A Survey on Black Hole Attack on AODV Routing Protocol in Wireless Adhoc Networks

Er.Sarabjeet Kaur
M.Tech (CSE)
BBSBEC Fatehgarh Sahib

Er.Birinder Singh
Assistant Professor
BBSBEC Fatehgarh Sahib

Abstract

Adhoc network is a collection of mobile nodes with temporary wireless connections without any centralized and management point like the access point in 802.11 infrastructure. Every node in ad-hoc network operates as both host and router. Routing is very important component in adhoc networks and routing protocols are used to find path from source to destination. Due to lack of infrastructure in adhoc networks, routing protocols are vulnerable to various types of attacks. AODV (Adhoc on demand distance vector routing) protocol is one of the reactive routing protocol suitable for adhoc networks and it is more vulnerable to blackhole attack which is one of possible attacks .A black hole attack is network layer attack in which malicious node falsely advertise the source node that it is having shortest path to destination, actually it does not have and drops the packets. In this paper a survey of black hole attack in AODV routing protocol is done.In future we will modify feature of AODV protocol using Qualnet simulator.

1. Introduction

A wireless ad-hoc network is a decentralized type of wireless network that does not rely on a preexisting infrastructure, such as routers in wired networks or access points in infrastructure wireless networks. Each node participates in routing by forwarding data for other nodes. On the basis of network connectivity, the determination of which nodes forward data is made dynamically. In an ad hoc network all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Ad-hoc networks have a dynamic topology in which nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battle field or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Wireless adhoc networks can be classified by their application as: Mobile adhoc networks (MANET), wireless mesh networks (WMN), wireless sensor networks (WSN).Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure; they provide the connectivity by forwarding packets over themselves. To Support this connectivity nodes use some routing protocols such as AODV such as AODV (Ad-hoc On-Demand Distance Vector routing), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Each node can act as a host as well as router to discover path and forwards packet to the nodes in the network. As wireless ad-hoc networks lack an infrastructure, routing protocols are exposed to lots of attacks. One of these attacks is the Black Hole attack on AODV routing protocol. In a blackhole attack the malicious node easily misroute network traffic to itself and then drop the packets, causes loss of packets. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV.

2. Routing protocols

In ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All

nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Routing protocols are required to establish route from source to destination. The available routing protocols are mainly categorized into proactive routing protocols, reactive routing protocols.

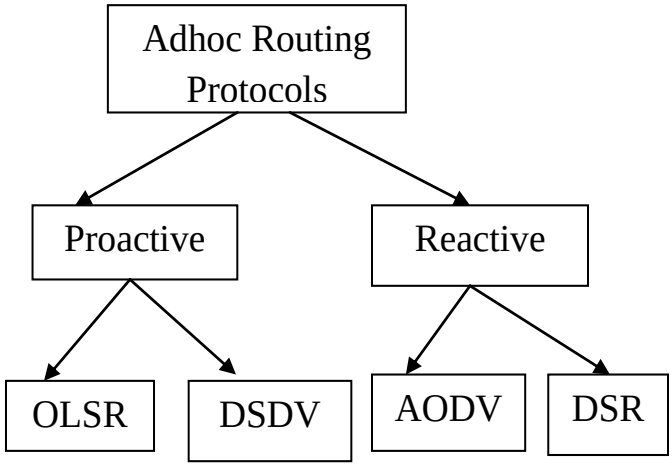

Figure 1: Routing Protocols

2.1. Proactive routing (or table-driven protocol)

Every node in ad hoc network environment need to know the topology in advance and aware of the every path to each node. So every node maintains its own routing table. Proactive protocols are better for environment with fixed nodes. Examples of proactive routing: DSDV (Destination-sequenced distance vector) routing, OLSR (Open link state routing).

Advantage

1. Efficient way to communicate with every node
2. There is no effort of path discovery before transmitting packets.

Disadvantages

1. Proactive routing protocol must broadcast its own routing table to maintain the latest topology periodically,
2. Wastage of lots of battery power and bandwidth in mobile ad hoc networks

When a source node wants to send data packets to destination node, it initiates a path-discovery process to locate the other node. The source node broadcasts a RREQ packet with its IP address, Broadcast ID (BrID),

2.2. Reactive routing (or on demand protocol)

It only operates when a mobile node wants to transmit data packet without knowing the proper path to the destination, such as Dynamic Source Routing (DSR), Zone Routing Protocol, and Ad hoc On-Demand Distance Vector Routing (AODV).Reactive protocols are better for environment with mobile nodes.

Advantage

Little consumption of bandwidth.

Disadvantage

Its drawback is due to the effort of path discovery. It must find a path to the destination before each transmission of packet. This mechanism increases the delay time between every transmission of packets.

3. AODV

AODV (Adhoc on demand distance vector routing protocol) is a reactive routing protocol for wireless adhoc networks. It uses on demand approach for finding routes that means a route is established only when it is required by a source node for transmitting data packets. In AODV the source node floods the route request packet in the network when route is not available for desired destination. It may obtain multiple routes to different destinations from a single route request. When an intermediate node receives a route request it either forwards or prepare route reply if it has route to destination. All intermediate node or destination nodes itself are allowed to send route reply packets to the source. AODV consists of two phases:

1. Route discovery
2. Route maintenance

Route discovery

The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the active route. Two types of control messages used for the discovery of route are as follows:
Route Request Message (RREQ) and
Route Reply Message (RREP)

and the sequence number of the source and destination. The BrID and the IP address pair is used to uniquely identify each request, the sequence numbers are used to determine the timeliness of each packet. Receiving nodes set the backward pointer to the source and generates a RREP unicast packet if it is the destination or contains a route to the destination with a sequence number greater than or equal to the destination sequence number contained in the original RREQ. As the RREP is routed back to the source, forward pointers are setup by the intermediate nodes in their routing tables.

Route maintenance

Route Error Message (RERR) is used to notify breakage of route. The neighborhood nodes are monitored. When an active route is lost, the neighborhood nodes are notified by route error message (RERR) on both sides of link.

Hello Messages

AODV uses hello messages to maintain the connectivity of neighboring nodes. The hello protocol yields a greater knowledge of the network and can improve the route discovery process. In AODV; HELLO messages are broadcasted in order to inform the neighbors about the activation of the link.

Example: AODV route discovery process

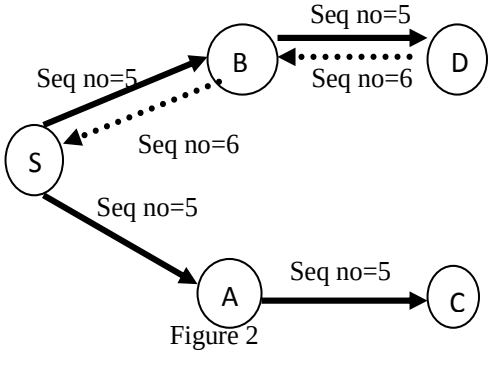

Figure 2

S-Source node — REEQ

D-Destination node — RREP

A, B, C-Intermediate nodes

Seq no=destination sequence no.

Figure 2 illustrates the example of route discovery process in AODV. First, the source node S sends a Route Request (RREQ) message using broadcasting in case where there is no route to destination node D.RREQ ID increases one every time node S sends a RREQ.Upon receiving the RREQ message, node A, B either :-

a) Reply RREP message to the source node if the node is the destination node or the node is an intermediate node with a 'fresh enough' route information to the destination. A route reply (RREP) message is generated and sent back to source if a node has route with sequence number greater than or equal to that of RREQ or

b) Update the routing table entry as the reverse path and rebroadcasting the RREQ message until the destination node or intermediate node with 'fresh enough route' is received the RREQ message with incremented hop count parameter.

They also judge that RREQ received is a repeated RREQ or not. If such RREQ is received, it will be discarded. When node D receives the RREQ, it sends a RREP to node S via node B. When node S receives the RREP, then a route is established. In case a node receives multiple RREPs, it will select a RREP whose the destination sequence number (Dst Seq) is the largest amongst all previously received RREPs. But if Dst Seq were same, it will select the RREP whose hop count is the smallest.

Example: Route maintenance process

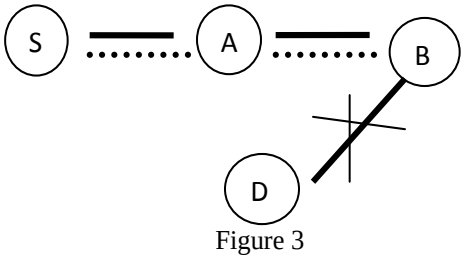

Figure 3

Route

RERR

In Figure 3, when node B detects disconnection of route, it generates Route Error (RERR) messages and puts the invalidated address of node D into list, then sends it to the node A. When node A receives the RERR,it refers to its route map and the current list of RERR messages. If there was a route to destination for

node D included in its map, and the next hop in the routing table is a neighboring node B, it invalidates the route and sends a RERR message to node S. In this way, the RERR message can be finally sent to the source node S.

4. Problem formulation:Blackhole attack in AODV

Ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network. Another classification of attacks is related to protocol stacks i.e. network layer attacks and blackhole attack is one of the network layer attacks. AODV suffers blackhole attack.

A black hole attack is a type of denial of service attack in which malicious node intercept all data packets being sent to the destination node. In this attack the malicious node listen to a route request packet in the network, and advertise the source node with claim of having most reliable link and an extremely short route to the destination node, even if it does not have any such route. As a result, the malicious node easily misroute network traffic to it and then drop the packets.

Example: Blackhole attack

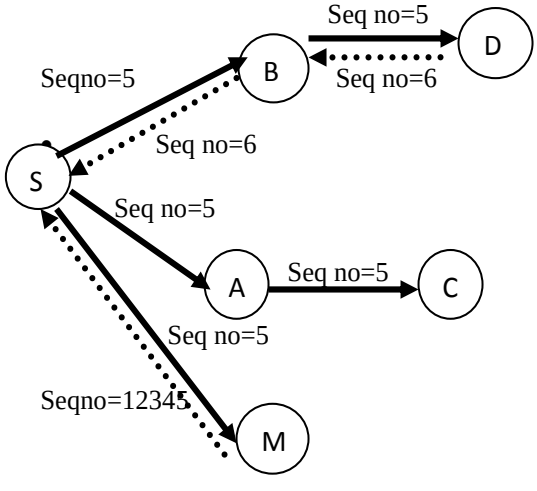

Figure 4

S-Source node — REEQ

D-Destination node ⋯◀ RREP

A, B, C-Intermediate nodes

M-Malicious node

Figure 4 shows example of blackhole attack in AODV.Source node S broadcasts a route request packet RREQ to its neighbors (A, B, M) to discover a route to the destination node D.The routing table of node B has a route to the destination node D and node M is the malicious node in the network.

When the node S sends a RREQ packet to its neighbors node B, node A and node M ,the malicious node M will not check its own routing table, and directly sends a fake RREP to node S, so the malicious node RREP reaches fastest to the node S as compare to the other nodes in the network. At this time node S accept the short route from the malicious node M and rejects the other RREP packets and sends data toward destination node along the opposite direction route of the malicious node RREP. Source node S believes that the data has been sent to destination node D, but data has been discarded by the malicious node M. A malicious node (performing a black hole attack) drops all data packets rather than forwarding them to the destination node D.As a result packet loss increases and throughput decreases.

5. Literature survey

In[1] authors analyzed the performance of adhoc network under blackhole attack which is one of the possible attacks on AODV routing protocol. Blackhole attack is simulated with the help of network simulator .(NS-2).The simulation results show the packet loss, throughput, and end-to-end delay with blackhole and without blackhole on AODV in MANET. It has beenanalyzed that the packet loss increases in the network with a blackhole node. Also it has been observed that the throughput and end to end delay decreases in the network with a blackhole node.

In[2] authors have done simulation study of blackhole attack in the mobile ad hoc networks. Due to security vulnerabilities of the routing protocols, wireless adhoc networks may be unprotected against attacks by the malicious nodes. In this study the effects of black hole attacks on the network performance is observed. The simulation of blackhole attacks on AODV (Ad hoc On Demand Distance Vector) routing protocol has been done with the help of Qualnet Simulator and the packet loss in the network with and without a blackhole is measured. The network performance in the presence of a blackhole is reduced

up to 26%.In this paper the effect of Packet Delivery Ratio,Throughput, End-to-End Delay and Jitter has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, End-to-End Delay, and Jitter.

In[3]authors have done behavioral Study of AODV with and without Blackhole Attack in MANET. The objective of this paper is to analyze the performance of ad-hoc routing protocol AODV with and without black hole attack in wireless network. The performance analysis is based on variation in speed of nodes in a network with 50 nodes. All simulation is carried out with QualNet 5.0 simulator. This paper presents an analysis of AODV routing with and without black hole attack in different scenario (in terms of throughput, total packets received, end-to-end delay, and jitter) in ad hoc network. By different analysis it has been observed that AODV performs better without presence of black hole attack in all situations. It has been observed that throughput of AODV rises; end to end delay goes down without presence of attack. It can be observed that performance of AODV without attack performs well in terms of packets received. It is observed that Avg. jitter effect in AODV without attack and AODV with attack changes by increasing or decreasing the pause time. The Jitter effect decreases as the pause time increases.

In[4] authors have done a survey on black hole attacks on AODV protocol in MANET .In this paper, authors surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks. This paper has analyzed various works related to black hole attack detection mechanism in AODV-based MANETs. The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every proposal has its own disadvantages in their respected solutions and made a comparison among the existed solutions. It has been observed that the mechanisms detects black hole node, but there is not any reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations.

In [5] authors analyzed the effect of Black Hole in AODV network. For this the black hole attack is simulated with the help of NS-2, it has been seen that The Black Hole Attack affects the overall network connectivity and causes data loss in network. Therefore to minimize the black hole effect, IDSAODV protocol is implemented .The IDSAODV protocol will improve packet delivery ratio and minimize the data loss. The advantage of this approach is that the implemented protocol does not make any modification in packet format and can work together with AODV protocol. Another advantage is that the proposed IDSAODV does not require any additional overhead and require minimum modification in AODV protocol.

In[6] performance of AODV is evaluated in presence of black hole attack (malicious node) and without black hole attack with CBR traffic under different scalable network mobility using NS-2 simulator. For this analysis RWP model is used. In this paper the performance of AODV with and without black hole (malicious node) attack has been analyzed under the circumstances of different parameters. Simulation results show, that when a node become as a malicious node it will effect on the AODV performance. The

route discovery process in the AODV is susceptible to black hole attack and therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

6. Proposed solution

AODV is a reactive routing protocol that is more vulnerable to blackhole attack due to lack of security. In future we will modify AODV routing protocol to enhance fault tolerance to blackhole attack in IEEE 802.11 based adhoc network. In AODV routing protocol there is one feature that intermediate nodes and destination node can send reply messages to source node. As black hole attack is caused by fake reply messages by intermediate (malicious) nodes. We will make AODV protocol more secure by modifying this feature of AODV protocol. Then we will compare the results of AODV protocol without blackhole attack, AODV protocol with blackhole attack and AODV protocol with blackhole attack but by modifying its feature.

7.References

[1].Bala,A.,Bansal,M.,Singh,J.(2009)"Performance Analysis of MANET under BlackholeAttack" In Proceedings of IEEE International Conference on Networks and Communications, NETCOM '09.,pp.141 - 145

[2].Sharma, Sheenu and Gupta, Roopam(2009)"Simulation study of blackhole attack in the mobile ad hoc networks", Journal of Engineering Science and Technology Vol. 4, No. 2 ,pp243 – 250

[3].Sharma, Arti and Jain, Satendra(2011) "A Behavioral Study of AODV with and without Blackhole Attack in MANET" International Journal of Modern Engineering Research (IJMER) Vol.1, Issue.2, pp-391-395

[4].Madhusudhananaga Kumar, K.S and Aghila,G (2011)"A Survey on Black Hole Attacks on AODV Protocol in MANET**",** International Journal of Computer Applications ,Vol 34– No.7

[5]Suryawanshi, Ranjeet and Tamhankar,Sunil (2012) "Performance Analysis And Minimization Of Black Hole Attack In MANET"International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4,pp.1430-1437

[6]Sushil kumar Chamoli , Kumar, Santosh, Deepak Singh Rana(2012) "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks"Int.J.Computer Technology and applications(IJCTA) Vol.3 issue 4,pp1395-1399