International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 06 (November – December, 2016)

# Review of Mobile Ad-hoc Network (MANET) Routing Protocols

**Sandeep Monga**
Research Scholar, Department of Information Technology
UIT, RGPV, Bhopal, Madhya Pradesh, India
smongaphd6@gmail.com

**ABSTRACT** Mobile Adhoc Network (MANET) is a dynamic network framed by an accumulation of wireless nodes. As it is a dynamic network all nodes are in the network must play the role of a router. Way should be developed by every node in the event that it needs to communicate with the other node. A node can discover way to other node either by a proactive or a reactive or a hybrid routing protocol. Numerous mobility models and protocols are accessible to discover way. Every mobility model and protocol has its own particular quality and shortcoming relate to MANET condition. In this we have discussed the advantages and disadvantages are compared

## I. INTRODUCTION

With the growth of wireless technology its area of application has extended many folds. Effectively the wireless technology has been widely arranged into two Classifications: Infrastructure- based and Infrastructure-less technology. As the name determined the Infrastructure based technology includes the use of an access point, which is utilized for interfacing a wired network with the wireless nodes. This scenario can be found in Airports, Hotels, Universities and so forth. On the other hand, the infrastructure less technology also called the Ad-hoc network interfaces with the wireless node without the use of any access points. At the point when such sort of wireless nodes are moving then they called Mobile-Ad-hoc Network (MANETs). Examples of MANETs are building-to-building, vehicle-to-vehicle, ship-to-ship and so forth.

## II. CATEGORIZATION OF MANET ROUTING PROTOCOLS

Before going through MANETs Protocols categorization, firstly we will look at distinctive broadcasting strategies that use in MANETs: -

**Uni-casting:** It is characterized as a broadcasting process where the data is send from the source to a single destination.

**Multicasting:** It is characterized as a broadcasting process where the data is send from a source to many destinations.

**Broadcasting:** It is characterized as a broadcasting process where the messages are sending from a source to all other nodes in the predefined networks.

**Geo-casting:** It is characterized as broadcasting process of sending of information from the source to all other nodes inside a geographical region. The characterization of the routing protocol in MANETs [4] is widely based on two methodologies: Qualitative approach and Quantitative approach. The Qualitative approach primarily incorporates the following measurements –

**Loop Free Network:** In wireless network where the data transfer capacity (bandwidth) is constrained the interference from the neighbouring nodes will prompt the collision of the transmitted packets. Furthermore, in this way the packet is re-transmitted until it is not received by the destination which will leading to the formation of a loop. In this way avoid these loops for the effective bandwidth utilization and time processing is required.

**On request routing behaviour:** For the best possible bandwidth utilization the route for a specific path are made on demand by spreading the flow of control messages. This sort of reactive routing protocol introduces medium to high latency. *Proactive behaviour:* To accomplish low latency and where the bandwidth requirement prerequisite is not the prime issue, in such places this sort of routing protocol is used.

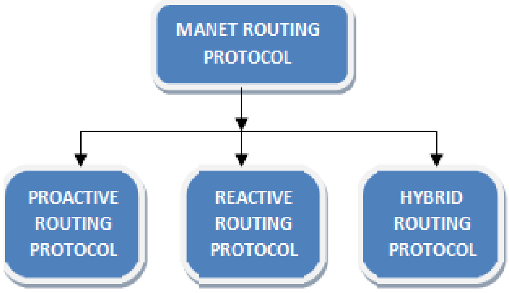

Figure-1 Categorization of MANET Routing Protocols

**Unidirectional connection Support:** the node in the wireless network may impart in a unidirectional connection. The routing protocol should be designed in such a way that it should support both unidirectional and bidirectional connections. From the above approach we have concluded that MANET efficient routing protocol have to maintained the following parameters: routing overhead, energy consumption, node participation in the routing process, latency and security vulnerability. Quantitative approach includes the following parameter.

**End to end data throughput and delay***:* The delay should be minimized and the throughput should be increased to ensure the efficient working of the routing protocol.

**Route acquisition time:** In order to reduce the delays in a routing protocol the way should be so developed that the route should take the lesser time for its route detection and this can be done by this metric.

**Out of order delivery:** The delivery of the data packets should be in an exact order, if it goes out of order then it will influence the performance of the routing protocol.

**Efficiency:** Some other metrics are mandatory to check the effectiveness of the routing protocols such as packet delivery ratio, bandwidth utilization.

A) **Proactive Routing Protocol** This protocol maintains routing tables of identified destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using identified routes, however routing tables must be kept update; this uses memory and nodes periodically send update messages to neighbours, even when no traffic is present, wasting bandwidth [1]. Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads.

B) **Reactive Protocols** use a route discovery process to flood the network with route query requests when a packet needs to be routed using source routing or distance vector routing. Source routing uses data packet headers containing routing information meaning nodes don't need routing tables; however this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store active routes information until no longer required or an active route timeout occurs, this prevents stale routes [1]. Flooding is a reliable method of disseminating information over the network, however it uses bandwidth and creates network overhead, reactive routing broadcasts routing requests whenever a packet needs routing, this can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and has typically lower memory usage than proactive alternatives, this increases the scalability of the protocol [2].

C) **Hybrid Routing Protocols:** The features of both the protocol types are combined to satisfy the requirement based on the scenario. These protocols can act as reactive or proactive in different situations like increase in network size and density.

## III. ROUTING PROTOCOLS

This section describes the nature of each and every protocol considered for comparison. In a MANET environment the routing protocols use three types of control packets to find and maintain the path. • Route requisition is done from source using route request packet (RREQ), Reply sent from destination node using route reply packet (RREP), Route update is done using hello packet , Route failure or error is intimated using route error packet (RERR).

1. **Destination-Sequenced Distance Vector (DSDV)** In DSDV sequence numbers are assigned by each source while route request packets are sent to neighbours, which avoid looping and help to select a latest route. Global view of network topology is not available. All the nodes in the network maintain routing information to all known destinations and route updates are done periodically [3].
2. **On-Demand Anonymous Routing in Ad Hoc networks (ODAR)** Initial routing process of ODAR follows DSR algorithm. The protocol uses a data structure called bloom filter which stores a set of element. Each element is tested if it is a member of the set or not. Elements involved in the set or permanent. Once if the source hashes the route information it cascades it to the bloom filter. An intermediate node will forward the packet if and only if its ID is in the bloom filter, otherwise it will simply drop the packet [4].
3. **Link State Routing (LSR)** Route is found using Dijkstra's shortest path method based on current conditions. Each node has topology view of the entire network and is updated regularly through link state packet (LSP). This is circulated among the neighbour nodes till all are updated [5].
4. **Secure Position Aided Ad hoc Routing (SPAAR)** Along with the destination ID, distance from the source and exact coordinates are included. Specialty of SPAAR is that the routing information is encrypted with a group encryption key. The receiving node decrypts the information and the successful nodes informing the sender are the one hop neighbours. Similarly the remaining route estimation is done at the intermediate nodes by adding their IDs to the RREQ. The route cache is maintained for the reverse path. RREP generated at the destination is also in an encrypted form of details like sequence number, velocity, destination's coordinates and timestamp [6].
5. **Anonymous Location-Aided Routing in Suspicious MANETs (ALARM)** Nodes are grouped on location basis and are lead by a group manager. Each node register itself with the group manager gets a group signature. The protocol sends Location Announcement Messages (LAM) from time to time to the nodes in the group. The LAM message has details like nodes current position, time stamp and a session key. Only valid members with the signature can decrypt the packets and read. Concatenation of nodes temporary ID and the group signature forms the pseudonym [7].

6. **A Geo-casting Protocol for Mobile Ad Hoc Networks Based on GRID (GeoGRID)** Geographic area is divided as a number of grids. Each grid has a grid leader. Only the leader can propagate the packets to the members in the grid. Geo-GRID is available I two versions namely flooding-based and ticket-based. GeoGRID is appreciated well in crowded MANET [8].
7. **Ad-hoc on demand Distance Vector (AODV):** Route is initiated by the node which needs to communicate with a destination only on a demand. The source initiates path finding through RREQ to its one hop neighbours. The packet is forwarded by an intermediate node its one hop neighbours if it is not a destination. On reception of this RREQ at destination, A RREP is generated and sent back to the source. Nodes store only the active route information which results in reduced control overhead [9].
8. **Dynamic source Routing (DSR)** In DSR path finding is almost similar as in AODV. No periodic exchange of control packets. During packet forwarding in intermediate nodes, not like AODV, they store their ID and update their cache with the active routing information. Route discovery and recovery are done only when it is required. Routing overhead is scaled to the actual size [10].
9. **Cluster-based routing protocol (CBRP)** Nodes are organized in a hierarchical manner and grouped into clusters. Each cluster is represented using a cluster-head. Data transmission is done through the cluster heads between the clusters which reduces the control overhead [11].
10. **Zone Routing Protocol (ZRP)** This hybrid protocol acts as both reactive and proactive routing protocols. Within a zone it acts as a proactive routing protocol using Intra Zone routing protocol (IARP). Between zones it acts as a reactive protocol using Inter Zone Routing Protocol (IERP). Path can be constructed to destination node within the local region using the proactively cached routing information. If the destination is away from the local region then the route discovery is done reactively through the border nodes. The border nodes pass the request by adding their ID to the RREQ to the next zone if the destination is not within the local zone [12].
11. **Fisheye State Routing (FSR)** Each node stores the link state for every destination in the network. This link state update of a destination is periodically broadcasted to its neighbours. Update messages contain information only about closer nodes and not farther [13].
12. **Link Aided Routing (LAR)** Network identifies two zone namely requested zone and expected zone. Instead spreading the RREQ packets to the entire network, the packets are sent to the zones where the destination is expected to be. Using an algorithm with the GPS location the requested zone is obtained. The source node estimates the expected zone of the destination based on the previous location. The RREQ is flooded only to the requested zone inclusive of the expected zone [14].
13. **Optimal Link State Routing (OLSR)** OLSR is a proactive routing protocol. The routing information is updated periodically through the nodes one hop neighbour selected namely multipoint relay (MPR). The traffic and control overhead is reduced as the packets are sent through the MPRs [15].
14. **Privacy-Preserving Location-Based On-Demand Routing in MANETs (PRISM)** Routing is done based on AODV and do not propagate topology information. PRISM mainly concentrates on the security aspect against the insider and outsider attacks. Hash of RREQ, RREP is used as a route identifier and group signatures are used for authentication [16].
15. **Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK)** The node identities are masked with the help of a group pseudonym. In order to find the path, first the node which needs to communicate authenticates the neighbouring node by sending a challenge with the pseudonym selected in random. Then the master key is calculated by the challenged node and gives authentication to the sender. Based on the master key both of them generate link ID and session keys [17].
16. **Anonymous Routing Protocol for mobile ad hoc networks (ARM)** The RREQ is generated in such a way that the nodes except destination cannot be aware of the destination. With the help of the pseudonym the intermediate nodes can conclude that they are not the destination node. For each communication a secret key and current pseudonym are shared between the source and destination. The destination sends the RREP in an encrypted for with its broadcast ID [18].
17. **Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks (AnonDSR)** The communication process involves three protocols in different levels. At first level a shared key and a nonce is generated between the source and the destination. Using this trapdoor is created in second level. Each intermediate node has a shared session key. Finally after the route discovery the communication is done using this session key [19].
18. **Security Aware Routing protocol (SAR)** SAR aims at security based on the trust values and trust relationships associated with adhoc nodes and this value is used to take routing decisions. Security is provided through symmetric encryption method. Routing is done only through trusted nodes to which trust values are already assigned. Nodes which satisfy the required level of security only can participate in routing [20].
19. **Signal Stability Based Adaptive Routing (SSA)** In SSA the routes are analyzed and categorized as

strong and weak nodes based on their signal stability. This protocol works on an on demand basis. During path finding the node selection is done through the strong nodes. Channelling the packets through the strong signal nodes avoid link failure due to signal level [21].

20. **Temporally-Ordered Routing Algorithm (TORA)**
**TORA** follows a hierarchical topology of nodes. Route construction is done on a directed acyclic graph (DAG) form. Information always flows from the higher level to the lower level as a fluid. The node which requires communicating with the destination node will find path through the upper node in upper level [22].

Comparison of the Protocols based on the parameters like category, security advantage and disadvantage.

Table-1 Comparison of Protocols

| # | Protocol | Type | Security / Privacy | Advantage | Disadvantage |
|---|---|---|---|---|---|
| 1 | LSR | Proactive | Not specific | Loop free Fast route discovery | Considerable memory demand |
| 2 | OLSR | Proactive | Not specific | Immediate availability of routes | More overhead and usage of resources |
| 3 | DSDV | Proactive | Not specific | Loop free Dynamic reaction to topology changes | More overhead due to unwanted information storage |
| 4 | SPAAR | Proactive | Third party certificate | No injection false routing information by intruders Loop Free | More Overhead |
| 5 | ALARM | Proactive | Node communication cannot be traced | Protection against outsider and insider attacks | Not suitable in large networks |
| 6 | Geo-GRID | Proactive | Not specific | Better suited for crowded environment | No security measures |
| 7 | AODV | Reactive | Not specific | Reduced control overhead | Suitable only for less dense network |
| 8 | DSR | Reactive | Not specific | No periodical flood to the network | Connection setup delay is higher Performance degrades rapidly with increasing mobility |
| 9 | FSR | Reactive | Not specific | Consumes less bandwidth Reduced control overhead Reduced message size | Poor performance in small sized network |
| 10 | ODAR | Reactive | Key & Encryption | Identity, topology and routing details are secured | False positive results in unnecessary packet forwarding |
| 11 | PRISM | Reactive | Node movement cannot be traced | Path discovery is done independent of current topology | Source node should determine the destination location Routing overhead is little higher |
| 12 | MASK | Reactive | Nodes are unlocatable and intractable | Source and destination anonymity End-to-end flow cannot be tracked | Resilient to wide range of attacks |
| 13 | ARM | Reactive | Destination privacy | Simple cryptographic process Done only by source and destination. | Many assumption with practical difficulty like shared secret key, pseudonym, permanent ID |
| 14 | AnonDSR | Reactive | Not specific | Good level of anonymity Scalable | Assumption of secret key |
| 15 | SAR | Reactive | Not specific | Suitable to different environments | Not suitable for with high-risk background |
| 16 | SSA | Reactive | Not specific | Reduces path failure by signal stability | More overhead |
| 17 | CBRP | Hybrid | Not specific | Reduced control overhead | Communication is possible only through cluster head |
| 18 | ZRP | Hybrid | Not specific | hybrid approach provides combined advantage of other protocols | Delay is more |

## IV. CONCLUSION

There are lots of protocols in existence for the MANET. Each has a different functioning principle pertain to a situation. From the study it is observed that no single protocol is best amongst all, as each has better performance over the other at a particular metric and time. Advantages and disadvantages of those protocols are compared in a table for better understanding of the protocols, which helps in selecting a protocol suitable for the environment and the circumstances.

## REFERENCE

[1]. H. Amri, M. Abolhasan, and T. Wysocki, “Scalability of MANET routing protocols for heterogeneous and homogenous networks,” Computers and Electrical Engineering, vol. 36, no. 4, pp. 752–765, 2010.

[2]. E. Alotaibi and B. Mukherjee, “A survey on routing algorithms for wireless Ad-Hoc and mesh networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56, no. 2, pp. 940–965, October 2011.

[3]. Guoyou He., “Destination-sequenced distance vector (DSDV) protocol”, Technical report, Helsinki University of Technology, Finland.

[4]. D. Sy, R. Chen, and L. Bao, “Odar: On-demand anonymous routing in ad hoc networks”, IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 267–276, 2006.

[5]. C. Adjih, E. Baccelli, P. Jacquet, “Link State Routing In Wireless Adhoc Networks”, Proceedings of the IEEE conference on Military communications, Volume 2 ,pp. 1274-1279, 2003.

[6]. S. Carter and A. Yasinsac, “Secure position aided ad hoc routing,” Proceedings of IASTED International Conference on Communications and Computer Networks (CCN02), pp. 329–334, 2002.

[7]. K. El Defrawy and G. Tsudik, “Alarm: Anonymous location-aided routing in suspicious MANETs”, IEEE International Conference on Network Protocols, pp. 304–313, 2007.

[8]. Wen-Hwa Liao, Yu-Chee Tseng, Kuo-Lun Lo, and Jang-Ping Sheu, “GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID”, Journal of Internet Technology, Vol. 1, Issue 2, pp.23-32, 2000.

[9]. S.A. Hussain, K. Mahmood and E. Garcia, “Factors affecting performance of AODV”, Information Technology Journal, Vol. 6, Issue 2, pp 237-241, 2007

[10]. Narendra Singh Yadav and R.P. Yadav, “The Effects of Speed on the Performance of Routing Protocols in Mobile Ad-hoc Networks”, International Journal of Electronics, Circuits and Systems, Vol. 1, Issue 2, pp 79-84, 2009.

[11]. Yogesh Chaba, Yudhvir Singh, Manish, “Performance Evaluation and Analysis of Cluster Based Routing Protocols in MANETs” Proceedings of IEEE/ACEEE ACT, pp. 64-66, 2009.

[12]. Ashish K. Maurya, Dinesh Singh, “Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocols in MANET”, International Journal of Computer Applications, Volume 12– Issue 2, pp.23-28, 2010.

[13]. R. Mkhija and R.Saluja, “Performance Comparison of Ad-Hoc Routing Protocol in Different Network Size”, Proceedings of 2nd National Conference of Mathematical Techniques: Emerging Paradigms in Electronics and IT Industries, 2008.

[14]. Young-Bae Ko and Nitin H. Vaidya, “Location-Aided Routing (LAR) in mobile ad hoc networks”, Springer –verlog, New York, “Wireless Networks”, vol. 6, pp. 307–321, 2000.

[15]. Jacquet. P, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, “ Optimized link state routing protocol for ad hoc networks” Proceedings of IEEE Multi Topic International Conference on Technology for the 21st Century, pp. 62–68, 2001.

[16]. Karim El Defrawy and Gene Tsudik, “Privacy-Preserving Location-Based On-Demand Routing in MANETs”, IEEE journal on selected areas in communications, Vol. 29, Issue 10, pp. 1923-1934, 2011.

[17]. Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Mask: anonymous on-demand routing in mobile ad hoc networks,” IEEE Transactions on Wireless Communication, Vol. 5, Issue 9, pp. 2376–2385, 2006.

[18]. S. Seys and B. Preneel, “Arm: anonymous routing protocol for mobile ad hoc networks,” International Journal of Wireless and Mobile Computing., vol. 3, Issue 3, pp. 145–155, 2009.

[19]. R. Song, L. Korba, and G. Yee, “AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks,” Proceeding of the 3rd ACM workshop on Security of ad hoc and sensor networks, NewYork, pp. 33–42, 2005.

[20]. Seung Yi, Prasad Naldurg, Robin Kravets, “Security -Aware Ad hoc Routing for Wireless Networks”, Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, pp.299-302, 2001.

[21]. R. Dube, C. D. Rais, K-Y. Wang and S. K. Tripathi, "Signal Stability Based Adaptive Routing for Ad Hoc Mobile Networks", IEEE Personal Communication, vol. 4, Issue 1, pp. 36-45, 1997.

[22]. V.D.Park and Scott.M.Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”, Proceedings of 16th IEEE Annual Joint Conference of Computer and Communications Societies, Vol.3, pp.1405-1413, 1997.