Secure and Effective Reactive Protocol for Mobile Adhoc Network-AODV

[1]Reema Gupta ,[2]Dr. Sukhvir Singh,[3]Pardeep Maan

[1]M.Tech Student, [2]Associate Professor, [3]Lecturer
NCCE,Israna (Panipat)
[1]Reema2405@gmail.com, [2]boora_s@yahoo.com, [3]pardeep.maan1@gmail.com

***Abstract* - Mobile Ad hoc networks are characterized by multi-hop wireless connectivity, frequently changing network topology and the need for efficient dynamic routing protocols. There are many existing protocols for ad-hoc network that can generally be categorized into pro-active and re-active protocols types. In Reactive we will discuss about AODV [2,3,4](Ad Hoc on-Demand Distance Vector Routing) protocol. AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. An important feature of AODV is the maintenance of time based states in all nodes. For the route discovery the control packets are used: Route Request (RREQ), Route Reply (RREP), Route Error (RERR).This paper is an effort to provide overview and working of the AODV protocol.**

***Index Terms* – MANET, Proactive, Reactive, AODV, RREQ, RREP, Vunerabilites**

I. Introduction

MANET protocols are typically categorized as either proactive or on-demand (reactive). Proactive MANET protocols update routing information in a proactive manner by exchanging route information at periodic intervals. The exchange of Table-based route information is evenly distributed across the wireless network. As a result, routes are established prior to being needed, providing a wireless network that is low in latency, at the expense of increased overhead. Rather than distribute all route information across the entire network, MANET protocols perform route maintenance only when required. On-demand protocols create less network overhead since the exchange of routing information is localized rather than evenly distributed. The result is a network with less overhead, at the expense of increased latency due to the route discovery process. Numerous MANET protocols exist; yet, very few have been implemented outside of the research community. Some of the better known MANET protocols are AODV, TORA, DSR and OLSR. Each protocol has evolved over time to better suit the particular requirements of various types of mobile ad hoc networks.

Mobile adhoc networks due to their dynamic nature suffer with frequent and unpredictable topology changes [4], moreover, in them not only limited network bandwidth is available but also in most of the cases mobile devices are operated on limited battery power. These all issues make Routing problem an interesting challenge of this area. This paper is organised into many sections. Section II describes Overview of Adhoc protocols-proactive and reactive protocols. Section III describes the working of AODV(Adhoc On-Demand Distance Vector protocol).Section IV describes Vulnerabilities in AODV and Section V describes Security requirement in AODV.

Overview of Adhoc Network Protocols

Adhoc Network Protocols are broadly divided into two categories: - one is table driven (Proactive protocol) and On-demand (reactive protocol). In Proactive Routing protocols, each node maintains up-to-date routing information to every other node in the network. Routing information is kept in a number of routing tables and updates to these tables are periodically transmitted throughout the network to maintain table consistency. Thus, in proactive routing, routes can be quickly established without any delay. However, it requires a significant amount of resources to keep routing information up-to-date. Table is maintained for every route from one node to other. Reactive or On-demand routing Protocols are designed to overcome the increased overhead problem in proactive protocols. Unlike proactive protocols, Reactive protocols create a route only when desired. If a node desires to send a message to a destination node for which it does not have a valid route to, it initiates a route discovery to locate the destination node. The process is completed when a source node finds a route to the destination. A route Maintenance procedure is implemented to maintain a route until the destination is no longer available or not desired. Even though reactive protocols overcome increased overhead problem, but they exhibit end-to-end delay since routes are created on demand.

II. AODV Protocol

AODV is a reactive protocol[8], i.e. it creates route on-demand, as requires. When a source node needs a route to some destination node, it broadcasts a route request message to its neighbours including the last known sequence number for that destination. Each node that forwards the route request creates a reverse route for itself back to the source node. When the route request reaches a node with a route to destination node that node generates a route reply that contains the number of hops necessary to reach destination and the sequence number for destination most recently seen by the node generating the REPLY. The state created in each node along the path from source to the destination is hop-by-hop state that is each node remembers only the next hop and not the entire route, as would be done in source routing. Even though reactive protocols overcome increased overhead problem, but they exhibit end-to-end delay since routes are created on demand. AODV is designed for use in networks Where the nodes can all trust each other, either by use of preconfigured keys. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV.

Route Discovery [1]

On-Demand protocols employ a route discovery procedure, by which a source node discovers a route to a destination, for which it does not already have a route in its cache. The process broadcasts a ROUTE REQUEST packet, which is flooded across the network. In addition to the source node address and target node address, the request packet contains a route record, which records the sequence of hops taken by the request packet as it propagates through the network. RREQ packets use sequence numbers to prevent duplication. The request is answered by a ROUTE REPLY packet either from the destination node or an intermediate node that has a cached route to the destination.

Type	FLAG	RESERVED	HOP COUNT
RREQ ID			
DESTINATION IP ADDRESS			
DESTINATION SEQUENCE NUMBER			
ORIGINATOR IP ADDRESS			
ORIGINATOR SEQUENCE NUMBER			

Fig 1 RREQ Message Format

Route Reply

The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.

Type	FLAG	RESERVED	HOP COUNT
DESTINATION IP ADDRESS			
DESTINATION SEQUENCE NUMBER			
ORIGINATOR IP ADDRESS			
LIFETIME			

Fig 2 RREP Message Format

Every neighbor that receives the RREQ, either:

1. Returns a route reply packet (if route information about destination in its cache), or
2. Forwards the RREQ to its neighbors (if route information about destination not in its cache).

If a node cannot respond to the RREQ, the node increment the hop count, saves information to implement a reverse path set up. The information that are saved are: neighbor that sent the RREQ packet, destination IP address, source IP address, broadcast ID, source node's sequence number and expiration time for reverse path entry.

Route Error (RERR)

Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR[6,7] message indicates those destinations (possibly subnets) which are no longer reachable by way of the broken link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination. The information in the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to a node in a precursor list.

Type	FLAG	RESERVED	DESTCOUNT
UNREACHABLE DESTINATION IP ADDRESS			
UNREACHABLE DESTINATION SEQUENCE NUMBER			

Fig 3 RERR Message Format

The RERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbors.

Route Reply Acknowledgment (RREP-ACK)

The Route Reply Acknowledgment (RREP-ACK) message must be sent in response to a RREP[6] message with the 'A' bit set.This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle.

TYPE	RESERVED

Fig 4 RREP-ACK Message Format

Route Maintenance

On-Demand protocols also employ a route maintenance procedure, where nodes monitor the operation of the route and inform the sender of any routing error. If a route breaks due to a link failure, the detecting host sends a ROUTE ERROR packet to the source, which upon receiving it, removes all routes in its cache that use the hop in error and initiates a new route discovery process. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all routes. The protocol is based on two phases, route discovery and route maintenance. A node does not perform route discovery or maintenance until it needs a route to another node or it offer its services as an intermediate node.

Route changes can be detected by failure of periodic HELLO Packets, failure or disconnect indication from the link level, or failure of transmission of a packet to the next hop (can detect by listening for the retransmission if it is not the final Destination). The upstream (toward the source) node detecting a failure propagates a route error (RERR) packet to the source. The source (or another node on the path) can rebuild a path by Sending a new RREQ packet.

Route Table Entries

When a node receives an AODV control packet from a neighbor, or creates or updates a route for a particular destination or subnet, it checks its route table for an entry for the destination. In the event that there is no corresponding entry for that destination, an entry is created. The sequence number is either determined from the information contained in the control packet, or else the valid sequence number field is set to false. The route is only updated if the new sequence number is either

1. Higher than the destination sequence number in the route table, or
2. the sequence numbers are equal, but the hop count (of the new information) plus one, is smaller than the existing hop count in the routing table, or
3. The sequence number is unknown.

Generating Route Replies

A node generates a RREP if either:

1. It is itself the destination, or
2. It has an active route to the destination, the Destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the Destination Sequence Number of the RREQ.

Generating Route Error

A node initiates processing for a RERR message in three situations:

1. If it detects a link break for the next hop of an active route in its routing table while transmitting data (and route repair, if attempted, was unsuccessful), or
2. If it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or
3. If it receives a RERR from a neighbor for one or more active routes.

III. Vulnerabilities[3] In AODV

1. **Deceptive incrementing of Sequence Numbers**

   Destination Sequence numbers determine the freshness of a route. The destination sequence numbers maintained by different nodes are only update when a newer control packet is received with a higher sequence number. However, a malicious node can increase this number in order to advertise fresher route to a particular destination.
2. **Deceptive decrementing of Hop Count**

   AODV prefers route freshness over route length. A node would prefer a control packet with a larger destination sequence number and hop count over a control packet with a smaller destination sequence number and hop count. However, in case where the destination sequence numbers are same for two control packets, the route with the smaller hop count is chosen. A malicious node can easily exploit this mechanism by decrementing the Hop Count to generate fallacious smaller routes to destination.

IV. Security requirement of AODV

1. *Source authentication:* The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.
2. *Neighbor authentication:* The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.
3. *Message integrity:* The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.
4. *Access control:* It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

.

V. Conclusion

This paper concludes that due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. MANET is growing field and have various protocols used for transfer packet from one node to other. AODV is most efficient ,reactive protocol that uses RREQ,RREP,RERR,RREP-ACK messages used in AODV for route discovery.Further, MANET requires more security against attacks as compared to wired networks.

References

[1] "Study and Design of New Reactive Routing Protocol Advance AODV for Mobile Ad hoc Networks" Anurag Porwal1, B.L.Pal2, Rohit Maheshwari3, Gaurav Kakhani4

[2] "Routing protocols for mobile ad hoc networks" Humayun Bakht

[3] "Secure Routing with AODV Protocol for Mobile Ad Hoc Networks"Tahira Farid_ and Anitha Prahladachar

[4] " Mobile Ad hoc Networking (MANET) with AODV Revision 1.0" White Paper

[5] "A Performance Comparison of Routing Protocols for adhoc networks"Azzedine Boukerche.

[6] "Survey of Routing Protocols for Mobile Ad-hoc Network" Taitec College Manchester , United Kingdom

[7] "Ad-Hoc On Demand Distance Vector Routing" Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)

[8] "*AODV Routing Protocol Implementation Design*" Ian D. Chakeres and Elizabeth M.Belding-Royer.