SECURITY STUDY OF AODV FOR MANETS

Bhavik Patel*

Abstract—

MANETs routing protocols are being developed without having security in mind. In most of them it is assumed that all the nodes in the network are friendly and trusted. I consider the problem of incorporating security mechanism into routing protocols for ad hoc networks. I look at AODV (Ah-hoc On-demand Distance Vector) in detail and try to check possibility to develop a security mechanism to protect its routing information.

AODV is one of the widely used routing protocols that is currently undergoing extensive research and development. AODV is reactive which means that it builds routes only when they are first needed. AODV is based on distance vector routing, but the updates are shared not on a periodic basis but on an as per requirement basis. The control packet contains a hop count and sequence number field that identifies the freshness of routing updates. As these fields are mutable, it creates a potential vulnerability that is frequently exploited by malicious nodes to advertise better routes. Similarly, transmission of routing updates also discloses vital information about network topology, which is again a potential security hazard. So here I will try to focus first on various possible security flaws and then on possible security solutions of AODV.

Keywords— MANET, Security, AODV, Ad-hoc

* 3rd Sem M. E. Computer Science & Engineering PG Student, GTU, Ahmedabad

I. INTRODUCTION TO AODV

Ad-hoc On-Demand Distance Vector (AODV) is inherently a distance vector routing protocol that has been optimized for ad-hoc wireless networks. It is an on demand protocol as it finds the routes only when required and is hence also reactive in nature. AODV borrows basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. To avoid the problem of routing loops, AODV makes extensive use of sequence numbers in control packets. When a source node intends communicating with a destination node whose route is not known, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains an ID, source and the destination node IP addresses and sequence numbers together with a hop count and control flags. The ID field uniquely identifies the RREQ packet; the sequence numbers inform regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Each recipient of the RREQ packet that has not seen the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain interval of time. When the RREQ packet reaches the destination node or any node that has a fresher route to the destination a RREP (Route Reply) packet is generated and unicasted back to the source of the RREQ packet. Each RREP packet contains the destination sequence number, the source and the destination IP addresses, route lifetime together with a hop count and control flags. Each intermediate node that receives the RREP packet, increments the hop count, establishes a FORWARD ROUTE to the source of the packet and transmits the packet on the REVERSE ROUTE. For preserving connectivity information, AODV makes use of periodic HELLO messages to detect link breakages to nodes that it considers as its immediate neighbors. In case a link break is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route. Optionally, a Route Reply Acknowledgement (RREP-ACK) message may be sent by the originator of the RREQ to acknowledge the receipt of the RREP. RREP-ACK message has no mutable information.

II. AODV MESSAGE FORMATS

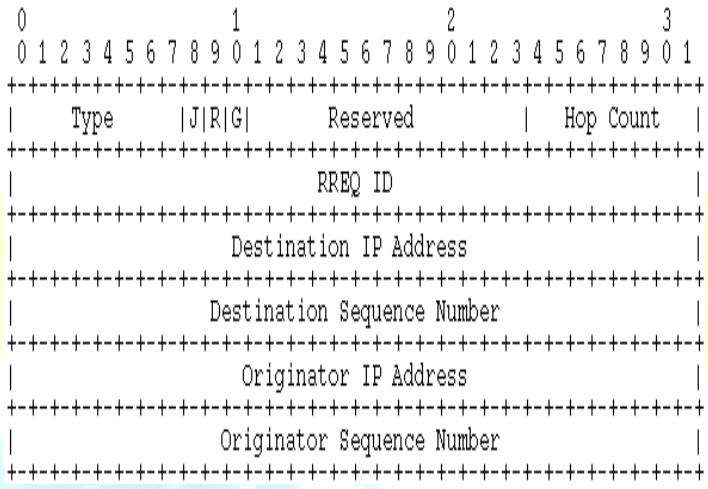

Figure 1: Route Request (RREQ) Message Format

Mutable fields: Hop Count

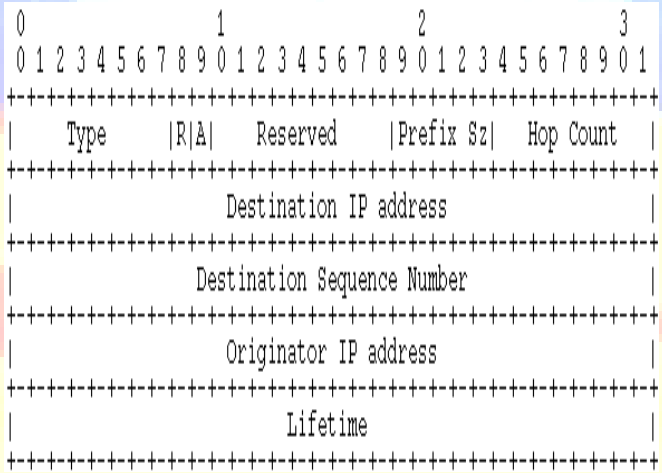

Figure 2: Route Reply (RREP) Message Format

Mutable fields: Hop Count

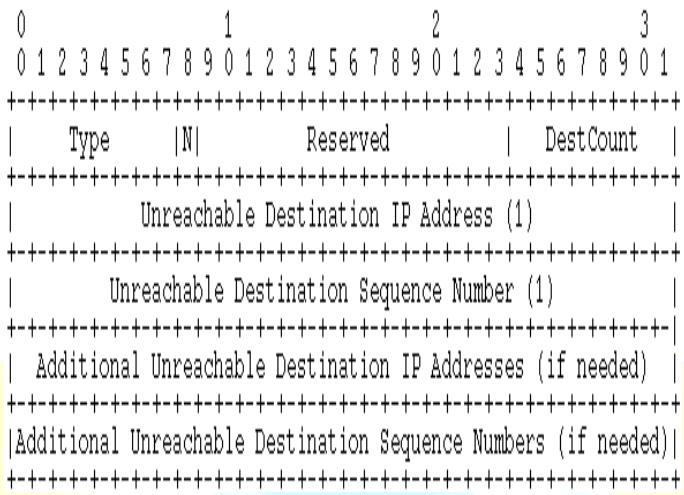

Figure 3: Route Error (RERR) Message Format

Mutable fields: None

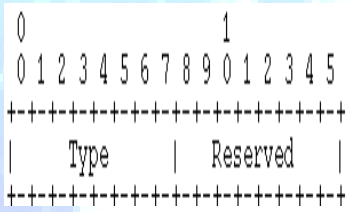

Figure 4: Route Reply Acknowledgment (RREP-ACK) Message Format

Mutable fields: None

III. SECURITY FLAWS OF AODV

The The major vulnerabilities present in the AODV are:

(i) Deceptive incrementing of sequence numbers and

(ii) Deceptive decrementing of hop-count.

Actually there are seven main requirements to secure AODV protocol properly.

A. Authorized nodes to perform route computation and discovery

B. Minimal exposure of network topology

C. Detection of spoofed routing messages

D. Detection of fabricated routing messages

E. Detection of altered routing messages

F. Avoiding formation of routing loops

G. Prevent redirection of routes from shortest paths

Moreover since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out the following attacks (among many others) against AODV:

1. Impersonate a node S by forging a RREQ with its address as the originator address.
2. When forwarding a RREQ enervated by S to discover a route to D, reduce the hop count field to increase the chances of being in the route path between S and D so it can analyze the communication between them.
3. Impersonate a node D by forging a RREP with its address as a destination address.
4. Impersonate a node by forging a RREP that claims that the node is the destination and, to increase the impact of the attack, claims to be a network leader of the subnet SN with a big sequence number and send it to its neighbors.
5. Electively, not forward certain RREQs and RREPs, not reply to certain RREPs and not forward certain data messages

IV. SECURING AODV

We assume that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. How this is achieved depends on the key management scheme.

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. The figures given above show the structure of the AODV messages and indicate what the mutable fields of the messages are.

In short, securing the AODV protocol can be divided into the following three broad categories: 1) Key Exchange, 2) Secure Routing and 3) Data Protection

V. CONCLUSIONS

AODV is being developed without having security in mind. Because of that there are many security flaws inside AODV have been observed. So there is a solid need to improve AODV by adding security extensions using key management, digital signature, hash chains etc.

FUTURE WORK

- Study of available secure versions of AODV.
- Try to find major problems in existing secure versions of AODV

REFERENCES

[1] [1] Manel Zapata, N. Asokan, "Securing Ad hoc Routing Protocols" (2002) ACM

[2] [2] Pirzada, McDonald, "Security Routing with the AODV Protocol" (2005) IEEE pp.57-61

[3] [3]Kullberg "Performance of the Ad hoc On demand Distance Vector Routing Protocol"