IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 12-17
www.iosrjournals.org

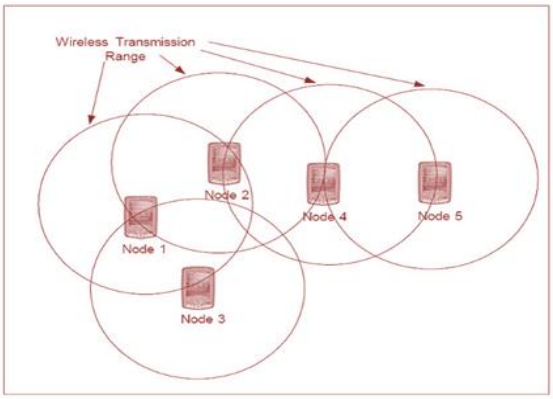
Performance Analysis of Routing Protocols in Mobile AD-HOC Networks (MANETs)

[1]Konduri.Sucharitha, [2]Dr.R.Latha
[1]*Research Scholar, Department of computer Science & Applications, Bharathiar University, Coimbatore, India*
[2]*Professor & Head, Department of Computer Applications, St.Peter's University, Avadi, Chennai -600 054, India*

Abstract: *A mobile ad-hoc network (MANET) is a self starting dynamic network comprising of mobile nodes, where each and every participation node voluntarily transmit the packets destined to some remote node using wireless (radio signal) transmission. The main aim behind the developing of ad hoc networking is multi-hop relaying. Wireless Ad hoc networks or infrastructure less networks are very easy to establish by using radio waves as transmitting medium without the requirements of any other equipment or infrastructure. An ad hoc network doesn't have any centralized arbitrator or server. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging in many areas such as routing, bandwidth, security, power consumption, collisions, simulations, and topology control due to moving nodes. This paper provides an overview of AODV, DSR, and TORA. The comparisons among three routing protocols are based on the various protocol property parameters such as Route Discovery, Network Overhead, Periodic Broadcast, Node overhead etc. different routing protocols proposed in literature and also provide a comparison between them.*
Keywords*: Mobile Adhoc Network, Protocol property, AODV, DSR, TORA , Route Discovery*

I. Introduction:

In MANET each and every mobile node is assumed to be moving with more or less relative speed in arbitrary direction. The main aim behind the developing of ad hoc networking is multi-hop relaying. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions as proposed by their Quality of service offerings.



II. FEATURES OF Manets:

Multi hop routing:

When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

Dynamic topology: Nodes are free to move arbitrarily in any direction thus the topology of the network change unpredictably.

Limited Bandwidth: the bandwidth available for wireless networks is generally low than that of wired networks. The throughput of these networks is generally low due various noises, fading effects.

Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

Constrained operation: the nodes are portable devices and are dependent on batteries. This is the most important design consideration of the MANET.

Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.
Security: wireless networks are more prone to threats than wired networks. The increased possibility of various security attacks like eavesdropping, denial of service should be handled carefully.

III. Evaluation Of Security In Manets:

In Manet's attention in many areas are necessary, such as routing, bandwidth, security, power consumption, collisions, simulations, and topology control due to moving nodes. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:
Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.
Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Integrity assures that a message being transferred is never corrupted.

Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

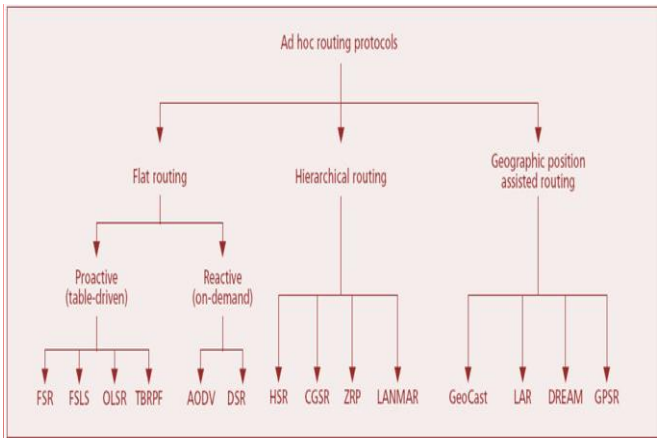
Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

Freshness: It ensures that malicious node does not resend previously captured packets.

IV. Routing Protocols

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. In MANET, there are different types of routing protocols each of them is applied according to the network circumstances. Figure 1 shows the basic classification of the routing protocols in MANETs.



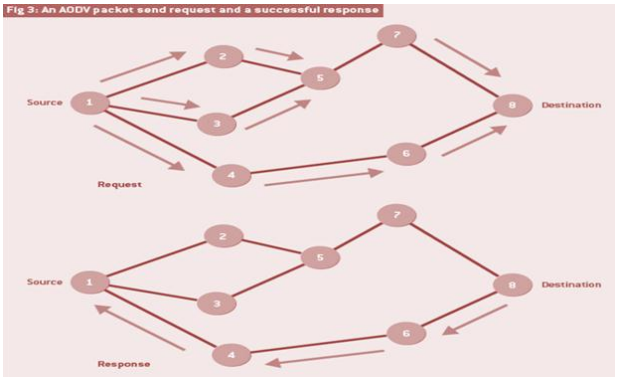
Routing protocol for ad-hoc network can be categorized in three strategies.

- Pro- active routing protocol.
- Re- active routing protocol.
- Hybrid protocols.

Ad-Hoc on Demand Distance Vector Protocol (AODV):

AODV stands for Ad-hoc On demand Distance Vector. AODV is distance vector type routing where it does not involve nodes to maintain routes to destination that are not on active path. As long as end points are valid AODV does not play its part. Different route messages like Route Request, Route Replies and Route

Errors are used to discover and maintain links. AODV is reactive protocol, when a source wants to initiate transmission with another node as destination in the network, AODV use control messages to find a route to the destination node in the network. AODV will provide topology information (like route) for the node. Fig.2 shows the message routing for AODV protocol. Node "A" wants to send messages to another node "F". It will generate a Route Request message (RREQ) and forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. Whenever the route to destination node is located or an intermediate node have route to destination. They generate route reply message (RREP) and send to source node. When the route is established between "A" and "F", node then they communicate with each other.



Route Table Management

Each mobile node in the network maintains a route table entry for each destination of interest in its route table. Each entry contains the following information:

- Destination
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for this route
- Expiration time for the route table entry

The other useful information contained in the entries along with source and destination sequence numbers is called soft-state information associated to the route entry. The info about the active neighbors for this route is maintained so that all active source nodes can be noticed when a link along a path to the destination breaks. And the purpose of route request time expiration timer is to purge the reverse path routing entries from all the nodes that do not lie on the active route.

Limitations/Disadvantages of AODV:

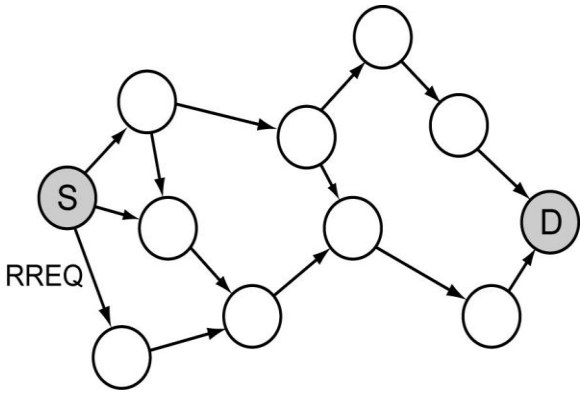
- Requirement on broadcast medium: The algorithm expects/requires that the nodes in the broadcast medium can detect each others' broadcasts
- Overhead on the bandwidth: Overhead on bandwidth will be occurred compared to DSR, when an RREQ travels from node to node in the process of discovering the route info on demand, it sets up the reverse path in itself with the addresses of all the nodes through which it is passing and it carries all this info all its way.
- No reuse of routing info: AODV lacks an efficient route maintenance technique. The routing info is always obtained on demand, including for common case traffic.
- It is vulnerable to misuse: The messages can be misused for insider attacks including route disruption, route invasion, node isolation, and resource consumption.
- AODV lacks support for high throughput routing metrics: AODV is designed to support the shortest hop count metric. This metric favors long, low bandwidth links over short, high-bandwidth links.
- High route discovery latency: AODV is a reactive routing protocol. This means that AODV does not discover a route until a flow is initiated. This route discovery latency result can be high in large-scale mesh networks.

Dynamic Source Routing (DSR):

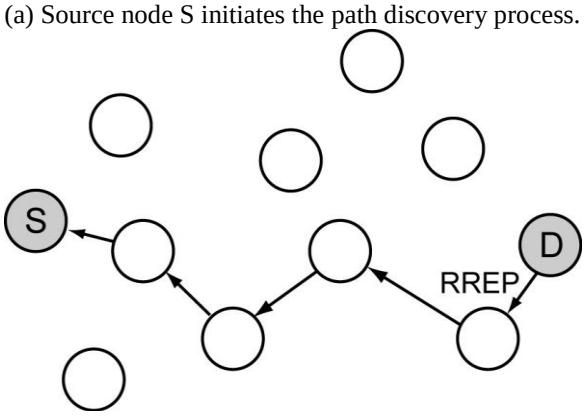
DSR is also a reactive routing protocol which uses the concept of source routing. In source routing the sender knows complete hop-by-hop route to the destination. All the routes are stored in the route cache. When a node attempts to send a data packet to a destination for which it does not know the route. In DSR each node maintains a route cache with route entries which are continuously updated as and when route learns new routes.

The biggest advantage of DSR is that no periodic routing packets are required. DSR has also the capability to handle unidirectional links. Unlike other protocols DSR requires no periodic packets of any kind at any layer within the network. It allows the network to be completely self-organizing and self-configuring and does not need any existing network infrastructure or administration. DSR uses no periodic routing messages like AODV, thereby reduces network bandwidth overhead, conserves battery power and avoids large routing updates. However, it needs support from the MAC layer to identify link failure. The DSR routing protocol discovers routes and maintains information regarding the routes from one node to other by using two main mechanisms: (i) Route discovery – Finds the route between a source and destination and (ii) Route maintenance –In case of route failure, it invokes another route to the destination.

DSR uses source routing concept. When packets are flooded by a source node, the sender node caches complete hop-by-hop route to the receiver node. These route lists are caches in a route cache. The data packets carry the source route in the packet header.DSR uses Route Discovery process to send the data packets from sender to receiver node for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. In Route discovery DSR works by flooding the data packets in network with route request (RREQ) packets. RREQ packets are received by every neighbor nodes and continue this flooding process by retransmissions of RREQ packets, unless it gets destination or its route cache consists a route for destination .Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to real source node .source routing uses RREQ and RREP
packets. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path toward the back. The source caches backward route by RREP packets for upcoming use. If any connection on a source route is wrecked, a route error (RERR) packet is notified to the source node.



(a) Source node S initiates the path discovery process.



(b) A RREP packet is sent back to the source

Advantages and Disadvantages of DSR:

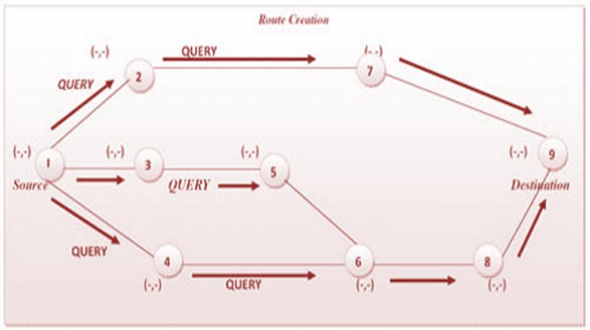
- One of DSR main advantages is the fact that it is a reactive (on-demand) protocol hence it does not flood the network with routing updates even when the link is not in use.
- A route is only determined when needed. There is no need to discover routes to all the nodes in the network. And the cached information in the intermediate nodes is used to reduce routing overhead.
- The disadvantage is that failed routes are not repaired locally. The cached information in the nodes may result in building inconsistent routes during reconstruction.
- There is high setup latency compared to the table-driven protocols.
- DSR is well suited for static and low-mobility networks. High mobility reduces its performance.

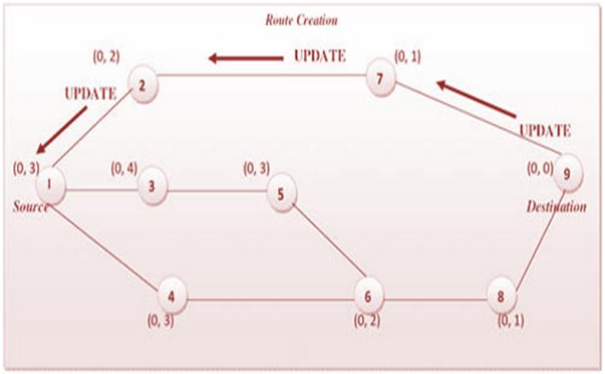
Temporally-Ordered Routing Algorithm (TORA):

A as its name suggest, is a routing algorithm. It is mainly used in MANETs to enhance scalability. TORA is an adaptive on demand routing protocol for multi hop networks. It is therefore used in multi-hop networks. A destination node and a source node are set. TORA is source initiated specially proposed routing protocol for highly dynamic mobile, multi-hop wireless networks. TORA is based on link reversal algorithms. The three steps involved in TORA are: a) route creation, b) route maintenance, and c) route erasure.

TORA establishes scaled routes between the source and the destination using the Directed Acyclic Graph (DAG) built in the destination node. This algorithm does not use 'shortest path' theory, it is considered secondary. TORA builds optimized routes using four messages . Its starts with a Query message followed by an Update message then clear message and finally Optimization message. This operation is performed by each node to send various parameters between the source and destination node. The parameters include time to break the link (t), the originator id (oid), Reflection indication bit (r), frequency sequence (d) and the nodes id (i). The first three parameters are called the reference level and last two are offset for the respective reference level. Links built in TORA are referred to as 'heights', and the flow is from high to low. At the beginning, the height of all the nodes is set to NULL i.e. (-,-,-,-,i) and that of the destination is set to (0,0,0,0,dest). The heights are adjusted whenever there is a change in the topology.

A node that needs a route to a destination sends a query message with its route-required flag. A query packet has a node id of the intended destination. When a query packet reaches a node with information about the destination node, a response known as an Update is sent on the reverse path . The update message sets the height value of the neighboring nodes to the node sending the update. It also contains a destination field that shows the intended destination. This proc ess is expressed in Figure.





The above figure shows, source node (1) broadcasts QUERY to its neighbor's node. Node (6) does not propagate QUERY from node (5) as it has already seen and propagated QUERY message from node (4). A source node (1) may have received a UPDATE each from node (2), it retains that height. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad-hoc network. The establishment of the route mechanism based on the Direct Acyclic Group (DAG). Using DAG mechanism, we can ensure that all the routes are loop free. Packets move from the source node having the highest height to the destination node with the lowest height like top-down approach.

Advantages:

 TORA supports multiple routes between source and destination. Hence, failure or removal of any of the nodes quickly resolved without source intervention by switching to an alternate route to improve congestion.

 TORA does not require a periodic update, consequently communication overhead and bandwidth utilization is minimized.

 TORA provides the supports of link status sensing and neighbor delivery, reliable, in-order control packet delivery and security authentication.

Disadvantages:
 It depends on synchronized clocks among nodes in the ad hoc network.
 The dependence of this protocol on intermediate lower layers for certain functionality presumes that the link status sensing, neighbor discovery, in order packet delivery and address resolution are all readily available. This solution is to run the Internet MANET Encapsulation Protocol at the layer immediately below TORA.
 This will make the overhead for this protocol difficult to separate from that imposed by the lower layer.

V. Comparitive Study Of Ad Hoc Routing Protocols:

Protocol Property	**AODV**	**DSR**	**TORA**
Table driven/ Source Routing	Table driven and Source Routing	Source Routing	Table driven and Source Routing
Need of Hello message	Yes	No	No
Route Discovery	On Demand	On Demand	On Demand
Node overhead	Medium	High	Medium
Multi-hop Wireless Support	Yes	Yes	Yes
Unidirectional link support	No ,yes	Yes	Yes
Network Suitable for	Highly Dynamic	Up to 200 nodes	Highly Dynamic
Route Discovery	Yes	Yes	Yes
Route Maintenance	Yes	Yes	Yes
Reactive/ Proactive	Reactive	Reactive	Reactive
Routing Overhead	High	Low	Average
Routing Philosophy	Flat	Flat	Flat
Route mechanism/ Maintenance	Route table with next hop	Complete Route cached	Route Table(Adjacent nodes on-hop knowledge)

This paper does the comparison of three routing protocols AODV, DSR and TORA. The significant observation is, comparison results agree with expected results based on theoretical analysis. As expected, reactive routing protocol AODV performance is the best considering its ability to maintain connection by periodic exchange of information, which is required for TCP, based traffic. DSR/AODV is based on route discovery and route maintenance Mechanism. Flat Routing Philosophy is used in DSR, AODV and TORA. Packet size is uniform for DSDV; AODV. Packet size is non uniform for DSR. Loop free routing Protocol Property is available to DSR, AODV and TORA.

VI. Conclusion:

In this article, we presents the comparative study and performance analysis of three mobile ad hoc routing protocols (AODV, DSR and TORA) on the basis of end to end delay, packet delivery ratio, media access delay, path optimality, routing overhead performance metrics. The quantitative study of these routing protocols shows that AODV keeps on improving in packet delivery ratio with dense networks. The performance of all protocols was almost stable in sparse medium with low traffic. TORA performs much better in packet delivery owing to selection of better routes using acyclic graph. It has been concluded that performance of TORA is better for dense networks. The AODV is better for moderately dense networks and for real time traffic AODV is preferred over DSR. The future work suggested that the effort will be made to enhance ad hoc network routing protocol by tackling core issues.

References

[1] Charles E.Perkins and Elizabeth M. Royer, "*Ad hoc on demand distance vector (AODV) routing (Internet-Draft)*", Aug-1998.
[2] C. E. Perkins and E. M. Royer; "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), PP: 90-100, 1999.
[3] V. Park and S. Corson, "Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification",IETF Internet draft, http://www.ietf.org/internet-drafts/draftietf-manet-tora-spec-01.txt, 1998.
[4] Sachin Kumar Gupta and R.K.Saket; "PERFORMANCE METRIC COMPARISON OF AODV AND DSDV ROUTING ROTOCOLS IN MANETs USING NS-2",IJRRAS 7 (3). JUNE 2011, PP: 339 – 350.
[5] Padmini Misra, *"Routing Protocols for ad hoc mobile wireless Networks",* http://www.cse.ohio-state.edu /~jain/cis788-99/ftp/adhoc_routing/#TDRP, Nov-1999.
[6] Loutfi, Valerie, Bruno. *"Securing mobile adhoc networks",* MP71 project, 2003