BLACK HOLE ATTACK AND ITS MITIGATION TECHNIQUES IN AODV AND OLSR

Anjaly Joy
Department of Information Technology
Rajagiri School of Engineering and Technology
Kochi, India
anjalytjoy@gmail.com

Sijo Cherian
Department of Information Technology
Rajagiri School of Engineering and Technology
Kochi, India
sijoc@rajagiritech.ac.in

Abstract- MANET is a self configurable, self deployable and infrastructure less network in which nodes are continuously moving and creates dynamic topology. For routing the main protocols using are AODV, OLSR, DSDV, DSR etc. AODV and DSR are reactive protocols, where DSDV and OLSR are proactive protocols. This paper deals with AODV and OLSR protocols. Since the topology is dynamic the attacker presence is more. Many attacks such as black hole, worm hole, grey hole , flooding attack etc can occur among this black hole is the main one. The attacker acts as a black node which will fake the source node showing more attractive path to the destination. As a result the source will forward the data through the black node and it will drop the packets. This paper presents a survey on black hole attack in OLSR and AODV protocols and the corresponding mitigation techniques.

Keywords-*:* MANET, AODV, OLSR, Black hole attack

I. INTRODUCTION

A Mobile Adhoc network is a collection of mobile devices that can communicate with each other without any predefined administration and infrastructure. The mobile hosts are not bound to any centralized control like base stations or switching centers. Although this offers unrestricted mobility and connectivity to the users. Due to the limited transmission range of each node multiple hops may be needed for one node to exchange data with another across the network. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. As a result they are losing their energy through the packet forwarding. The concept of MANET is also called infrastructure less networking, because the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. Due to this dynamic mobility routing is so much difficult and complex. Currently, several efficient routing protocols have been using in MANET. These protocols are classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol[10], nodes find routes only when required. They will initialize a Route Request to the network.

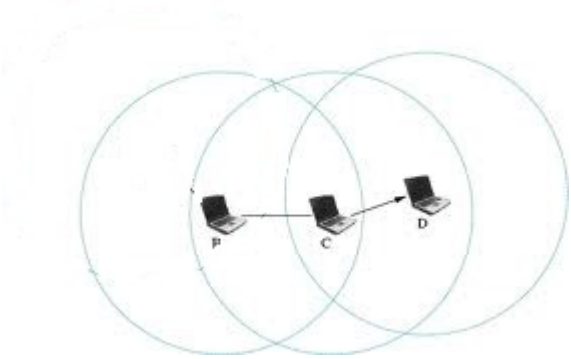

Fig 1: Mobile Adhoc Network

Several Route replies come and selects the best one. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [9] , nodes obtain routes by periodic exchange of topology information.

For maintaining this information routing tables are using. Due to the lack of centralized administration most of these protocols are depending on each other to get updated. In such a network an attacker has more possibility to launch an attack by denying the services or changing the basic characteristics of the network and as a result disrupting the routing.

Many counter measures are developing for avoiding the attacking possibilities. Among them the first one is effective intrusion detection system such as watchdog, path rater[11] etc. There are many techniques for protecting the routing protocols in the network. They are key management, encryption techniques etc which provides confidentiality, authentication and integrity. As a result it prevents the joining of unauthorized nodes into the network and protects it. The problem in key management is that it will cause heavy traffic by exchanging keys. And also for a bandwidth limited network such as MANET this exchanging of keys will result in high cost constraints[3]. Another preventive measure is the use of secure routing protocols such as authenticated routing for ad hoc networks (ARAN), Ariadne, secure AODV (SAODV), SEAD(Secure Efficient Adhoc Distance Vector) routing protocol[5]. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation. The existing security solutions for wired networks cannot be applied directly in wireless MANETs.

In this article, we survey the current state of the art of black hole attack in MANET under OLSR and AODV protocol, and its countermeasures in a MANET. The rest of the paper is organized as follows: a detailed study about the two protocols. Next section deals about black hole attack, and its effects in OLSR and AODV protocols. Coming sections are mitigation techniques, conclusion and directions for future works.

II. RELATED WORK

The goal of routing protocol in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. Routing protocols in a MANET are divided into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR) [4].

Table-driven (Proactive): Table driven routing protocols essentially use proactive schemes. When the network is formed the first thing each node performs is the information exchange. Based on the received neighboring information each node identifies their neighbors and make a table known as routing table. After the completion of a full table it will be propagated to the network. Whenever a new change occurred in the network or to a node, then that change will be updated in the table. Then the updated table will be propagated to the network and the remaining nodes will do the same

On demand (reactive): A diverse approach from table driven routing is source-initiated on-demand routing. This type of routing creates routes only when they need a novel route to a specific node. When a node requires a route to a destination, it initiates a route discovery process by sending a route request within the network. This route request will propagate until it reaches the destination. Then the destination initiates a route reply to the source node. Upon receiving this the source will forward the data. In this section, we define two standard routing protocols that are currently being explored actively, that is, AODV and OLSR.

A. AODV(Adhoc On Demand Distance Vector)

AODV is a reactive routing protocol designed for a MANET [3, 10]. In AODV, If S is the source node and wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. Destination node chooses the first RREQ packet that it has been received.

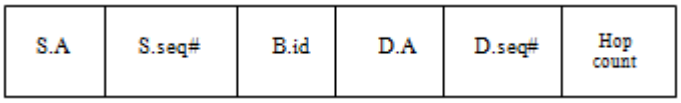

Fig 2: Packet format of AODV

S.A: Source address

S.seq#: source sequence number

B.id: Broadcast ID

D.A: Destination Address

D.seq#: Destination Sequence number

As the broadcast id is incremented for each route request, the node can discard duplicate copies of the RREQ. An intermediate node receiving a RREQ and if a valid route is available to the destination it can send a route reply (RREP) through the reverse path to the source, else the node rebroadcast the RREQ. The two

sequence numbers, the source sequence number and the destination sequence number, included in the RREQ packet are used to maintain freshness information about the reverse route to the source. If the intermediate node has found a route to the destination, it determines whether the route is valid by comparing the destination sequence number in its own table entry to the destination sequence number in the RREQ. A higher Sequence numbers signifies a fresher route.

B. OLSR (Optimized Link State Routing)

OLSR[3, 9] is a proactive routing protocol, which is based on periodic exchange of topology information from routing table. The key concept of OLSR is the use of multipoint relay (MPR) nodes. It provides an efficient flooding mechanism by reducing the number of transmissions required and hence reduces the traffic. In OLSR, each node selects some nodes as its MPR nodes from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising. The source first sends the message to its neighbors. Then the nodes receiving this message checks the MPR selector list to know that it is an MPR node of the source node or not. If it is then send the packet to its neighbors, otherwise process the packet and don't forward it. Usually, in the OLSR protocol, two types of routing messages are used, namely, a HELLO message and a topology control (TC) message. HELLO message is used to detect the neighbors for making the MPR selector list.

Destination	Next Hop	Distance

Fig 3: Routing table format of OLSR

Each node generates a HELLO message periodically. HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not furthered to other nodes. A TC message is used for route calculation. Each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR nodes and is known as MPR selector list. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn about the overall network topology and can build a route to every other node in the network.

MPR Selection

For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

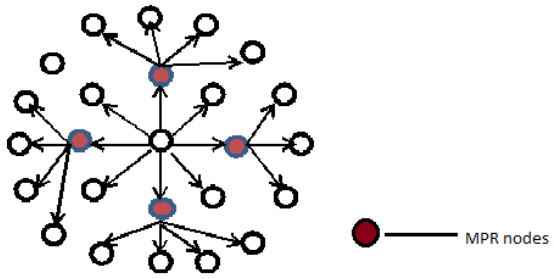

Fig 4: MPR nodes of a node

III. BLACK HOLE ATTACK

In a black hole attack[2, 3], a malicious node sends fake routing information, claiming that it has a finest route and causes other good nodes to route data packets through the malicious one. As a result it will attract all packets and drop it and hence denying the destination of getting its data. The black hole attack has two characteristics. First, the node exploits the mobile ad hoc routing protocol, such as AODV or OLSR, to advertise itself as having a valid route to a destination node, even though the route is unauthentic, with an objective of capturing packets. Second, the attacker consumes the intercepted packets without any forwarding. An attacker overwhelms or modifies packets originating from some nodes, at the same time leaving the data from the other nodes unaffected. So it is difficult for a network analyzer to spot the attack.

a. Black hole attack in AODV

The attacker sends a fake RREP (containing a fake destination sequence number which is equal to or greater than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. As a result the source node selects the route which is having this particular attacker.

Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic[2].

b. Black Hole attack in OLSR

In OLSR the network topology information is built from HELLO and TC messages. A node acting as black hole sends fake HELLO messages. In these messages the malicious node argue that it have more links to neighbors than it actually has. Thus, there is a larger possibility of selecting this node as an MPR node of the source. The more neighbors the attacker node have, the larger the possible influence of the attack. Due to the fake messages of the attacker, in its neighborhood falsified TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture routes[2].

IV. RESULTS

The following analysis is based on the simulation performed in OPNET modeller. Simulated results are provided in Figures (5,6) gives the variation in network nodes while under Black Hole attack. To evaluate the behaviour of simulated intrusion based black hole attack, we considered the performance metrics of throughput and network load.

From Fig.5, for 20 nodes, it is obvious that the throughput for OLSR is high compared to that of AODV. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput.

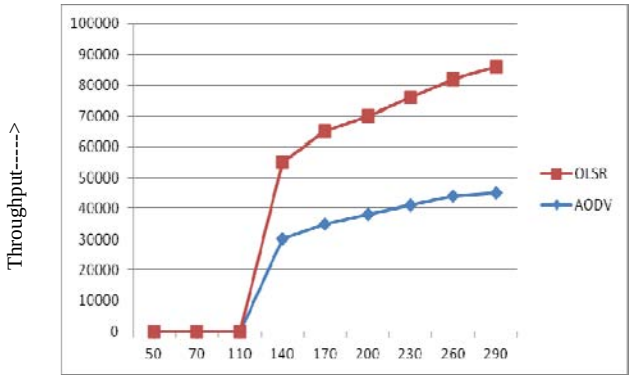

Fig 5: Throughput of 20 nodes AODV vs. OLSR with attack

The network load of OLSR is higher as compared to AODV. In case of 20 nodes the network load of OLSR is 2 times higher than AODV which implies that it is actually routing its packet to the entire destination properly. But under attack it cannot send its packet i.e. packet discarding leads to a reduction of network load.

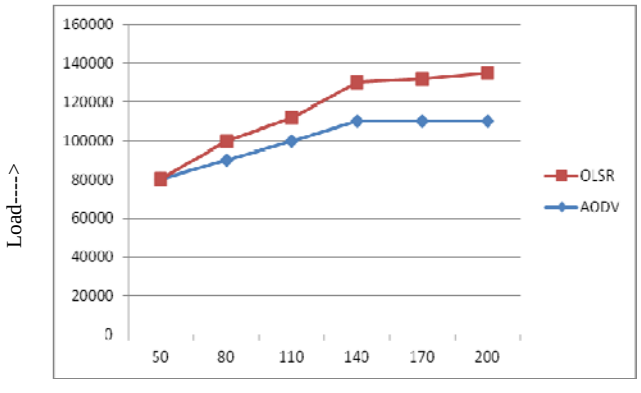

Fig. 6: Network load 30 nodes AODV vs. OLSR with attack

We have analysed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR.

V. MITIGATION TECHNIQUES

Since black hole attack is a common attacking scenario in MANET there are many possible mitigation techniques are using. Here in this survey paper mitigation Techniques from different papers are proposing. Attacks which modify routing messages can be mitigated by the use of source authentication. Up to certain level of security can be attained at network layer in internet by the use of IPSec. Protocols such as ARAN, SAODV, ARIADINE, SEAD[5] etc are protocols which provides the protection from Black Hole attack.

a. Mitigation Technique using Dempster shafer theory

In [1] Dempster Shafer theory is proposed. It is a mathematical theory of evidence which collects some evidences from the given scenario and based on that the system reaches some conclusions. This can be applied in OLSR routing protocol. Evidence calculation is done from the routing table. So three types of evidences are collected from the table; Missing entry, alert confidence from IDS and changing entry. From these evidences risk value is calculated. If the risk value is above higher threshold then the node must be isolated. If it is below the lower threshold value then No isolation and if the value is between the two thresholds then temporary isolation.

b. Mitigation by SAODV protocol

SAODV is proposed in [7] to use a signature to authenticate most fields of a route request (RREQ) and route reply (RREP) and to authenticate the hop count hash chains are using. SAODV designs signature extensions to AODV. Network nodes authenticate AODV routing packets with an SAODV signature extension, which prevents certain masquerade attacks. SAODV can effectively prevent Black Hole attack in Mobile Ad-hoc network and maintain better routing efficiency. It is better than AODV in terms of security and routing efficiency.

c. Use of data routing information table

This is applicable when multiple black hole attacks are present. Along with routing table, another table known as Data Routing Information Table(DRTI) [3] which contains three fields are using. The fields are node id, from and through. From and through is denoted using binary values (0 and 1). 0 represents ‘true’ and 1 value ‘false’. From field represents the node from which the data is send and through field represents the node through which the data has been arrived. If both of these fields are 0 then the node is a black node.

d. Use of confirmation request message

Route confirmation request message (CREQ) and route confirmation reply (CREP) proposed in [6] is used in order to avoid Black Hole attack. In this proposal when intermediate sends RREPs to the source node its send CREQ to its next hop node in direction of destination node. After receiving CREQ, the next hop look for route in its destination in cache. If it receive CREP during this time it will confirm the validity of path in RREP and in CREP. Upon matching the source node will recognize the route being correct. Its drawback is that it cannot detect multiple Black Hole attacks.

e. Mitigation by using destination sequence number

In [8] the author projected that black hole attacker node increments the destination sequence number to please its Path to the destination. So to detect this mistake, the destination sequence numbers are subtracted at the source. If it is higher then black hole can be detected.

VI. CONCLUSION

This survey paper is based on various mitigation techniques for the black hole attack under OLSR and AODV protocols. Both OLSR and AODV are MANET protocols. As proactive protocol, OLSR reduce the control overhead, also the efficiency is gained and through simulation it is proved that it has more throughput and slightly more network load compared to AODV. So the performance of OLSR is more when considering attack and its delay. Several Mitigation techniques are proposed based on the attack nature. As a future enhancement we can consider more MANET protocols such as DSR, DSDV, TORA and further more attacks.

REFERENCES

[1] Ziming Zhao, Gail-Joon Ahn ,“Risk Aware Mitigation For MANET Routing Attacks,” IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012

[2] Anuj Gupta, Navjot Kaur, Amandeep Kaur, “A Survey on Behaviour of AODV and OLSR Routing Protocol of Manets under Black Hole Attack” in IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A Survey of Routing Attacks in Mobile Ad Hoc Networks,” IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85- 91, Oct. 2007.

[4] H. Deng, W. Li, and D. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[5] Y. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[6] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006

[7] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.
[8] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic".
[9] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003
[10] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
[11] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.