Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.219 – 224

REVIEW ARTICLE

Study of Flat - Reactive On-Demand Routing Protocol (DSR & AODV): A Review

Atul D.Atalkar
Second Year(III[rd] SEM), M.E (EXTC), ARMIET, Sapgaon,Thane.Dist.,M.H.
atul_atalkar@rediffmail.com

Prof. Prashant S.Wankhade
M.E (ELEX), DMCE, Airoli, Navi Mumbai. Dist. M.H
prashant6929@gmail.com

Abstract— Mobile Ad-Hoc Network is a collection of mobile node, which communicates with each other to share information among them. Each node acts as a router itself. They are freely to move and change their position within a network and arrange themselves share all resources with each other. But to share information a routing protocol is needed. Routing protocol plays an important role in network design and provides the simplicity, decision rights to network, which will increase the performance of network in various aspects. Like packet delivery ratio, packet delay, throughput, best route path, etc.
Keywords- MANET, DSR, AODV, PDF

*****

I. INTRODUCTION

Mobile ad-hoc network is collection of mobile nodes, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.
Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multi-hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions. MANETs are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network.

A. Characteristics of a MANET:

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes
Almost all the nodes in an ad hoc network rely on batteries or other exhaustive means for their energy. The battery depletes due to extra work performed by the node in order to survive the network. Therefore, energy conservation is an important design optimization criterion.

Wireless links have significantly lower capacity than infrastructures networks. Throughput of wireless communication is much less because of the effect of the multiple access, fading, noise, interference conditions. As a result of this, congestion becomes a bottleneck in bandwidth utilization.
MANETs are generally more prone to physical security threats than wireless networks because the ad hoc network is a distributed system and all the security threats relevant to such a system are pretty much present, as a result, there is an increased possibility of eavesdropping, spoofing, masquerading, and denial-of-service type attacks**.** Due to all these reason traditional routing protocols are not suitable for MANET.

B. MANET Protocols:
The network topology of ad hoc networks is unstable and changes frequently with nodes mobility, traditional routing protocols in static network are not efficient for ad hoc networks. Routing protocols for ad hoc networks can be classified broadly as either proactive, reactive and hybrid.
Proactive protocols continuously exchange network topology information so as to constantly monitor topology changes and use that knowledge for efficient, low latency. Common proactive routing protocols include Dynamic Destination- Sequenced Distance- Vector Routing (DSDV), Optimized Link State Routing (OLSR).
Reactive protocols were introduced to remedy. Where nodes react only on demand to data transmission and perform path finding operations only when needed. The most common reactive protocol includes **Ad hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR)**

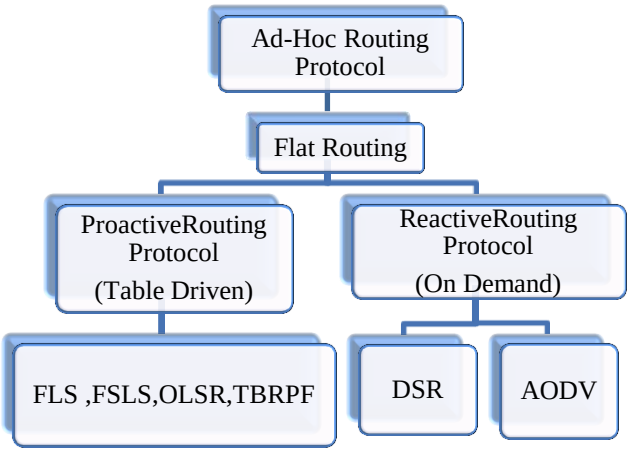

fig. a. Classification of MANET Routing Protocol

Types of Protocol

1. Proactive (Table-Driven) Routing
In proactive or table-driven routing protocols, each node consistently maintains up-to-date routing information for all known destinations. These types of protocols keep routing information in one or more tables and maintain routes at each node by periodically distributing routing tables (RTs) throughout the network or when the topology changes. Each node keeps information of all the routes, regardless of whether or not these routes are needed. Therefore, control overhead in these protocols would be significantly high, especially for large networks or in a network where nodes are highly mobile. However, the main advantage of these protocols is that the routes are readily available when required and end-to-end delay is reduced during data transmission in comparison to the case in which routes are determined reactively, which introduces a latency to discover a route to the destination.

2. Reactive (On-Demand) Routing.
In Reactive or on-demand routing protocols, the routes are discovered only when they are actually needed. These protocols consist of route discovery and route maintenance processes. The route discovery process is initiated when a node wants to send data to a particular destination. Route discovery usually occurs by flooding the network with route-request packets. When a destination node or node holding a route to destination is reached, a route-reply is sent back to the source node by instantiating routing information at the appropriate intermediate nodes. Once the route reply reaches the source, the data can be sent to the destination. The route maintenance process deletes failed routes and re-initiates route discovery in case of topology change. The advantage of this approach is that overall overhead is likely to be reduced compared to proactive approaches. However, as the number of sessions increases, the overhead generated by route discovery became high and may exceed that of proactive protocols. Examples of reactive routing protocols are the dynamic source **Routing (DSR), & Ad hoc on-demand distance vector routing (AODV)**

3. Hybrid Routing

The hybrid routing protocols combine the advantages of both proactive and reactive routing. These protocols usually divide the network in zones such that each node sees the network in number of zones. The routes to nodes close to each other or within a particular zone are proactively maintained and the routes to far-away nodes are determined reactively using a route discovery strategy.

C. Routing Protocol:

DSR (Dynamic Source Routing)

Dynamic Source Routing (DSR) is an on demand source routing protocol in MANET. On demand source routing protocol execute path finding process. When path is required by a node. Dynamic source routing is a representative on demand protocol designed to restrict the bandwidth consumed by control packet in ad-hoc wireless network. Dynamic source Routing .In DSR, when a source S wants to send message(s) to a destination D, S initiates the route discovery process. S generates a route request (RREQ) message and broadcasts it to it's the neighbors. A RREQ message has unique request identifier and a record field. The purpose of the record field (initially empty) is to record the ids of the intermediate nodes from source to destination. When a node receives RREQ message, it first checks is it the intended destination or does it have a route to destination D in its cache. If so, it returns back a route reply (RREP) message to source. Otherwise it appends its identifier to the RREQ packet and rebroadcasts it. RREQ packet is rebroadcasted, until it reaches to destination D. When D receives RREQ packet, it generates a RREP message and sends back to S via the path obtained by reversing the order of nodes in route list. Thus a path is established between S and D.

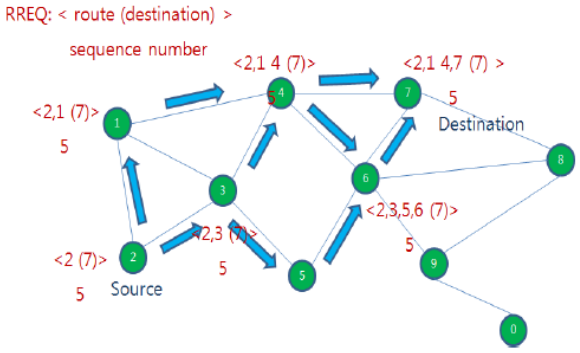

Fig. b. RREQ Propagation

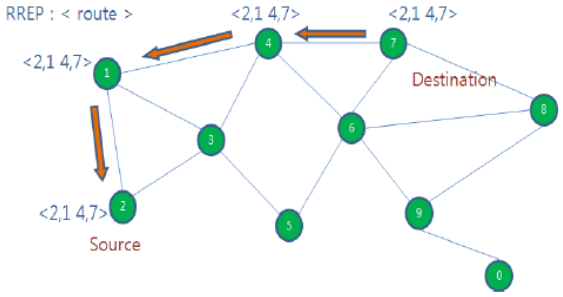

Fig. c. RREP Propagation

node cannot deliver a packet to the next node over the chosen route due to link break or any other reason, it u Whenever unicasts a route error (RERR) message back to the source. Due to open medium and multi hop scenario, an attacker can easily capture the packet or inject the forge route control message in network. The success of DSR Protocol depends on the assumption that all the nodes are cooperative. An attacker can exploit this assumption and may advertise malicious routing information such as it has less number of hops to the destination known as Black Hole attack. Another attack malicious node can broadcast a forge route request (RREQ) packet to jam the network, if there is no authentication. An attacker can perform denial of service (DOS) attack by flooding several wastage packets into networks. Furthermore, attacker can inject, drop or modify the packets in between source and destination nodes. Many of the security solutions to secure the routing in MANETs have been proposed. These protocols are vulnerable either to active attack or passive attack. In propose work a secure protocol that authenticates source, destination and intermediate nodes that make up the route from source to destination. MAC function provides the message integrity and confidentiality can be achieved by message encryption.

AODV (Ad-hoc On-Demand Distance Vector Routing Protocol)

It is an on-demand distance-vector routing protocol. When a destination node demand for route AODV establish it.AODV is compatible with both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. Additionally, the sequence numbers are used by AODV uses the sequence numbers updated routes entries. It is loop-free, self-starting, and scales to large numbers of mobile nodes. There are three types of control messages for route maintenance in AODV.
RREQ- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_ id. The RREQ contains the following field.

Source Address	**Broadcast ID**	**Source Sequence No.**	**Destination Address**	**Destination Sequence No**	**Hop Count**

The pair <source address, broadcast ID> uniquely identifies a
RREQ. Broadcast ID is incremented whenever the source issues a new RREQ. RREP- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator. ERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ―precursor list", containing the IP address for each its neighbours that are likely to use it as a next hop towards each destination.

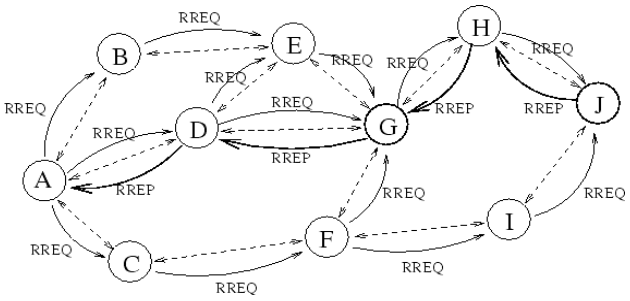

Fig. d. AODV route lookup session

The above Figure illustrates an AODV route lookup session.
Node A wants to initiate traffic to node J for which it has no route. A transmit of a RREQ has been done, which is flooded to all nodes in the network. When this request is forwarded to J from H, J generates a RREP. This RREP is then unicast back to A using the cached entries in nodes H, G and D.AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node getting the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicast a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

D. Comparison of DSR & AODV:
DSR and AODV can be compared on the following points

1. Multicast Route: Multicast Route is supported by DSR where as AODV will not.
2. Route Maintain: Route is maintained in DSR in the form of Route Cache; where as in AODV Route is maintained in Route Table.
3. Unidirectional link Support: DSR Support unidirectional Link, where as AODV will Not.

4. Periodic Broadcast: DSR will not periodically broadcast information, where as AODV will broadcast information.
5. Routing Overhead: DSR has less routing overhead than AODV.
6. Normalized MAC Overhead: AODV has less normalized MAC overhead than DSR
7. Routing Mechanism: DSR is based on a source routing mechanism whereas AODV uses a combination of DSR and DSDV mechanisms.
8. Performance: AODV has better performance than DSR in higher-mobility scenarios
9. Route Discovery: DSR has less frequent route discovery processes than AODV**.**

CONCLUSION

It is very difficult to compare & comes on result, that witch reactive protocol is best for our network. Both DSR & AODV protocol having their own properties, advantages & disadvantages. Depending upon the structure of network, location of network, traffic, and no of nodes we conclude that, in real time network traffic the performance of AODV is better and useful than DSR.AODV gives an uniform PDF (packet Delivery Fraction) than DSR, as DSR is good when less no of nodes and less traffic present in network, but as the nodes and traffic is increase the performance of DSR is decrease. But both DSR & AODV protocols are uniform in case of END-TO-END Delay than any other MANET Protocols.

REFERENCES

[1] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts,Mahendra Srivastava. An Overview of AODV Routing Protocol. International Journal of Modern Engineering Research (IJMER)Vol.2, Issue.3, May-June 2012 pp-728-732]
[2] Amith Khandakar .Foundation Program, Qatar University. Step by Step Procedural Comparison of DSR, AODV and DSDV,Routing protocol. 2012 4th International Conference on Computer Engineering and Technology (ICCET 2012)IPCSIT vol.40 (2012) © (2012) IACSIT Press, Singapore.
[3] Arun kumar .B.R Dr.C. Lokanatha Reddy and Dr.P.S. Hiremath. High performance Modified DSR with Power Consumption Optimization for Mobile Adhoc Networks. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.5, May 2007
[4] Ejiro .E. Igbesoko, Thaddeus Onyinye Eze, Mona Ghassemian. Performance Analysis of MANET Routing Protocols over Different Mobility ModelsSchool of Computing and Mathematical Sciences University of Greenwich London, United Kingdom {ie903, et701
[5] Amit N. Thakare Mrs. M. Y. Joshi. Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc NetworksMobile Ad hoc Networks. IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs, 2010
[6] Mamoun Hussein Mamoun .Faculty of Computer and Information Sciences. Important Characteristic of Differences between DSR and AODV Routing Protocol, MCN 2007 Conference, November 7-10, 2007
[7] G. Jose Moses* D. Sunil Kumar Prof.P.Suresh Varma N.Supriya. A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 3, March 2012 ISSN: 2277 128X
[8] Sachin Kumar Gupta* & R. K. Saket. PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2. IJRRAS.7(3).June.2011.www.arpapress.comVolumes/Vol7Issue3/ IJRRAS_7_3_15.pdf
[9] Performance Comparison of on-Demand and Table Driven Ad Hoc Routing Protocols using NCTUns by Khaleel Ur Rahman Khan Rafi U Zaman A. Venugopal Reddy, Tenth International Conference on Computer Modeling and Simulation, Pages 336-341.
[10] Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment, by Nor Surayati Mohamad Usop, Azizol Abdullah, IJCSNS International Journal of Computer Science and Network Security, **9**, No.7, July 2009.
[11] "Performance Measurement of Various Routing Protocols in Ad-hoc Network", Md. Anisur Rahman, Md. Shohidul Islam, Alex Talevski, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009, **1**, IMECS 2009, March 18 - 20, 2009, Hong Kong.
[12] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek,and M. Degermark. "Scenario based Performance Analysis of Routing Protocols for Mobile Ad-hocNetworks", Mobicom'99, 1999, Pages 195-206.
[13] Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks

AUTHORS:

Atul D.Atalkar

Second Year(IIIrd SEM)
M.E (EXTC)
ALAMURI RATNAMALA INSTITUTE ENGINEERING & TECHNOLOGY, Sapgaon, Thane. Dist.,M.H.
atul_atalkar@rediffmail.com

Prof. Prashant S.Wankhede

M.E (ELEX)
DATTA MEGHE COLLEGE OF ENGINEERING, Airoli, Navi Mumbai. Dist.M.H
prashant6929@gmail.com

