ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A Study of Security Flaws and Attacks on AODV Routing Protocol

A.Vani

Assistant Professor, Dept. of ECE, CBIT, Hyderabad, India

ABSTRACT: Many attacks in MANET target the particular routing protocols. This is caused by developing routing services without considering security issues. Most of the current research suffers from this problem. The AODV considered as the default routing protocol as it is presently going to be the acceptable standard for ad hoc network. So, herein most important attacks on AODV or major flaws of this protocol are described. It is to be known that it is not hard to transform similar type of attacks on other protocols, such as DSR. In this paper, security attacks on ad hoc on-demand distance-vector (AODV) routing protocol highlighted, which is on the verge of being the default routing standard for ad hoc network.

KEYWORDS: Security, Routing, Attacks, AODV, MANET.

I. INTRODUCTION

The Ad Hoc On-Demand Distance-Vector (AODV) routing protocol has designed is particularly for mobile ad hoc network. It provides very fast and efficient route establishment between communicating nodes. In majority of the protocols, the overhead is incurred by the fact that each transmitted packet contains the source route to the destination. AODV protocol eliminates this problem by maintaining only the next hop information to reach a particular destination.

Ad hoc on-Demand Distance-Vector Routing Protocol.

AODV routing protocol uses on-demand approach for discovering routes, that is, a route is established only when it is necessary by a source node for transmitting data packets [1]. It employs destination sequence number to identify the most recent path. AODV works on the router request (RREQ)/route reply (RREP) query cycle. Route request packet (RREQ) is sent from source to destination node when route does already not exist between them. AODV uses a destination sequence number (DestseqNum) to determine an updated path to destination. A node updates its path information when DestSeqNum of the current packet received is greater than the last destSeqnum stored at the node. In this protocol, a node unicast a RREP back to the source. If received RREQ is already processed, simply they remove the RREQ and do not forward it. The source node sends the data packets to the destination node after receiving the RREP. If source node later receives the RREP of greater sequence number or same sequence number with less hop count then the routing table is updated and uses the better route to destination. [9]

Path Discovery

When a node needs to communicate with another node but does not have the routing information, the source node then initiates the path discovery process. Every node maintains two counters [10]:

1. A node sequence number
2. A broadcast ID

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

The source node then broadcasts a route request (RREQ) packet to its neighbours as shown in fig.1. Each RREQ is uniquely identified by <IP address, Broadcast ID>. The value of broadcast ID is incremented every time a node issues a RREQ request.

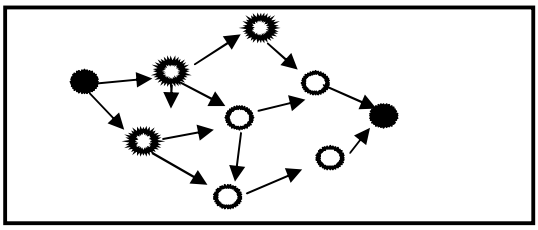

Figure: 1.Propagation of RREQ request

A node when receives a RREQ request have two options:
i. Sends a reply RREP back to the source
ii. Increments the value of hop count filed and rebroadcasts the RREQ to its neighbours

Action occurs under of the two conditions: either the node is the destination or the intermediate node knows the route to the destination of the RREQ (with equal or higher sequence number). It is possible for a node to obtain multiple copies of same RREQ packet. Duplicate packets are simply discarded or else, it records the following information that is used for reverse and forward path set up procedures discussed in the next sections

- Destination IP address
- Source IP address
- Broadcast ID address
- Expire Time for the reverse path route entry
- Sequence number of the source

Reverse Path Setup

The RREQ packet travels from the source to several intermediate nodes and finally reaches the destination. During the mean time a reverse path from all nodes to the requesting node (source) is established .To establish reverse path entry each intermediate node records the address of the neighbor node from which it got the first copy of the RREQ packet [10][11].

Forward Path Setup

After travelling some nodes, the RREQ packet will arrive at either destination node or any intermediate node. An intermediate node when first receives the RREQ checks its own routing table with destination specified in the packet. If so, it compares the destination sequence number with that of contained in the packet. If the packet's destination sequence number is larger than the sequence number in the local routing table the intermediate node will not respond to the RREQ. Then, it rebroadcasts the packet to its neighbors. The intermediate node can only respond when it has a route with a greater sequence number and if the packet has not been processed earlier. In order to reply, an intermediate node unicasts a route reply packet (RREP) back to its neighbor from which it got the packet [11]. The information of RREP packet is explained in the figure 2.

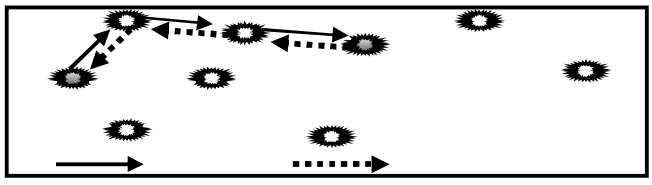

Figure: 2. Propagation of Route Information

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

When an intermediate node receives a RREP, it establishes a forward path entry to the destination in its routing table. The forward path entry contains the subsequent information:

- IP address of the destination
- The IP address of the neighbor where the RREP came
- The hop count to the destination

After processing the RREP, the node forwards the reply towards the source. It is explained in the fig 2. In addition, is possible for a node to get multiple copies of the same reply from different neighbors. It forwards the first replica of the request. It will process the next copy if that copy contains a greater sequence number or less hop count. Otherwise, the packet is discarded.

Route Maintenance

After the successful route discovery process, the route is maintained only if the source node requires it. Node movement is very common in ad hoc network environment. If it does not affect the discovered path, no action is taken by the protocol. If the source node moves during an active session, it reinitiates the route discovery process.

When the destination or any intermediate node moves a Route Error message (RERR) sent back to the corresponding nodes. The node that is closest to the source [11] initiates the error message.

Local Connectivity Management

Neighboring node information is maintained by periodically broadcasting message. Each time a node receives a broadcast from its neighbor it updates the lifetime for that node in the local routing table. If a node does not broadcast anything within the last hello interval, it then broadcasts a Hello packet to inform its neighbors to inform that it is still within its radio signal [10].

The main design issue of AODV protocol is to achieve efficiency in an ad hoc network environment. Expensive encryption is a feasible solution due to the energy-constraint property of the nodes participating in the network. In routing of packets, there are both mutable and immutable fields. Link to link encryption is unattainable for mutable fields like hop count and destination sequence number. Therefore, an attack can easily modify them and cause different security problems in routing.

II. SECURITY THREATS ON AODV ROUTING PROTOCOL

1. Traffic Redirection by Modification

Modification of Sequence Number and Hop Count:

In AODV protocol, a monotonically increasing sequence numbers to a particular destination maintains each route. Here any node may divert traffic through itself by advertising a better route to a destination, i.e. a sequence number better than the authenticated value. It could also cause DOS attack or a black hole attack [5].

In AODV protocol, attacker can set the value of hop count field to zero so that it can later include itself with the route. Alternatively, it can set the value to infinity to exclude from the route.

2. Replay Attacks

There are two types of replay attacks in ad hoc networks [2].

RREQ Flooding Attack

In AODV protocol when a node wants to communicate with another node but does not have the route information it broadcasts a RREQ packet in an incremental way, which is bounded by the value of TTL in the IP header. The objective is to reduce flooding overhead. If it fails to receive any route information then it increments the broadcast diameter by a predefined value, the procedure continues until a valid route discovered.

Each node maintains a sequence number and RREQ_ID to avoid the packets from being replayed. The higher the sequence numbers the fresher the information about the particular destination. It is easy to note that an attacker can record the RREQ of one node and circulate it to another area. If the new area is up-to-date, no harm is caused, as it

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

simply discards the packet. Though, the information of the nodes in the new area is not up-to-date it will cause extra unnecessary processing of packets which, in turns, causes a denial of service attack.

3. Wormhole Attack

It exploits the following two properties:

1. In AODV protocol when a node (source) needs to communicate with another ode (destination) but the source does not have the route, it broadcasts RREQ to its neighbors. The process continues until an immediate node having the fresh route to the destination is found (or the destination itself is found). To thwart unnecessary processing of same RREQ packet from different neighbors, each node processes the RREQ packets that first arrives and ignores other copies.
2. A direct (tunneling) link (wired/wireless) is faster than a general hop-by-hop propagation.

Usually it involves two attackers, one near the source and another near the destination. When a source broadcasts an RREQ packet, the first attacker records it and transmits directly through a tunnel to the second attacker (who is near the destination). Any neighbor of destination receives the RREQ from the attacker it normally processes. In the meantime, the original RREQ comes to it by hop-by-hop propagation, it simply discards it. Because, already it has received the packet.

This can cause DOS attack. In additional, it bounds the source and destination to use the attacker nodes.

False Route Error

After a route from a source S to a destination D has been established, the route is maintained only if it is needed by the source. If the source changes location, a new route discovery procedure is launched. When the destination or any intermediate node (i.e. any participating node of the route discovered) changes its location a route error message RERR sent back to the active nodes of the path.

3. Black hole Attack

The black hole attack is performed in two steps. On first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to relay itself as having a valid route to a destination node, although the route is unauthentic, with the intention of intercepting the packets. In second step, the attacker suppresses or modifies packets originating from several nodes, at the same time as leaving the data from the other nodes impervious. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. [7][8].

4. Requirements for a secure Routing protocol

By virtue of attacks presented, the lists of fundamental requisites of a secured routing protocol for MANET are; (1) Routing messages cannot be changed in transit, except according to the regular functionality. (2) Route signalling cannot be spoofed. (3) Fabricated routing messages cannot be injected into the network. (4) Routing loops cannot be created through malicious action.(5) Routes cannot be redirected from the shortest path through malicious action.(6) Unauthorized nodes should be excluded from route computation and discovery.(7) The network topology must not be exposed by the routing messages either to adversaries or to authorized nodes.[3][4]

III. CONCLUSION

Secure routing in the field of adhoc wireless networks is one of the most emerging areas of research. Designing a fool-proof security protocol for ad hoc routing is a challenging task from review of all, there is no mechanism (protocol) to detect the different attacks. The Ad-Hoc On-demand Distance vector (AODV) routing algorithm is a reactive algorithm that routes data across wireless mesh networks. The advantage of AODV is that it is easy, requires less memory and does not generate extra traffic for communication along existing links. With AODV; the attacker may advertise a route with a smaller distance metric than the original distance or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

REFERENCES

1. C.E.Perkins and E.M.Royer," Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999,pp.90-100.February 1999.
2. M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks". In proceedings of Workshop on Dependable Network Computing and Mobile system In Conjunction with 28th IEEEInternational Symposium on Reliable Distributed Systems:2009.
3. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network". Journal of Theoretical and Applied Information Technology JATIT-2009.
4. M.Zapata and N.Asokan .Securing ad hoc routing protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe02), pages1-10 September 2002.
5. B.Wu, J. Chen, J.Wu, and M. Cardei, A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, ser. Network Theory and Applications, Y. Xiao, X. Shen, and D. Z. D. (eds.), Eds. Springer, 2006, vol. 17.
6. D.Sreenivasa Rao, A.Vani,"Secure Routing Protocols for Wireless Ad hoc Networks",GITAM Journal of Information and Communication Technology,vol.1,No.1, july-December 2008,pp.143-148.
7. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, AbbasJamalipour, and Yoshiaki Nemoto. ―Detecting Black holeAttack on AODV based Mobile Ad hoc networks byDynamic Learning Method‖. International Journal ofNetwork Security, Vol.5, No.3, PP.338–346, Nov 2007.
8. C.Siva Ram Murthy and B.S.Manoj, A text book on Ad Hoc Wireless
9 .Charles E.Perkins and Elizabeth M. Royer."Ad-Hoc On-Demand Distance Vector Routing." In proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90-100, February 1999.
10 .Charles E. Perkins. AD Hoc Networking. Addison-Wesley. 2001.
11. E.M. Belding-Royer and C.K. Toh. A review of current routing protocols for adhoc mobile wireless networks. *IEEE Personal Communications Magazine*, pages 46-55, April 1999.