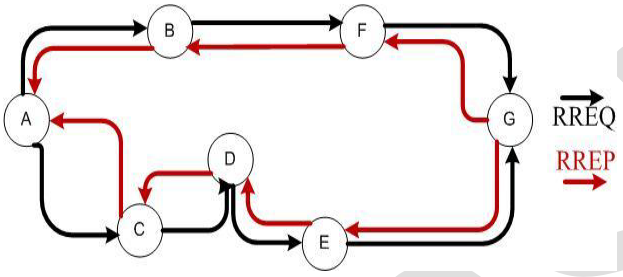

Fig.1.0 AODV Route Discovery

When there is a link down or a link between destinations is broken that causes all the nodes are disconnected form source node, the RERR message is sent to the source node. When the location of destination node is broadcasting by RREQ i.e. from node "A" to the neighbours nodes, at node "E" the link is broken between "E" and "G", so a RERR route error message is generated at node "E" and transmitted to the source node informing the source node a route error [7]. The scheme is shown in the Fig.1.1 below.

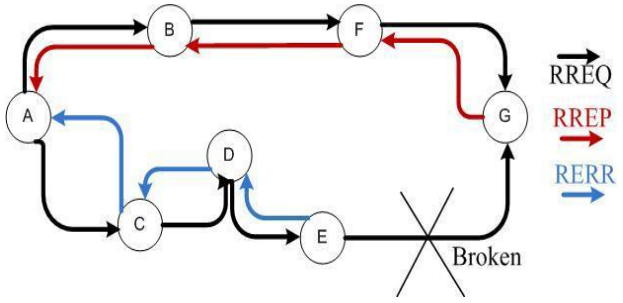

Fig. 1.1 Route Error Message in AODV

2.2. OLSR (Optimized Link State Routing)

It is a proactive routing protocol and OLSR is also called as table driven protocol because it permanently updates and stores its routing table.OLSR keeps track of routing table in order to provide a route if needed. OLSR can be implemented in MANET's as well as in any ad hoc network. Due to its nature OLSR is called as proactive routing protocol. OLSR has also three types of control messages which are as follows.

Hello-for sensing the neighbour and for Multi Point Distribution Relays (MPR) calculation this control message is being sent.

Topology Control (TC) - MPRs are used to optimize the messaging, which are link state signalling being performed by OLSR.

Multiple Interface Declaration (MID)- the list of all IP addresses used by any node in the network,is contained in the MID messages.All the nodes which are running OLSR transmit these messages on more than one interface.

III. BLACK HOLE ATTACK

In Black Hole Attack, in order to advertise itself for having the shortest path to the destination node a malicious node uses its routing protocol or to the packet it wants to intercept. The availability of fresh routes is being advertised by this hostile node without checking its routing table. By this way, the node which is the attacker willalways have the availability in replying to the route request and thus intercept the data packet and retain it [3]. In protocol based on flooding, the malicious node reply will be received by the node which is requesting, before the reception of reply from the actual node;
Hence a malicious and forged route is created. After this route is being established, it's up to the node whether to drop all the packets or forward it to the unknown address.

Fig. 1.2 shows how Black Hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "E" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. Before any other node, it will then send the response to node "A". In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "E". In this way all the data packets will be lost or consumed.

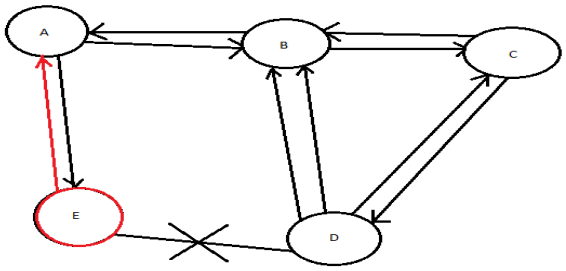

Figure 1.2 Black Hole Problems.

In AODV, in order to distinguish the kind of black hole attack, two types of attacks can be described

- *Internal Black Hole Attack:* This type of attack has an internal malicious node which fits in between the routes of given source and destination. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

- *External Black Hole Attack:* External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

Black Hole Attack in AODV protocol can be classified into two categories: black hole attack caused by RREP and black hole attack caused by RREQ.

3.1. Black Hole Attack caused by RREQ

With sending fake RREQ messages an attacker can form Black Hole Attack as follows:

a) The originator IP address in RREQ is set to the originating node's IP address.
b) The destination IP address in RREQ is set to the destination node's IP address.
c) The source IP address of IP header is set to its own IP address.
d) The destination IP address of IP header is set to broadcast address.
e) Choose high sequence number and low hop count and put them in related fields in RREQ.

So, the information about source node which is false is inserted to the routing table of nodes that gets fake RREQ. Hence, if these nodes want to send data to the source, at first step they have to send it to the malicious node.

3.2. Black hole attack caused by RREP

Along with fake RREP messages, an attacker can form Black hole attack too. A malicious node can generate black hole attack by sending RREP, after receiving RREQ from source node, as follow:

a) The originator IP address in RREP is set to the originating node's IP address.
b) The destination IP address in RREP is set to the destination node's IP address.
c) The source IP address of IP header is set to its own IP address.
d) The destination IP address of IP header is set to the IP address of node that RREQ has been received from it.

IV. RESEARCH METHODOLOGY

The research design is divided the whole research into four stages.

- Problem Identification and Selection.
- Literature study.
- Building simulation.
- Result analysis.

Problem Identification and Selection— The Most Important part in MANET the focus was given to the security issues and its effect on AODV & OLSR routing protocols.

Literature Study— Literature study is conducted to develop a solid background for the research. The functionality of different simulation tools is studied.

Building Simulation—To build and develop simulation the knowledge the background which was developed in the literature phase is combined.According to the requirements of the problems different scenarios are developed and are simulated.

a. SIMULATION TOOL— In this research, OPNET tool is selected to carry out the simulation. OPNET provide technologies, protocols, communication devices for academic research, assessment and improvement. It is efficient, failure proof and highly reliable which gives the user the ease of graphical interface, developing and running the simulation and validation of the results.

b. PERFORMANCE METRICS—

I. Network Throughput—A network throughput is the average rate at which message is successfully delivered between a receiver (destination node) and its sender (source node). It is also known as the ratio of the amount of data which is received from its sender to the time in which the last packet reaches its destination [8]. Throughput can be calculated as bits per second (bps), packets per second or packet per time slot and it is expressed in bits per second by OPNET Modeler.

Throughput= (number of delivered packet * packet size)/total duration of simulation.

II. End-to-end Delay—The time delay which a network source takes to deliver a packet to its destination is called packet end-to-end delay. Thus, it is the total amount of delay which it finds in the

complete network at every hop which is going to its destination.

III. *Packet Delivery Ratio*—Packet delivery ratio is refers to the ratio of the total number of data packets that reach the receiver (destination node) to the total number of data packets sent by the source node.

IV. *Result Analysis*—We study and analysed the impact of Black Hole attack in MANETs using AODV and OLSR protocols on the basis of throughput, end to end delay and packet delivery ratio separately and comparatively also.

V. CONCLUSION

In our research we have analyzed the behavior and security challenges in mobile Ad-Hoc networks with solution finding technique.

In this thesis the simulation study consist of two routing protocol AODV and OLSR deployed over MANET using HTTP traffic analyzing their behavior with respect to three parameters delay, throughput and packer delivery ratio under the presence of malicious node. As the number of malicious nodes increases the average end to end delay also increases while throughput can be varied as the number of malicious nodes increases. In a network it is important to a protocol to be redundant and efficient in terms of security. From the above figures and tables it is concluded that the OLSR performs well as compare to AODV. AODV having higher as the number of malicious nodes increases as compare to the OLSR.

Based on our research and analysis of simulation results we draw the conclusion that AODV is more vulnerable to black hole attack than OLSR.

REFERENCES

[1]. Abolhasan, M. et al. (2003) "A Review of Routing Protocols for Mobile Ad Hoc Networks", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[2]. Barushimana, C.M., Shahrabi, A. (2003) "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks", Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[3]. Biswas, K. and Ali, M.L. (2007) "Security threats in Mobile Ad Hoc Network", Master Thesis, Blekinge Institute of Technolog Sweden, 22nd March 2007

[4]. http://www.olsr.org/docs/report_html/node28.html, "Multi point Relaying".

[5]. Murthy, C. andManoj, B. (2005) "Ad hoc Wireless Networks: Architectures and Protocols", Prentic Hall PTR , 2005

[6]. Perkins, C.E. and Royer, E.M. (1999) "Ad Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999

[7]. ShoaibRehmaan, I.U. (2010) "Analysis of Black hole Attack on MANET using different MANET routing protocols", Thesis no: MEE-2010-2698 June, 2010.

[8]. Trang, N. V. and Xing, X. (2005) "Rate-adaptive Multicast in Mobile Adhoc

AUTHORS

Prashant Kumar Varma received his Bachelor's Degree in electronics and communication from UPTU, Lucknow (U.P), India. Now he is pursuing his M.Tech. in Electronics and Communication from Mangalayatan University, Aligarh, Uttar Pradesh. His areas of interest are MANET and Wireless Network.