International Journal of Multidisciplinary Research and Modern Education (IJMRME)
ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume II, Issue I, 2016

AN OVERVIEW ON MOBILE AD-HOC NETWORKS

Payel Saha* & Asoke Nath**
* Student, Department of Computer Science, St. Xavier's College, Kolkata
** Associate Professor, Department of Computer Science, St. Xavier's College, Kolkata

Abstract:
The authors have observed the advancement in the field of internet due to wireless networking technologies. The emerging capabilities of mobile devices and routers have given a new direction to the internet and intranet communications, which decreases the cost and allow infrastructure less wireless networks i.e. Mobile Ad Hoc Wireless Network. Here in this paper we present the protocol, Ad hoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such mobile Ad hoc networks where each mobile host operates as a specialised router, and routes are otained as needed i.e. on demnad. With so many applications that MANETs provides us, there are still some challenges that are yet to overcome. This paper contains, the overview of MANET, the routing protocols followed by MANET, challenges (issues) involve in MANET and its applications in various fields.

Index Terms: Mobile ad-hoc Network (MANET), Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), Route Requests (RREQ), Route Replies (RREP), Route Errors (RRER), ZRP (Zone Routing Protocol), Destination Sequenced Distance Vector (DSDV) & User Datagram Protocol (UDP)

1. Introduction:

'Ad hoc' is the latin word which means something formed or used for a dedicated purpose and for an immediate need. A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves in a random fashion, thus the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc.

Each of the nodes i.e. the mobile routers has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple example of a mobile ad-hoc network with three nodes Node A, Node B, and Node C. Assuming, Node A and Node C are not within range of each other to exchange information; however the Node B can be used to forward data packets between Node A and Node C as Node B is within the range of both Node A and Node C. The Node B will act as a router and these three nodes together form a mobile ad-hoc network having the path named as A-B-C.

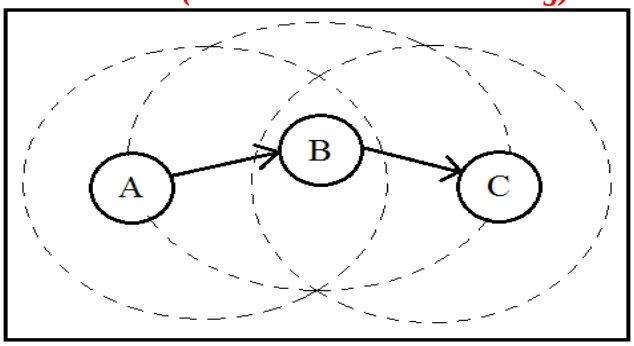

Figure 1: Example of a Mobile Ad-Hoc Network

2. Characteristics:

Characteristics of Mobile Ad hoc Network are as follows:-

- *Distributed nature:* The control of the network is distributed among the nodes, there is no centralize concept between nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.
- *Multi hop routing:* When any node tries to send information to other nodes, the destination node is not in the source node's communication range, the packet should be forwarded via one or more intermediate nodes.
- *Behave as an Autonomous terminal:* In MANET, each mobile node is an independent node, which could function as both a host and a router.
- *Dynamic topology:* Nodes can move arbitrarily with different speeds; thus, the network topology may change randomly at unpredictable time. The nodes in the MANET dynamically establish routing among themselves.
- *Light-weight terminals:* The nodes at MANET are mobile in nature having less CPU capability, power storage and small memory.
- *Shared Physical Medium:* With the appropriate equipment and adequate resources the wireless communication medium is accessible to any entity. Accordingly, access to the channel cannot be restricted.

3. Challenges and Limitations:

Some of MANET limitations and challenging fields [8, 11, 12, 13, and 16] can be described as follows:-

- *Bandwidth Limitation:* Wireless link continue with significantly lower capacity than infrastructure networks [8]. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
- *Dynamic topology:* The trust relationship may be disturbed for dynamic nature among nodes. The trust may also be disturbed if some nodes are detected as compromised.
- *Routing Overhead:* In wireless ad-hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead [11].
- *Hidden terminal problem:* The hidden terminal problem [12] refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

- *Due to transmission errors loss of packets:* Due to several factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, and frequent path breaks due to mobility of nodes ad hoc wireless networks faces a much higher packet loss.
- *Mobility-induced route changes:* Due to the movement of nodes the network topology in an ad hoc wireless network is highly dynamic; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.
- *Battery constraints:* In these networks which devices are used, have restrictions on the power source in order to maintain portability, size and weight of the device.
- *Security threats:* The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are exposed to numerous security attacks.

4. Applications:

Some of the typical applications [7, 9, 11, and 14] of MANET includes:-

a) *Military communication:* Ad-Hoc networking would allow the military to take advantage of commonplace network technology [7] to maintain an information network between the soldiers, vehicles, and military information head quarter.

b) *Collaborative work:* For some business environments, the need for collaborative computing might be more important outside office environments than inside and [9] where people do need to have outside meetings to cooperate and exchange information on a given project.

c) *Local level:* Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at e.g. a conference or a classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

d) *Personal area network and bluetooth:* A personal area network is a short range, localized network where nodes are usually associated with a given person. [11] Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

e) *Commercial Sector:* Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake [14]. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

5. Routing Protocols:

An ad hoc routing protocol is a convention, or standard, that controls how the mobile nodes decide which way to route the data packets between computing devices in a mobile ad hoc network including their movement. Ad-Hoc network routing protocols [2, 4, 5, and 6] are commonly divided into three main categories: Proactive, Reactive and Hybrid protocols as shown in Figure 2.

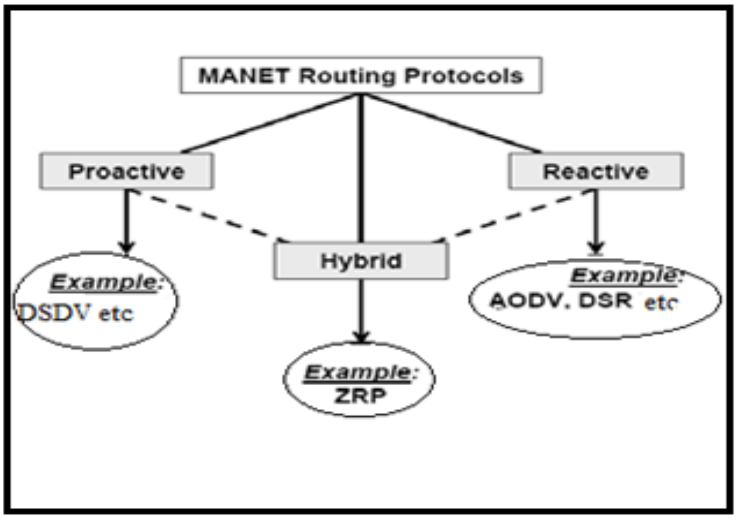

Figure 2: Classification of MANET routing protocols

5.1 Proactive Protocols:

Proactive or table driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Examples of such schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV) [7]. They attempt to maintain consistent, upto-date routing information of the whole network. It minimizes the delay in communication and allow nodes to quickly determine which nodes are present or reachable in the network.

5.2 Reactive Protocols:

Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) [3] and Dynamic Source Routing (DSR).

5.3 Hybrid Protocols:

They introduce a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory.

6. Proposed Routing Algorithm:

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

Reactive routing techniques or on-demand routing techniques are appropriately designed for ad hoc wireless topology that frequently changes its organized fashion. It does not continuously maintain a route between all pairs of network nodes, instead, routes are only discovered when they are actually needed. A benefit of this approach is that signaling overhead is much reduced compared to proactive approaches.

The Ad Hoc On-Demand Distance Vector Routing (AODV) [2, 10] is an on-demand routing protocol, which uses sequence numbers to identify the most recent path. This is a major difference between AODV and other on-demand routing protocols. AODV allows multi mobile nodes to obtain routes quickly for new destinations, and does

not include unnecessary nodes to maintain the routes to destinations that are not in active communication. When an active link breaks, its effect is notified by a set of nodes so that it is able to invalidate the routes using the lost links.

The algorithm's primary objectives are:-

- To broadcast data packets only when it is necessary through the discovered route.
- To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information.
- To distinguish between local connectivity management and general topology maintenance

Here in AODV protocol, three message types are defined and they are Route REQuests (RREQs), Route REPlies (RREPs), and Route ERRors (RERRs). All of AODV messages are sent by using port 654 on UDP. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. When the source node has data packets to be sent to the destination, it firstly checks its route table to determine whether it already has a route to the destination and if such a route exists, it can use that route for data packet transmissions. Otherwise, to find a new route for packet transmission it must initiate a route discovery procedure. A RREQ packet starts to discover the route of the destination. It places the destination node's IP address in this packet, the last known sequence number of that destination, the source's IP address, and the current sequence number. The RREQ also uses hop count to determine the shortest path and RREQ ID for unique identification. This RREQ sends a broadcast reach to the network.

When a neighboring node receives the RREQ, it firstly creates a reverse route to the source node then checks to determine whether it has received the RREQ with the same originator mobile node and RREQ ID within destination discovery time. The node must discard if the RREQ has been received. This node increases by one to get the hop distance to a RREQ packet. If it does not have a valid route to the destination node, it will simply re-broadcast the RREQ. Hence, The RREQ is flooding the network in search of a route to the destination via multi mobile nodes. If the node is found for matching destination address in its reverse route table, actions must be taken as follows:-

- The originator sequence number from the RREQ is compared to the corresponding destination sequence number in the route table entry and copied if it is greater than the existing value there.
- The next hop field in routing table becomes the node from which the RREQ is received.
- The hop count is copied from the hop count in the RREQ message.
- The node sends the RREP message back to the originator node.

As shown in Figure 3, the source node 1 initiates a path-finding process by originating the RREQ to flood in the network for the destination node 10. When neighbors which are node 2, 3, and 4 receive the RREQ packet, they check their routes to the destination which is node 10. They are not an available route to the destination, thus they forward the RREQ packet to its neighbors. When the RREQ reaches node 9 which has a route to the destination node, node 9 checks the sequence number compared between the RREQ and its cache. If its cache is equal to or greater than the RREQ then it generates the RREP to the source node.

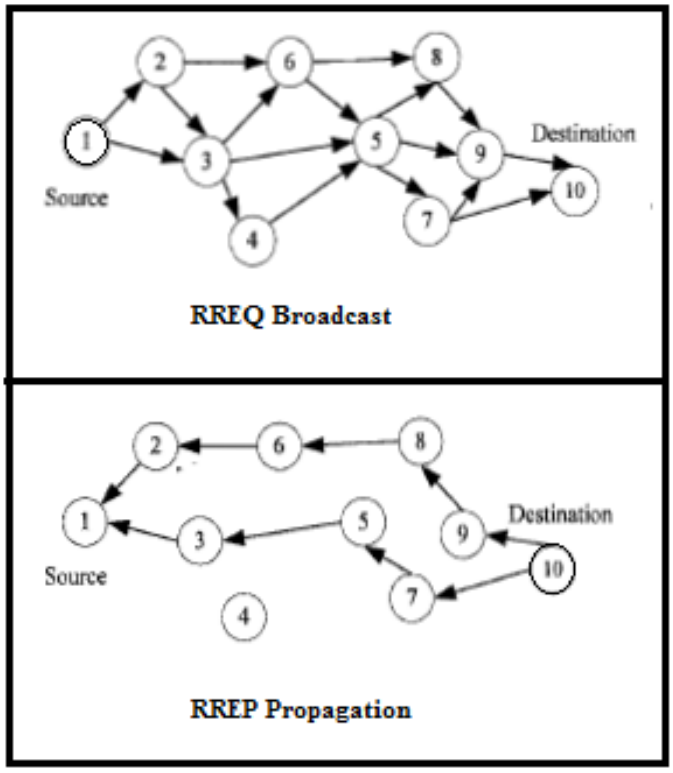

Figure 3: The AODV Route Discovery

Maintaining sequence number for representing freshness of its routing information of the source and destination nodes guarantees the loop-freedom of all routes towards that node. The sequence number is a 32-bit unsigned integer; the largest possible number is 4294967295. Before the originator node originates a route discovery, it increases its own sequence number and then put it into the RREQ to prevent conflicts with previously established reverse routes towards the originator of the RREQ. On the other hand, before the destination node originates the RREP in response to the RREQ, it increases to update its own sequence number and put it into the RREP. Every route table entry at every node must include the latest information available about the sequence number for the destination node for which the route table entry is maintained. It is updated whenever the node receives new information about the sequence number from RREQ, RREP, or RERR messages that are relatively received to that destination.

As per Figure 4, for maintaining routing, the node initiates a process for a RERR message if it detects a link break for the next hop of an active route in its routing table, or if it gets a data packet destined to the node for which it does not have an active route and is not repaired, or if it receives a RERR from a neighbor for one or more active routes. When a link breaks, which is determined by observing the periodical beacons or through link- level acknowledgments, the end nodes are notified. When the source node learns about a path break, it reestablishes the route to the destination if required by the higher layers. If the path break is detected at an intermediate node, the node informs the end nodes by sending an unsolicited RREP with the hop count set as 00.

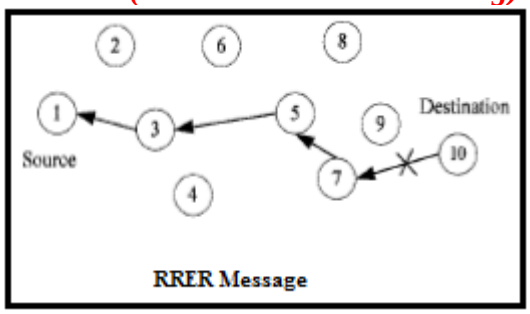

Figure 4: AODV Route mainetance using RRER message

Suppose a link breaks between node 9 and node 10 as shown in Figure 4, both nodes initiate the RERR to inform their end nodes about the link break. The end nodes delete the corresponding entries from their tables. The source node reinitiates the path-finding process with a new broadcasts ID and the previous destination sequence number.

7. Future Research:

More research is needed in the mobility of the nodes in order to comprehensively evaluate the impact of the malicious nodes movement on the protocol's performance.

8. Conclusion:

In this paper, overview of MANET, its characteristics, challenging fields, limitations, routing protocols, and one most commonly used protocol, have been described briefly. The ultimate goal of a routing protocol of MANET is to efficiently deliver the network data from the source to the destinations wirelessly.

Acknowledgement:

I would like to express my special thanks all professors of Department of Computer Science, St. Xavier's College (Autonomous), Kolkata for their continuous valuable support and guidance.

References:

1. Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
2. Humayun Bakht, "Survey of Routing Protocols for Mobile Ad-hoc Network", International Journal of Information and Communication Technology Research, 258-270, October 2011.
3. C.Perkins, E. Belding-Royer and S. Das, "Ad-Hoc On-Demand Distance Vector (AODV) Routing", RFC3561, July 003.
4. T. Goff, N. B. Abu-Ghazaleh, D. S. Phatak, and R. Kahvecioglu. Preemptive routing in ad hoc networks. In Proceedings of the seventh annual international conference on Mobile computing and networking, pages 43-52. ACM Press, 2001.
5. Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama. Encyclopedia of Telecommunications, chapter Wireless Ad Hoc Networks. John Wiley, 2002.
6. H. Hellbrück and S. Fischer. Towards analysis and simulation of ad-hoc networks. In Proceedings of ICWN02, pages 69-75, June 2002.
7. C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, pages 234-244, Sept. 1994.

8. Web page. Mobile Ad-hoc Networks (MANET): Routing Protocol Performance Issues and Evaluation Considerations. http://datatracker.ietf.org/doc/rfc2501
9. Dr.S.S.Tyagi and Arti, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
10. Web page. Mobile Ad-hoc Networks (MANET): Ad hoc On-Demand Distance Vector (AODV) Routing. https://datatracker.ietf.org/doc/rfc3561
11. Mohit Kumar and Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE).
12. Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester "An Overview of Mobile ad hoc Netwroks: Applications & Challenges". http://psut.jo/sites/raad/wireless_notes/MANET-Overview.pdf
13. Kavita Taneja, R.B. Patel "An Overveiw of Mobile Ad hoc Networks: Challenges and Future."
14. Vikaram Patalbasi, Sonali Mote "Mobile Ad hoc Networks: Opportunities and Future."
15. Ram Ramanathan and Jason Redi "A Brief Overview of Ad Hoc Networks: Challenges and Directions" IEEE Communications. Magazine- 50th Anniversary Commemorative Issue/May 2002
16. Imrich Chalmtac, Marco Conti, Jennifer J.-N. Liu " Mobile ad hoc networking: imperatives and challenges "