Research Inventy: International Journal Of Engineering And Science
Issn: 2278-4721, Vol. 2, Issue 3 (February 2013), Pp 27-29
Www.Researchinventy.Com

Adhoc on Demand Distance Vector Routing Protocol: A Review Study

[1,]Dr.A.A.Gurjar, [2], Mr.A.A.Dande
[1,]*Department Of Electronics & Telecommunication Sipna's C.O.E.T, Amravati*
[2,]*Second Year (M.E.), Computer Engineering Sipna's C.O.E.T, Amravati*

Abstract: *AODV Is Source Initiated A Routing Protocol. AODV Protocols Are Different From Traditional Proactive Protocols Since In Proactive The Routing Mechanism Is Based On Periodic Updates This Leads To High Routing Overhead. The Key Goal In Designing This Protocol Is To Reduce Overhead. Routing Messages In AODV Can Be Divided Into Path Discovery And Path Maintenance Messages. Path Discovery Includes The Route Request (RREQ) And The Route Reply (RREP), While The Latter Includes Route Error (RERR) And Hello Message. In AODV No Routing Structure Is Created Prior.*

Key Words: *Adhoc Network, Routing protocol, Flooding, Broadcasting, Active Route*

I Introduction

The route discovery process of AODV consists of two key methods. First one it is source routing. Second one is backward learning. Since this protocol uses the concept of periodic updates it is adapted to network dynamics. Source initiated means source floods the network with a route request packet when a route is required for a destination. The flooding is propagated outwards from the source. The flooding transmits the request only once. On receiving the request from the source node the destination replies to the request if it has the valid path. Reply from destination uses reversed the path of the route request. Since the route reply is forwarded via the reverse path which forms a forward path. Thus it uses forward paths to route data packets. AODV protocol uses hop-by-hop routing. That is each node forwards the request only once. In the meanwhile unused paths expire based on timer. AODV uses the concept of optimization that is any intermediate nodes can reply to route request if it has valid path which makes the protocol to work faster. But the major problem with optimization causes loops in the presence of link failure. Each node maintains sequence number. It acts as a timestamp. The most interesting feature of the sequence number is, it signifies the freshness of the route.

II Working Of AODV Protocol In Detail.

Whenever a source node wants to communicate, it broadcasts a Route Request (RREQ) message for the specified destination. Intermediate nodes forwards message towards the destination. For example in following Figure the source node S floods the RREQ (Route request) in the network. Each node in the network checks its own routing table and checks whether it is the destination or it has a route to the destination.

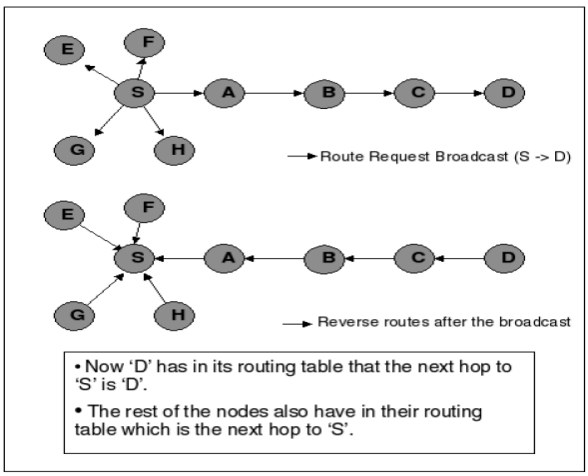

Figure: AODV route discovery using RREQ packet.

Simultaneously reverse path is set up along the way which it forwards the packets. RREQ message contains broadcast id; destination IP address; destination sequence number; source IP address; source sequence number; hop count. If it is not the destination node the nodes forward the packets. In above figure node A is not destination node, so node A again broadcasts the packets in the network. Finally when the node D receives the broadcasted message it confirms that it is the destination node and uses the reverse route to reply node D. The simple idea behind this routing is flooding done with the nodes in the network. Not only that each node forwards the request only once. Each node in the communication path maintains a sequence number which also act as a timestamp. The timestamp gets incremented whenever it starts sending any message or participates in the communication. Each route from source S also has a sequence number associated with it. Sequence number signifies the freshness of the route. The node which has highest sequence number specifies up-to-date information about routing. Intermediate node reply only when it has the highest sequence number instead of forwarding the message.

The following Figure illustrates the route reply (RREP) concept in detail.

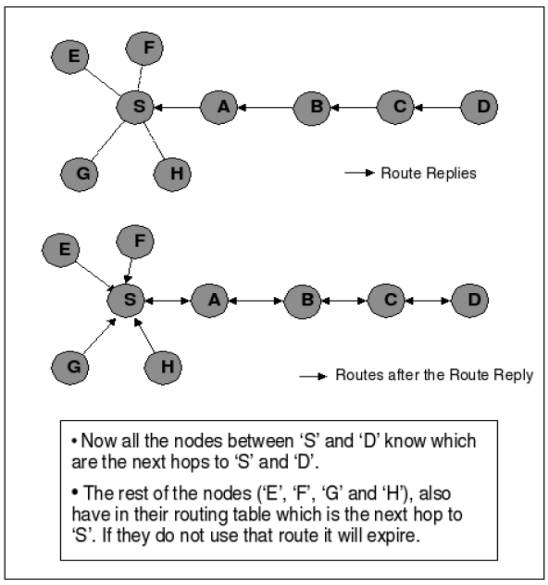

Figure: Route Discovery using RREP packet.

When node D receives a RREQ packet and it confirms that it has a current route to the target source S using routing table. After this process the node D unicasts a route reply (RREP) packet to the reverse path which it received the RREQ packet early. The unused path expires based on the timer. Thus the destination node D starts forwarding and receiving packets with source node S using the reverse path in the networks.

III Hello Messages And Route Table Information.

A node may offer connectivity information by broadcasting local Hellos messages. A node should only use hello messages if it is part of an active route. In every hello message interval, the node checks whether is has sent a broadcast within last hello message interval. If it has not, it may broadcast a RREP with TTL field equal to 1 called a Hello message. In addition to the source and destination sequence numbers, other useful information is also stored in the route table entries. Associated with reverse path routing entries is a timer, called the route request expiration timer. The purpose of this timer is to purge reverse path routing entries from those nodes that do not lie on the path from the source to the destination. The expiration time depends upon the size of the ad hoc network. Another important parameter associated with routing entries is the route caching timeout, or the time after which the route is considered to be invalid. In each routing table entry, the address of active neighbors through which packets for the given destination are received is also maintained. A neighbor is considered active for particular destination if it originates or relays at least one packet for that destination within the most recent active timeout period. This information is maintained so that all active source nodes can be notified when a link along a path to the destination breaks. A route entry is considered active if it is in use by any active neighbors. The path from a source to a destination, which is followed by packets along active route entries, is called an active path. A mobile node maintains a route table entry for each destination of interest. Each route table entry contains the information such as Destination IP Address, Destination Sequence Number, Valid Destination Sequence Number flag, Other state and routing flags, Network interface, Hop Count.

IV Route Error Messages And Route Expiration

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 message indicates those destinations 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 user it as a next hop towards each destination. The information the precursor lists is most easily acquired during the processing for generation of a RREP message, which by definition has to be sent to anode in a precursor list. Generally, route error and link breakage processing requires the following steps such as Invalidating existing routes, Listing affected destinations, Determination which, if any, neighbors may be affected, Delivering an appropriate RERR to such neighbors.A Route error (RERR) message may be broadcast, unicast, or iteratively unicast to all precursors. Even when the RERR message is iteratively unicast to several precursors, it is considered to be single control message for the purposes of the description in the text that follows. With that understanding, a node should not generate more that a RERR rate limit message per unit time. The RERR message format has been shown in the following figure.

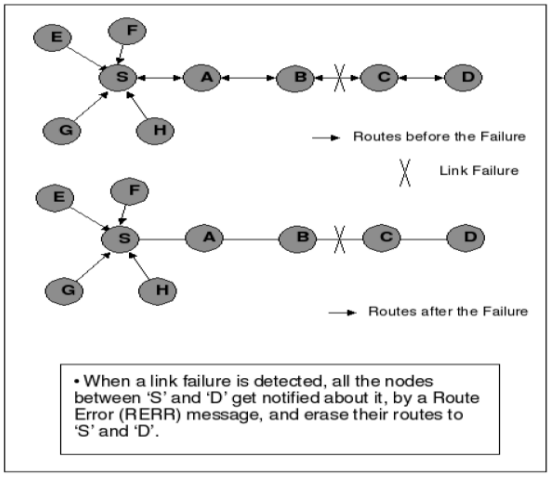

Figure: AODV routing protocol with route error message.

Within the limits imposed by worst-case route establishment latency as determined by the network diameter, AODV is an excellent choice for ad-hoc network establishment. It is useful in applications for emergency services, conferencing, battlefield communications, and community-based networking.

V Conclusion

AODV reduces memory requirements and needless duplications of packets to be transmitted in MANETs to a very considerable extent. It also has quick response to link breakage in active routes so it is effective and highly preferable. The most important feature that, it has loop-free routes maintained by the use of destination sequence numbers and can be scaled to large population of nodes in the network.

VI References

[1] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.
[2] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.
[3] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.
[4] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad-Hoc Networks"
[5] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-Hoc Networks," ACM Southeast Regional Conf. 2004."
[6] Akanksha Saini, and Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET", International Journal of Computer Science and Technology, Vol.1, issue 2, Dec 2010
[7] Shree Murthy and J. J. Garcia-Luna-Aceves. "An Efficient Routing Protocol for Wireless Networks". Mobile Networks and Applications, 1(2):183–197, 1996.
[8] C. E. Perkins and E. M. Royer, "The Ad Hoc On-Demand Distance Vector Protocol", Ad hoc Networking, Addison-Wesley, 2000, pp. 173-219.
[9] Elizabeth M. Royer, C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks".