Analysis of Black Hole Attack on MANET Using Different Routing Protocols

Vandna Dahiya
Assistant Professor, Dept of Computer Application
Kanya Mahavidalaya, MDU, Haryana

ABSTRACT

Wireless connections are gaining popularity day by day, as users want to connect to the network irrespective of their location at the globe. Due to unique characteristics of MANET, there is very much threat of malicious attacks on MANET. Black Hole is one of the threat where data of the network is routed towards a node which drops all the packets completely. It's an analogy to the black hole in the universe in which things disappear. The scope of this paper is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc on Demand Distance Vector (AODV). Comparative analysis of Black Hole attack for both protocols is taken into account. The impact of Black Hole attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements are taken in terms of throughput, end-to-end delay and network load. Simulation is done in Network Simulator (NS-2.35).

I. Introduction

Basic functionality of a network depends of security of communication [1, 2]. 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 issues because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. MANET are very much exposed to attacks [3, 4]. These attacks are used to destabilized the performance of the MANETs, sometime the attacking node in the network refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption. One of the most interesting attack in MANETs, where the attacker tries to discards all the packets of a destined node is black hole attack.

We investigate the consequences of black hole attack on MANET by measuring the performance impact of MANET under normal operation as well as under the Black Hole attack. This is important because of the factor to know how severe the attack is, how much the network is destabilized. We also investigate which of the two types of routing protocols are more vulnerable to the attack on MANET: Active or Proactive. Investigation is carried out by comparing the results for both types of protocols under the attack. This vulnerability of attack would lead us to research more on that particular protocol in order to make it more secure in such type of attack.

II. Related Work

Despite the fact of popularity of MANET, these networks are very much exposed to attacks [3,4].

Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication.

In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmissio [5, 6]. One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw.

In black hole attack, hostile node advertises its availability of fresh routes irrespective of checking its routing table. [7, 8]. A path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop.

Many solutions have been proposed to combat on Black Hole attack, one of the solution proposed by Deng [9] gives the approach of disabling the reply message by the intermediate.

The solution proposed in [10] focus on the requirement of a source node to wait unless the arrival of RREP packet from more than two nodes. When it receives multiple RREPs the source node check that there is any share hops or not. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node.

III. Black Hole attack and Classification

Black hole attack is a type of attack where the malicious node brands itself as having shortest route to some destination. It advertises its availability of fresh routes and thus intercepts the data packet and retain it [11]. 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 fake 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 [12].

Fig here 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 “C” is a malicious node then it will declare that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node. 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 “C”. In this way all the data packet will be consumed or lost.

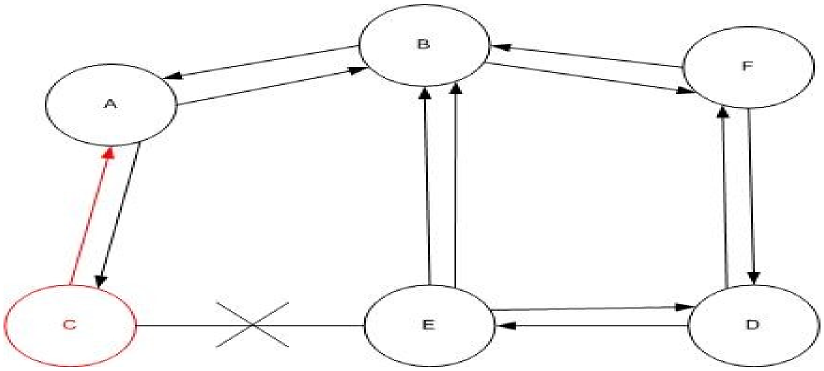

Fig 1: Black Hole Problem

Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

In this type of attack, the hostile node gets fits in between the routes of source and destination. Whenever the earliest it gets the chance to advertises its fake routes, it becomes active. At this stage it is now capable of conducting attack with the start of data transmission. 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. External black hole attack can be described as follows- Destination address get disclosed by malicious node which is outside the network and then it sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Sequence number is set to the highest value and hop count to the lowest. Malicious node send RREP to the nearest available node which belongs to the active route. If route is available, this can also be send directly to the source. The RREP received by the nearest available node to the malicious node will relayed through the established converse route to the data of source node. The new information received in the route reply will now allow the source node to update its routing table. New route is then selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route.

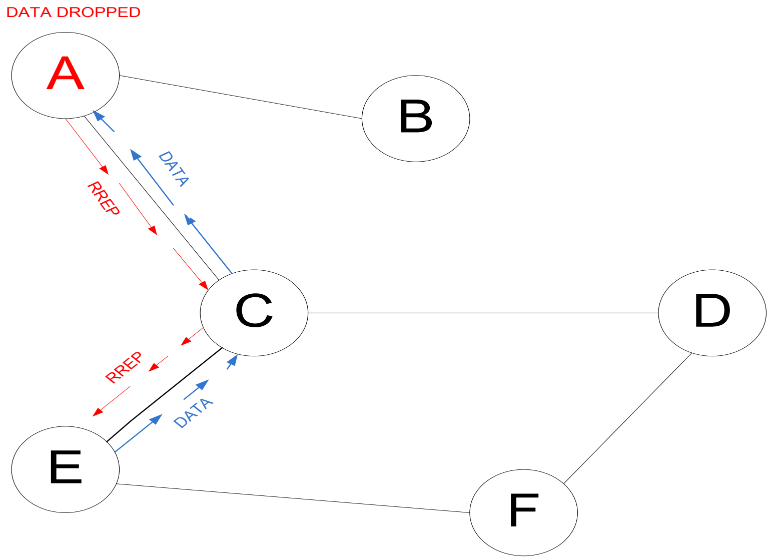

Fig 2: Black hole attack specification

In AODV black hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D”. The malicious node “A” then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

Black hole attack in OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR (Multi Point Relaying). Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack.The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

Black hole with other types of Attacks on MANET

There are certain attacks which together with black hole can affect the network far more severely than a standalone black hole attack. Following are some attack which can lead to a network attack with more malicious impact - Gray Hole attack, Flooding attack, Selfish node, Wormhole attack, Sleep deprivation torture attack, Jellyfish attack, Impersonation attack. These above different kind of attack can form collaborative attacks on a network with collaboration of one or more types of attacks.

IV. Performance parameters and Analysis

Three performance parameters i.e. end to end delay; throughput and network load is taken. The aim is to study the effect of black hole on AODV and OLSR by analyzing that how much performance of a network has been compromised. In other words these parameters show us extend of vulnerability of black hole attack of selected network protocol (AODV, OLSR).

The packet end-to-end delay is the average time in order to traverse the packet inside the network including delay of buffer queues, transmission time and routing activities

The throughput is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet, represented in bits per second or packets per seconds.

The third parameter is network load, it represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission

V. Simulation Setup and Results

NS-2.35 is used for modeling of network nodes, selecting its statistics and then running its simulation to get the result for analysis. Simulation setup of a single scenerio comprising of 21 mobile nodes moving at a constant speed of 10 meter per seconds. AODV and OLSR routing protocols are chosen which are reactive and proactive protocols respectively. CBR is used to generate the data with speed of 10 Mbps. Mobility of nodes is taken as random.

The goal is to determine the protocol which shows less susceptibility in case of black hole attack. The first simulation is building of MANET with normal behavior without any type of attack introduced.

In case of black hole attack single malicious node is introduced in the whole network. After simulation of the scenario the graphs are analyzed in comparison with normal working protocols of AODV and OLSR (without attack). The malicious node is place in the network between sender and receiver. This malicious node when receive any sort of packets actually discards out all the received data.

Packet End-to-End Delay

For packet end-to-end delay, the behavior of attack (Black hole) also depends on protocols, routing procedure and number of nodes involved. Fig below shows the delay for AODV and OLSR in case of 21 nodes. This result was carried out when black hole attack was introduced and the graph is compared with the normal working protocol so as to observe the effect of attack on the whole network. The graph shows higher delay when there is no malicious node present in the network.

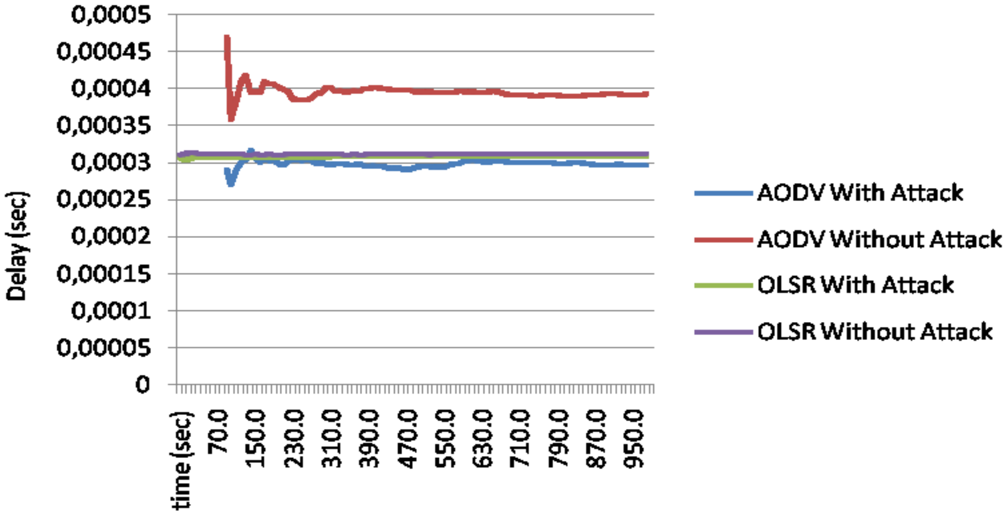

Fig 3: End-to-end delay for OLSR and AODV with vs. without attack for 21 nodes

AODV show high delay in comparison with OLSR. In terms of delay the performance of OLSR improves with the increase in number of nodes because of its table driven nature. It maintains up to date routing information from each node to every other node in the network.

Throughput

Fig below shows throughput for OLSR in case of no attack (no malicious node present) is higher than the throughput of OLSR under attack (in the presence of malicious node). 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. The same is observed in the case with AODV, without attack, its throughput is higher than in the case with under attack because of the packets discarded by the malicious node. Also when both protocols are compared with each other the throughput of OLSR is higher than that of AODV.

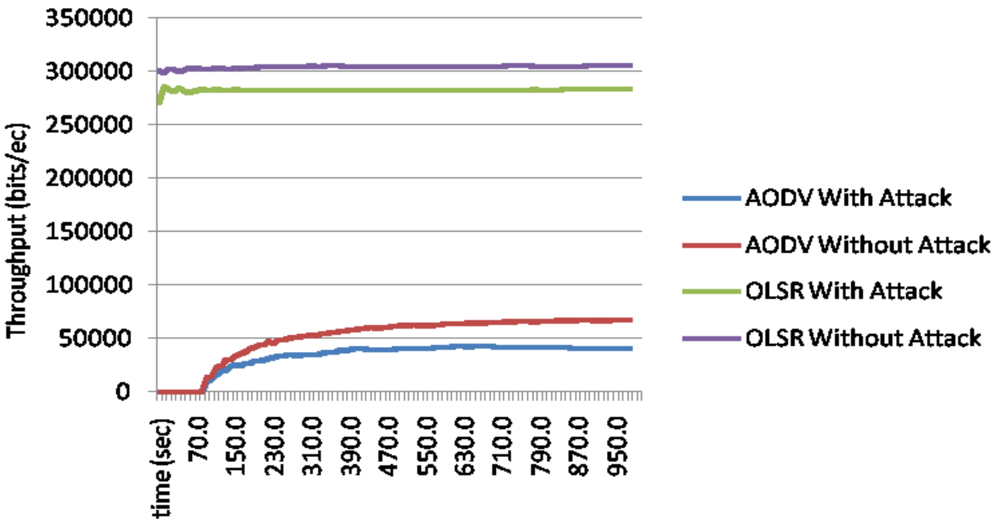

Fig 4: Throughput of OLSR and AODV with vs. without attack for 21 nodes

Network Load

Figure shows that OLSR and AODV have less network load when there is attack in the network. The reason is that the malicious node does not send any data within the network it just discard all the packets it receives, thus causing less network load. From figure it was analyzed that the network load of OLSR is nearly 3 times higher in case of without attack 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. The same pattern is followed by AODV in the same graph.

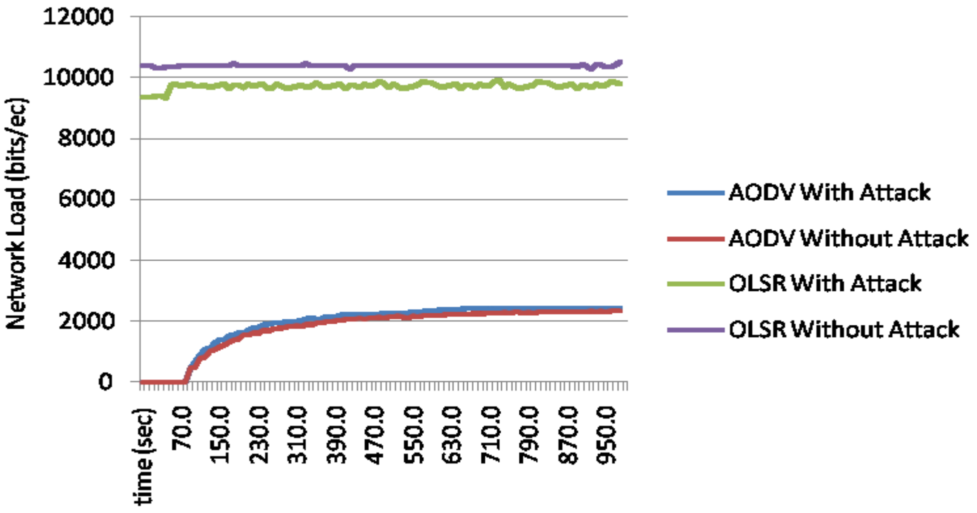

Fig 5: Network Load of OLSR and AODV with vs. without attack for 21 nodes

Similarly when both protocols are compared with each other it was analyzed that in case of OLSR, there is a high network load in presence of a malicious node as compare to that of AODV. In case of higher number of nodes AODV react more quickly as compare to OLSR which made the difference in network load much wider. As the node begins to pause and restarts and its mobility after the starting period having more stability make network load more pronounced.

VI. Conclusions

The aim in this research work is to determine the protocol which has low vulnerability for black hole attack taking AODV and OLSR routing protocols and that how much performance of a network has been compromised.

As in Black Hole attack, there is no need of RREQs and RREPs. So in the presence of malicious node (attack scenario) the delay has been reduced. The malicious node establishes a direct link with sender node. Now all the data sent through this malicious node never reaches the actual receiver causing the black hole effect. Also when both protocols is compared with each other in order to find the effect of attack on both protocols AODV shows more delay than OLSR.

For throughput considering low load of OLSR, in the presence of a malicious node is comparatively low with comparison to ADOV because of its fewer routing forwarding and routing traffic. The malicious node discards the data rather than forwarding it to the destination, thus effecting and manipulating the throughput. Throughput in case of AODV with presence of malicious node is comparatively higher than OLSR. This is because of the packets discarded by the malicious node. As the malicious node immediately sends its route reply and the data is sent to the malicious node which discard all the data. The network throughput is much lower.

In case of network load, at high speeds the routing protocols take much more time for adjusting and afterward sending of traffic to the new routes. In case of higher number of nodes AODV react more quickly as compare to OLSR, i.e. high network load for OLSR which made the difference in network load much wider. As the node begins to pause and restarts and its mobility after the starting period having more stability make network load more pronounced.

After analyzing the vulnerability of both protocols i.e. AODV and OLSR in terms of low network traffic and high network traffic, results shows that AODV is more affected by the black hole node. This level of delay affected is about 2 to 5 percent while in OLSR is about 5 to 10 percent. The delay of AODV in normal network is much higher than the delay in black hole attack. 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.

Based on this analysis of simulation results, AODV is more vulnerable to Black Hole attack than OLSR.

Future Work

Wireless Ad-Hoc networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. In this paper, efforts are done to discover and analyze the impact of Black Hole attack in MANETs using AODV and OLSR protocols. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP.

References

[1] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[2] T.Clausen, P.Jacquet , "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, 2003.

[3] C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: April. 10, 2010]

[4] H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.

[5] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks", University of Cincinnati, IEEE Communication Magazine, Oct, 2002.

[6] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[7] Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

[8] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 2002.

[9] M.Parsons, P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks", [Online]. Available: www.cse.buffalo.edu/srds2009/dncms2009_submission_person.pdf, [Accessed: April. 10, 2010].

[10] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[11] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[12] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265,