ISSN 2319-2720
Volume 3, No.3, July – September 2014
International Journal of Computing, Communications and Networking
Available Online at http://warse.org/pdfs/2014/ijccn04332014.pdf

A Comparative Study Of Routing Protocols In Ad Hoc Networks

R.Arthi[1], E.Padma2, Dr.N.Shanthi[3]
[1]PG Scholar (CSE), Nandha Engineering College, Erode, adjomn@gmail.com
[2]Assistant Professor (CSE), Nandha Engineering College, Erode, padmasents@gmail.com
[3]Professor and Dean (CSE), Nandha Engineering College, Erode, shanthi.moorthi@gmail.com

ABSTRACT

Mobile Adhoc Network (MANET) is assortment of multi-hop wireless mobile nodes that communicate with one another while not centralized management or established infrastructure. The wireless links during this network square measure extremely error prone and might go down often owing to quality of nodes, interference and fewer infrastructures. Therefore, routing in MANET could be an important task owing to extremely dynamic setting. In recent years, many routing protocols are projected for mobile adhoc networks and outstanding among them square measure DSR, AODV and TORA. This analysis paper provides an outline of those protocols by presenting their characteristics, practicality, edges and limitations thus makes their comparative analysis so to investigate their performance. The target is to form observations regarding however the performance of those protocols is often improved.

Key Words: MANET, AODV, DSR, TORA

1. INTRODUCTION

The wireless network may be classified into two types: Infrastructure or Infrastructure less. In Infrastructure wireless networks, the mobile node will move while communicating, , the base stations are fixed and as the node goes out of the range of a base station, it gets into the vary of another base station. In Infrastructure less or Ad Hoc wireless network, the mobile node will move while communicating, there are no fixed base stations and every one the nodes within the network act as routers. The mobile nodes within the unexpected network dynamically establish routing among themselves to make their own network 'on the fly' [12]. A Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary/short-lived network with none fastened infrastructure wherever all nodes area unit absolve to move regarding every which way and wherever all the nodes piece themselves. In MANET [1], every node acts each as a router and as a host & even the topology of network may change rapidly.

2. ROUTING PROTOCOL DESIGN ISSUES AND CHALLENGES

The particular features of MANETs make the design of a multicast routing protocol [13] a challenging one. These protocols must deal with a number of issues, including, but not limited to, high dynamic topology, limited and variable capacity, limited energy resources, a high bit error rate, a multihop topology, and the hidden terminal problem. The requirements of existing and future multicast routing protocols and the issues associated with these protocols that should be taken into consideration are listed in what follows[2, 3, 6]. It is very important to take into account the nondeterministic characteristics (power and capacity limitations, random mobility, etc.) of the MANET environment in coping with this issue.

1. Topology, Mobility, and Robustness
2. Capacity and Efficiency.
3. Energy Consumption.
4. Quality of Service and Resource Management.
5. Security and Reliability.
6. Scalability

2.1 Topology, Mobility and Robustness

In MANETs [14], nodes are free to move anyplace, any time, and at completely different speeds. The random and continued movement of the nodes ends up in a extremely dynamic topology, particularly in a very high-mobility environment. A multicast routing protocol ought to be sturdy enough to react quickly with the quality of the nodes and will adapt to topological changes so as to avoid dropping a knowledge packet throughout the multicast session, which might produce a low packet delivery quantitative relation (PDR: the amount of non duplicate information packets with success delivered to every destination versus the amount of information packets presupposed to be received at each destination). It is vital to reduce management overhead whereas making and maintaining the multicast cluster topology, particularly in an environment with restricted capacity.

2.2 Capacity and Efficiency

Unlike wired networks, MANETs are characterised by scant capability caused by the noise and interference inherent in wireless transmission and multipath attenuation [9]. Efficient multicast routing protocols are expected to produce a good variety of management packets transmitted through the network relative to the quantity of knowledge packets reaching their destination intact, and ways to boost and increase the offered capability got to be considered.

2.3 Energy Consumption

Energy potency is a very important thought in such associate surroundings. Nodes in MANETs rely on restricted battery power for their energy. Energy saving techniques geared toward minimizing the full power consumption of all nodes within the multicast cluster (minimize the quantity of nodes to establish multicast property[10], minimize the quantity of overhead controls, etc.) and at increasing the multicast lifetime ought to be thought of.

2.4 Quality of Service and Resource Management

Providing quality of service (QoS) assurance is one amongst the best challenges in coming up with algorithms for painter multicasts. Multicast routing protocols ought to be able to reserve totally different network resources to realize QoS needs like, capacity, delay, delay jitter, and packet loss [2]. It is terribly troublesome to fulfill all QoS needs at constant time attributable to the peculiarities of ad hoc networks. Although this can be done, the protocol are going to be terribly complicated (many routing tables, high management overhead, high energy consumption, etc.). As a result, doing therefore will not be appropriate for these networks with their scarce resources, and resource management and adaptive QoS ways are more convenient than reservation ways for MANETs.

2.5 Security and Reliability.

Security provisioning could be a crucial issue in MANET multicasting owing to the broadcast nature of this kind of network, the existence of a wireless medium, and therefore the lack of any centralized infrastructure. This makes MANETs vulnerable to eavesdropping, interference, spoofing, and so forth. Multicast routing protocols ought to take this into consideration, particularly in some applications like military (battlefield) operations, national crises, and emergency operations. Reliability is especially vital in multicasting, particularly in these applications,[6] and it becomes harder to deliver reliable knowledge to cluster members whose topology varies. A reliable multicasting style depends on the answers of the subsequent 3 queries. By whom are the errors detected? How are error messages signaled? How are missing packets retransmitted?

2.6 Scalability

A multicast routing protocol ought to be able to give an appropriate level of service during a network with an outsized variety of nodes.

3. TAXONOMY OF ROUTING PROTOCOLS

A routing protocol is required whenever a packet must be transmitted to a destination via range of nodes and diverse routing protocols are planned for such kind of ad hoc networks. These protocols realize a route for packet delivery and deliver the packet to the right destination. The studies on varied aspects of routing protocols are an energetic space of analysis for several years. Many protocols are steered keeping applications and sort of network in sight. Basically, routing protocols are often loosely classified into 2 sorts as (a) Table Driven Protocols or Proactive Protocols and (b) On-Demand Protocols or Reactive Protocols

Table Driven or Proactive Protocols:

In Table Driven routing protocols every node maintains one or a lot of tables containing routing data to each alternative node within the network. All nodes carry on change these tables to keep up latest read of the network. Some of the existing table driven or proactive protocols are: DSDV [17], [19], DBF [7], GSR [21], WRP [21] and ZRP [21],OSLR[19][21]

On Demand or Reactive Protocols:

In these protocols, routes square measure created as and once needed. once a transmission happens from source to destination, it invokes the route discovery procedure. The route remains valid until destination is achieved or till the route is no longer required. Some of the present on demand routing protocols are: DSR[4] [8][17],AODV [3], [8] and TORA [21].

The emphasis during this analysis paper is targeting the survey and comparison of varied On Demand/Reactive Protocols like DSR, AODV and TORA as these square measure best suited for Ad Hoc Networks. The successive sub-section describes the fundamental options of those protocols.

3.1 DYNAMIC SOURCE ROUTING

Dynamic source Routing (DSR) is a commercial Hoc routing protocol [4][8] that relies on the idea of source-based routing instead of table-based. This protocol is source-initiated instead of hop-by-hop. This can be significantly designed to be used in multi hop wireless accidental networks of mobile nodes. Basically, DSR protocol does not need any existing network infrastructure or administration and this permits the Network to be fully self-organizing and self-configuring. This Protocol consists of 2 essential elements of route discovery and route maintenance. Each node maintains a cache to store recently discovered methods. Once a node wishes to send a packet to some node, it first checks its entry within the cache. If it is there, then it uses that path to transmit the packet and conjointly attach its source address on the packet. If it is not there within the cache or the entry in cache is expired (because of lasting idle), the sender broadcasts a route request packet to any or all of its neighbors requesting a path to the destination. The sender are waiting until the route is discovered. Throughout waiting time, the sender will perform different tasks like sending/forwarding different packets. As the route request packet arrives to any to the nodes, they check from their neighbor or from their caches whether or not the destination asked is thought or unknown. If route information is known, they challenge a route reply packet to the destination otherwise they broadcast constant route request packet. Once the route is discovered, the desired packets are transmitted by the sender on the discovered route. Also an entry in cache entry within the cache is inserted for the long run use.

The node also will maintain the age info of the entry thus on understand whether or not the cache is recent or not. When a data packet is received by any intermediate node, it first checks whether or not the packet is supposed for itself or not. If it is meant for itself (i.e. the intermediate node is that the destination), the packet is received otherwise constant are forwarded victimization the trail connected on the information packet. Since in Ad Hoc network ,any link would possibly fail anytime. Therefore, route maintenance method can perpetually monitors and can conjointly give notice the nodes if there is any failure within the path. Consequently, the nodes will change the entries of their route cache.

Benefits and Limitations of DSR

One of the most good thing about DSR protocol is that there is no need to keep routing table thus on route a given knowledge packet as the entire route is contained within the packet header. the constraints of DSR protocol is that this can be not ascendible to large networks and even needs considerably additional process resources than most different protocols. Basically, In order to get the routing information, every node should pay lot of time to method any management knowledge it receives, not withstanding it is not the supposed recipient.

3.2 ADOV (AD HOC ON DEMAND DISTANCE VECTOR)

AODV [4],[5] is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol that is conjointly supported DSDV and DSR. It aims to attenuate the necessity of system-wide broadcasts to its extreme. It does not maintain routes from each node to each different node within the network rather are they are discovered as and once required & are maintained solely as long as they are needed. The key steps of algorithm employed by AODV for establishment of unicast routes area unit explained below.

3.2.1 Route Discovery

When a node desires to send a data packet to a destination node, the entries in route table are unit checked to make sure whether or not there is a current route to it destination node or not. If it is there, the data packet is forwarded to the acceptable next hop toward the destination. If it is not there, the route discovery method is initiated. AODV initiates a route discovery method victimization Route Request (RREQ) and Route Reply (RREP). The source node will produce a RREQ [18] packet containing its IP address, its current sequence number, the destination’s IP address, the destination’s last sequence number and broadcast ID. The broadcast ID is incremented on every occasion the source node initiates RREQ. Basically, the sequence numbers are used to verify the timeliness of every data packet and he broadcast ID & the IP address along kind a novel symbol for RREQ thus on unambiguously determine each request. The requests are sent using RREQ message and therefore the information in reference to creation of a route is sent back in RREP message.

The source node broadcasts the RREQ packet to its neighbours so sets a timer to attend for a reply. To process the RREQ, the node sets up a reverse route entry for the source node in its route table. This helps to understand a way to forward a [18] RREP to the source. Essentially a life is related to the reverse route entry and if this entry is not used among this life, the route info is deleted. If the RREQ is lost throughout transmission, the source node is allowed to broadcast once more victimization route discovery mechanism.

3.2.2 Expanding Ring Search Technique

The source node broadcasts the RREQ packet to its neighbours that successively forwards constant to their neighbours so forth. Especially, just in case of enormous network, there is a desire to regulate network-wide broadcasts of RREQ to regulate the same; the source node uses an expanding ring search technique. In this technique, the source node sets the Time to Live (TTL) value of the RREQ to an initial start value. If there is no reply among the invention amount, consecutive RREQ is broadcasted with a TTL value inflated by an increment value. The method of incrementing TTL value continues till a threshold value is reached, once that the RREQ is broadcasted across the whole network.

3.2.3 Setting up of Forward Path

When the destination node or intermediate node with a route to the destination receives the RREQ, it creates the RREP and unicast constant towards the source node victimization the node from that it received the RREQ because the next hop. When RREP is routed back on the reverse path and received by an intermediate node, it sets up a forward path entry to the destination in its routing table. When the RREP reaches the source node, it means that a route from source to the destination has been established and therefore the source node will begin the data transmission.

3.2.4 Route Maintenance

A route discovered between a source node and destination node is maintained as long as needed by the source node. Since there is movement of nodes in mobile accidental network and if the source node moves throughout a lively session [20], it will reinitiate route discovery mechanism to determine a brand new route to destination. Conversely, if the destination node or some intermediate node moves, the node upstream of the break initiates Route Error (RERR) message to the affected active upstream neighbors/nodes. Consequently, these nodes propagate the RERR to their forerunner nodes. This method continues till the source node is reached. once RERR is received by the source node, it will either stop causing the info or reinitiate the route discovery mechanism by causing a brand new RREQ message if the route continues to be needed.

3.2.5 Edges and Limitations of AODV

The benefits of AODV protocol area unit that it favors the smallest amount engorged route rather than the shortest route and it conjointly supports each unicast and multicast packet transmission seven for nodes in constant movement. It conjointly responds terribly quickly to the topological changes that affects the active routes. AODV does not place any extra overheads on knowledge packets because it does not build use of source routing.

The limitation of AODV protocol is that it expects/requires that the nodes within the broadcasting will sight every others' broadcasts. it\'s conjointly attainable that a sound route is expired and therefore the determination of an inexpensive termination time is tough. the rationale behind this can be that the nodes area unit mobile and their causing rates could dissent wide and might amendment dynamically from node to node. additionally, because the size of network grows, varied performance [16] metrics begin decreasing. AODV is liable to varied sorts of attacks because it supported the belief that each one nodes should collaborate and while not their cooperation no route will be established.

3.3 TORA (TEMPORARY ORDERED ROUTING PROTOCOL)

TORA may be a distributed extremely adaptative routing protocol designed to control during a dynamic multihop network. TORA uses an arbitrary height parameter to work out the direction of link between any 2 nodes for a given destination. Consequently, multiple routes typically exist for a given destination however none of them ar essentially the shortest route. To initiate a route, the node broadcasts a question packet to its neighbors. this question is rebroadcasted through the network till it reaches the destination or Associate in Nursing intermediate node that features a route to the destination. The recipient of the question packet then broadcasts the UPDATE packet that lists its height with regard to the destination. once this packet propagates within the network, every node that receives the UPDATE packet sets its height to a value larger than the peak of the neighbour from that the UPDATE was received. This has the result of making a series of directed links from the initial sender of the question packet to the node that originally generated the UPDATE packet. once it absolutely was discovered by a node that the route to a destination is not any longer valid, it will alter its height in order that it will be an area most with regard to its neighbours then transmits Associate in Nursing UPDATE packet.. When a node detects a network partition, it will generate a transparent packet that leads to reset of routing over the ad hoc network.

Benefits and Limitations of TORA

One of the advantages of TORA is that the multiple routes between any source destination try ar supported by this protocol. Therefore, failure or removal of the nodes is quickly ressolved while not source intervention by shift to an alternate route [11]. TORA is additionally not free from limitations. The dependence of this protocol on intermediate lower layers sure as shooting practicality presumes that the link standing sensing, neighbor discovery, so as packet delivery and address resolution are all without delay accessible. This can create the overhead for this protocol tough to cut loose that obligatory by the lower layer.

4. PERFORMANCE METRICS

There square measure range of qualitative and quantitative metrics which will be wont to compare reactive routing protocols. Most of the prevailing routing protocols make sure the qualitative metrics. Therefore, the subsequent totally different quantitative metrics are thought-about to form the comparative study of these routing protocols through simulation.

4.1 Routing overhead

This metric describes what percentage routing packets for route discovery and route maintenance got to be sent therefore on propagate the information packets.

4.2 Average Delay

This metric represents average end-to-end delay and indicates however long it took for a packet to travel from the source to the appliance layer of the destination. it\'s measured in seconds.

4.3 Throughput

This metric represents the full range of bits forwarded to higher layers per second [15]. it's measured in rate. It can even be outlined because the total quantity of knowledge a receiver really receives from sender divided by the time taken by the receiver to get the last packet.

4.4 Media Access Delay

The time a node takes to access media for beginning the packet transmission is termed as media access delay. The delay is recorded for every packet once it is sent to the physical layer for the primary time.

4.5 Packet Delivery Ratio

The magnitude relation between the number of incoming knowledge packets and really received knowledge packets .

4.6 Path optimality

This metric may be outlined because the distinction between the trail really taken and therefore the absolute best path for a packet to achieve its destination.

5. CONCLUSION

In this analysis paper, an attempt has been created to target the comparative study and performance analysis of assorted on demand/reactive routing protocols (DSR, AODV and TORA) on the idea of higher than mentioned performance metrics. The results after analysis have mirrored in Table1 and Table2. The Table 1 shows the description of parameters selects with reference to low mobility and lower traffic. It is been discovered that the performance of all protocols studied was virtually stable in distributed medium with low traffic. TORA performs far better in packet delivery due to choice of higher routes mistreatment acyclic graph. Table 2 shows the analysis of same parameters with increasing speed and providing additional nodes. The results indicate that AODV keeps on up with denser mediums and at quicker speeds.

The analysis predicts that in spite of slightly additional overhead in some cases DSR and AODV outperforms TORA all told cases. AODV remains higher in Route updation and maintenance method. It is been any over that owing to the dynamically ever-changing topology and infrastructure less, decentralised characteristics, security and power awareness is tough to attain in mobile ad hoc networks. Hence, security and power awareness mechanisms ought to be constitutional options for all kinds of applications supported ad hoc network. The main target of the study is on these problems in our future analysis work and effort are created to propose an answer for effective routing in ad hoc networks by endeavour these core problems with secure , minimum overhead , power aware/energy economical routing.

Table 1: Metrics W.R.T Low Mobility

Protocol	Routing Overhead	Average end to end delay	Packet Delivery Ratio	Path Optimality
DSR	Low	Average	High	Average
AODV	Low	Average	High	Average
TORA	Moderate	Low	High	Good

Table 2: Metrics W.R.T High Mobility

Protocol	Routing Overhead	Average end to end delay	Packet Delivery Ratio	Path Optimality
DSR	Average	Average	Average	Low
AODV	Very High	Average	Average	Average
TORA	High	More	Low	Average

REFERENCES

1. Falko Dressler _ Mario Gerla ,” A Framework For Inter-Domain Routing In Virtual Coordinate Based Mobile Networks”, Wireless Networks ,Vol 10.1007/S11276-013-0554-4 27 February 2013.
2. Zehua Wang, Student Member, IEEE, Yuanzhu Chen, Member, IEEE, Cheng Li, Senior Member, IEEE,” CORMAN: A Novel Cooperative Opportunistic Routing Scheme In Mobile Ad Hoc Networks”, IEEE Journal On Selected Areas In Communications, Vol. 30,No. 2, February 2012.
3. Shinsuke Kajioka , Naoki Wakamiya , Hiroki Satoh b, Kazuya Monden Masato Hayashi,Susumu Matsui , Masayuki Murata,” A QoS-aware routing mechanism for multi-channel multi-interface ad-hoc networks”, Elsevier , 1570-8705,15 October 2010.
4. Deepesh Man Shrestha , Cheolgi Kim , Young-Bae Ko ,” A Reliable Multi-Grid Routing Protocol for Tactical MANETs”, IEEE Transactions Wireless Networking, C1090-1121-0011, 2012.
5. Kaushik R. Chowdhury, Member, IEEE, and Ian F. Akyildiz, Fellow, IEEE,” CRP: A Routing Protocol for Cognitive Radio Ad Hoc Networks”, IEEE Journal On Selected Areas In Communications, VOL. 29, NO. 4, APRIL 2011.
6. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma,” A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, Journal Of Computing, Volume 3, Issue 1, Issn 2151-9617 January 2011.
7. Hassan Aboubakr Omar, Student Member, IEEE,Weihua Zhuang, Fellow, IEEE, and Li Li, Member, IEEE,” VeMAC: A TDMA-Based MAC Protocol for Reliable Broadcast in VANETs ”,IEEE Transactions On Mobile Computing, VOL. 12, NO. 9, September 2013.
8. Xin Ming Zhang, Member, IEEE, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, Senior Member, IEEE,” An Estimated Distance-Based Routing Protocol for Mobile Ad hoc Networks”, IEEE Transactions On Vehicular Technology, Vol. 60, No. 7, 3473 September 2011.
9. Milena Radenkovic , Andrew Grundy,” Efficient And Adaptive Congestion Control For Heterogeneous Delay-Tolerant Networks”, Elsevier, 1570-8705, 20 April 2012.
10. Mariam Kaynia, Student Member, IEEE, Nihar Jindal, Member, IEEE, and Geir E. Øien,Senior Member, IEEE,” Improving the Performance of Wireless Ad Hoc Networks Through MAC Layer Design”, IEEE Transactions On Wireless Communications, Vol. 10, No. 1, January 2011.
11. Hanan Saleet, Member, IEEE, Rami Langar, sMember, IEEE, Kshirasagar Naik, Senior Member, IEEE,Raouf Boutaba, Senior Member, IEEE, Amiya Nayak, Senior Member,IEEE, and Nishith Goel,” Intersection-Based Geographical Routing Protocolfor VANETs:A Proposal and Analysis”IEEE Transactions On Vehicular Technology”, Vol. 60, No. 9, November 2011.
12. Majid Khabbazian, Ian F. Blake Fellow, IEEE, Vijay K. Bhargava, Fellow, IEEE,” Local Broadcast Algorithms in Wireless Ad Hoc Networks: Reducing the Number of Transmissions”,IEEE Transactions on Mobile Computing, Page(s): 402 – 413,2012.
13. Javad Akbari Torkestani , Mohammad Reza Meybodi ,” Mobility-based multicast routing algorithm for wireless mobile Ad-hoc networks:A learning automata approach”, Elsevier,0140-3664 2009 ,November 2009.
14. Jin Hee Cho, AnanthramSwami , Ing-RayChen ,”Modeling and analysis of trust management with trust chain optimization

in mobile ad hocnetworks ",Elsevier , 1084-8045,March 2011.

15. Marcello Caleffi, Member, IEEE, Ian F. Akyildiz, Fellow, IEEE, and Luigi Paura, Member,IEEE," OPERA: Optimal Routing Metric for Cognitive Radio Ad Hoc Networks",IEEE Transactions On Wireless Communications, Vol. 11, No. 8, August 2012.
16. Pu Wang , Ian F. Akyildiz ,Abdullah M. Al-Dhelaan," Percolation theory based connectivity and latency analysis of cognitive radio ad hoc networks", Wireless Networks, Vol 17:659–669,1276-010-0304-9,2010.
17. Rajeshwar Singh, Dharmendra K Singh, Lalan Kumar," Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks",International Journal of Advanced Networking and Applications ,Volume: 02, Issue: 04, Pages: 732-737 ,2011.
18. Karim El Defrawy, Member, and Gene Tsudik, Senior Member," Privacy-Preserving Location-Based On-Demand Routing in MANETs",IEEE Journal On Selected Areas In Communications, Vol. 29, No. 10, December 2011.
19. M.Pushpavalli1 Dr.A.M.Natarajan2," Quality of Service in Mobile Ad hoc Networks using Two Bandwidth Estimation Method in Optimized Link State Routing protocol",International Journal of Computer Science and Network Security, VOL.12 No.1, January 2012.
20. Angela Sara Cacciapuoti , Marcello Caleffi , Luigi Paura," Reactive routing for mobiless cognitive radio ad hoc networks" ,Elsevier, 1570-8705,October 2010.
21. Gagangeet Singh Ajula,Sandeep Singh Kang "Comprehensive Evaluation Of AODV,DSR,DSR,GRP,OLSR and Tora Routing Protocols with varying number of nodes and traffic applications over MANETs", IOSR Journal of Computer Engineering ,2278-0661vol 9,Apr 2013.