Performance Comparison of Various Routing Protocols with Varying Number of Source Nodes

Kuldeep Singh
Department of Computer Science and Engineering
Jind Institute of Engineering and Technology, Jind, Haryana, India

Dr. Rajesh Verma
Department of Computer Science and Engineering
Kurukshetra Institute of Technology and Management, Kurukshetra, Haryana, India

Abstract- A Mobile Ad hoc Network (MANET) is a collection of wireless network that can exchange information dynamically, instead of using a central base station (access point) to which all computers must communicate. The routing protocols i.e. proactive, reactive and hybrid in an ad hoc network should be able to deal well with dynamically changing topology and nodes should exchange information on the topology of the network, in order to establish routes. In this paper, a comprehensive attempt has been made to compare the performance of three prominent reactive protocols DSR, AODV, CBRP. A simulation model has been used to study their performance using network simulator as GloMOSim-2.03 by measuring the metrics like Packet Delivery Ratio, End-to-End Delay and Normalized packet overhead.

Keywords – MANET, AODV, DSR, CBRP, PDR,GloMoSim.

I. INTRODUCTION

A mobile ad hoc network (MANET) [1] is a group of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. A MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes. It is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).

For the security issue in an ad hoc network and make it secure there are number of security goals that must be present in MANET. These goals are authentication, confidentiality, integrity, availability and non-repudiation [3]. The scopes of the adhoc network are also associated with Dynamic topology changes, Bandwidth-constrained, Energy constrained operation, Limited physical security, Mobility-induced packet losses, Limited wireless transmission range, Broadcast nature of the wireless medium, Hidden terminal problem, Packet losses due to transmission errors[4,5]. Routing in ad hoc networks has become a popular research topic. These MANET routing protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [3][4], nodes find routes only when required, DSR[4] in which data packets carry the source route in the packet header and in CBRP[6] the nodes of a wireless network are divided into several disjoint or overlapping clusters.

II. OVERVIEW OF ADHOC ROUTING PROTOCOLS

2.1 AODV (Ad Hoc on Demand Distance Vector Routing Protocol)

Ad Hoc On Demand Distance Vector (AODV) AODV [1,2] is perhaps the most well-known routing protocol for a MANET. It is a reactive protocol: nodes in the network exchange routing information only when a communication must take place and keep this information up-to-date only as long as the communication lasts.

When a node must send a packet to another node, it starts a route discovery process in order to establish a route toward the destination node. Therefore, it sends its neighbors a route request message (RREQ). Neighboring nodes receive the request, increment the hop count, and forward the message to their neighbors, so that RREQs are actually broadcasted using a flooding approach. The goal of the RREQ message is to find the destination node, but it also has the side effect of making other nodes learn a route towards the source node (the reverse route): a node that has received a RREQ message, with source address S from its neighbor A, knows that it can reach S through A and records this information in its routing table along with the hop count (i.e., its distance from node S following that route).

The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast, using the path towards the source node established by the RREQ. Similarly to what happens with RREQs, the RREP message allows intermediate nodes to learn a route toward the destination node.

Therefore, at the end of the route discovery process, packets can be delivered from the source to the destination node and vice versa.

A third kind of routing message, called route error (RERR), allows nodes to notify errors, for example, because a previous neighbor has moved and is no longer reachable. If the route is not active (i.e., there is no data traffic flowing through it), all routing information expires after a timeout and is removed from the routing table.

2.2 DSR (Dynamic Source Routing)

The key distinguishing feature of DSR is the use of source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a *route cach*e. The data packets carry the source route in the packet header. When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a *route discovery* process to dynamically determine such a route [4]. Route discovery works by flooding the network with *route request* (RREQ) packets. Each node receiving an RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a *route reply* (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path backward. The route carried back by the RREP packet is cached at the source for future use. If any link on a source route is broken, the source node is notified using a *route error* (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed. DSR makes very aggressive use of source routing and route caching.

2.3 CBRP (Cluster Based Routing Protocol)

In CBRP the nodes of a wireless network are divided into several disjoint or overlapping clusters. Each cluster elects one node as the so-called clusterhead. These special nodes are responsible for the routing process. Neighbours of clusterhead cannot be clusterhead as well. But clusterhead are able to communicate with each other by using gateway nodes.

A gateway is a node that has two or more clusterhead as its neighbors or when the clusters are disjoints at least one clusterhead and another gateway node. The routing process itself is performed as source routing by flooding the network with a route request message. Due to the clustered structure there is less traffic, because route requests are passed only between clusterhead.

2.3.1 Cluster Formation

Gerla and Tsai [6] found out, that identifier-based clustering is a better choice than connectivity-based clustering according to node movement. When using identifier-based clustering a node elects itself as the clusterhead if it has the lowest/highest ID in its neighborhood or a neighbor node if one has a lower ID. Connectivity-based clustering elects the node, which has the most neighbor nodes, as the clusterhead. So, whenever a clusterhead looses a neighbor node its connectivity decreases and it is most likely that another node has to be elected to act as clusterhead. While in the identifier-based approach, a new clusterhead has to be chosen only when nodes with lower/higher ID appear [6] [7].

2.3.2 Routing

CBRP uses two data structures to support the routing process: the cluster adjacency table (CAT) and the two-hop topology database. The CAT stores information about neighboring clusters. This is, whether they are bi-directonally or uni-directionally linked. That means, a cluster is called

• *Bi-directionally linked* if there is a bi-directional link between two nodes of the clusters, or if there are at least two opposite uni-directional links between two nodes.

• *Uni-directionally linked* if there is just one uni-directional link between them.

2.3.3 Route Discovery

Route discovery is done by using source routing. In the CBRP only clusterheads are flooded with route request package (RREQ). Gateway nodes receive the RREQs as well, but without broadcasting them. They forward them to the next clusterhead. This strategy reduces the network traffic. Initially, node S broadcasts a RREQ with unique ID containing the destination’s address, the neighbouring clusterhead(s) including the gateway nodes to reach them and the cluster address list which consists of the addresses of the clusterheads forming the route.

III. DESIGN OF THE EXPERIMENT & SIMULATION SETUP

The method for analyzing the routing protocols traffic is to begin with a carefully designed base configuration and network scenario for the experiment, and to vary the node density and mobility at a time to stress the network in different directions. Careful selection of these control parameters enables us to assess and isolate the effect of network size, with fixed application traffic CBR. In addition, design of the base condition, network topology, and routing are to be taken into account the real networks for which the results should be applicable. In this experiment, we noted down the throughput, collisions and energy consumption values for various few node. In the beginning of the experiment, the initial settings of the node and simulation times were thoroughly checked out. Care also is taken in selection of the terrain dimension, disabling the unnecessary filter components in the simulator settings.

The experiment is continued for different proactive and reactive protocols, we noted down the throughput, collisions and energy consumption after each simulation of the simulator.

We selected the terrain dimensions as 1200m x1000m, and nodes in the terrain are mobile. We fixed the simulation time 1000S by setting the minimum mobility speed 0 meter/second to 25 meter/second for all the node with 100 mobile node participating in the network and making the 10, 20, 30, 40, 50 CBR links. This simulation experiment is done by using the all three reactive routing protocol described earlier by using the GloMoSim network simulator [8][9]. The Global Mobile information systems Simulation provide a salable simulation environment for large wireless and wired communication network. It was designed as a set of library modules, each of which simulates a communication protocol in the protocol stack. GloMoSim simulates networks upto thousand nodes linked by heterogeneous communications capabilities that include multicast, asymmetric communications using direct satellite broadcasts.

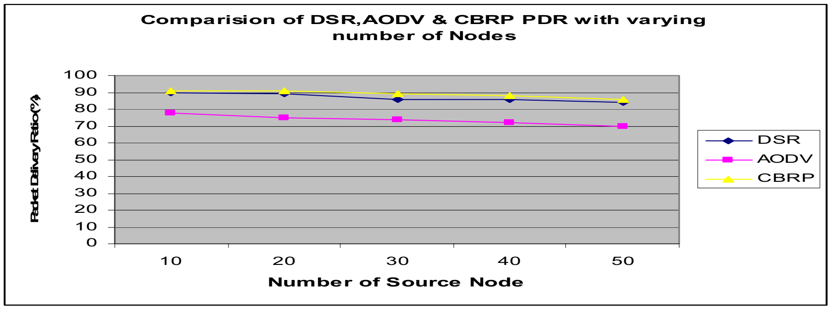
Table 1 Simulation Setup

Parameter	**Values**	**Description**
Simulation time (Sec)	1000S	Maximum execution time
Terrain Dimensions (Meters)	1200M,1000 M	Physical area in which the nodes are placed
Number of Nodes	100	Nodes participating in the network
Routing Protocols	CBRP, DSR,AODV	Routing protocol used
Traffic Model	CBR	Constant Bit Rate link used
Pause Time (Sec)	60	Mobility Pause Time Used
Node Placement	Random	Node placement policy
Mobility	0-25 (m/s)	Speed of node with which they are moving
MAC-Protocol	802.11	MAC layer protocol used

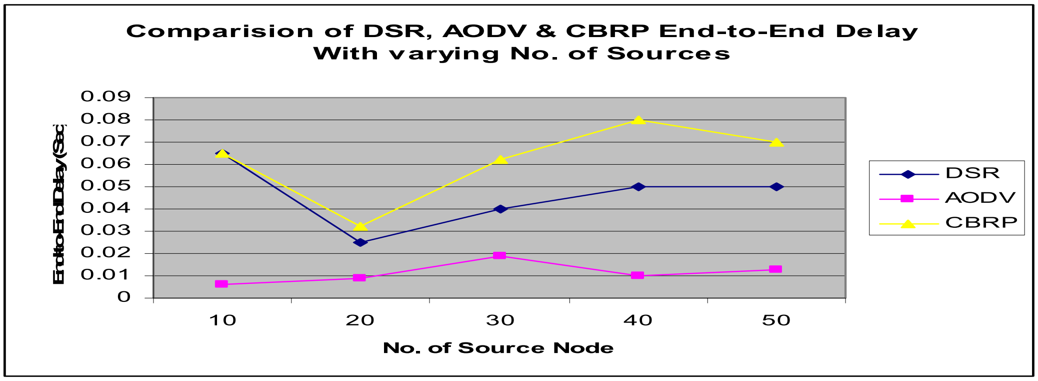
IV. EXPERIMENTAL RESULTS AND ANALYSIS

The following performance metrics are chosen to evaluate the comparison of the selected routing protocols.

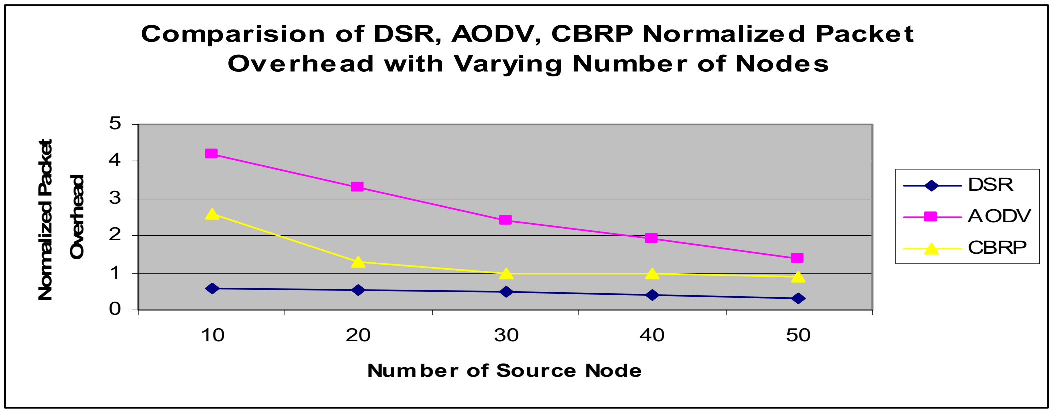
(i) Packet Delivery Ratio (PDR): It is the ratio of number of data packets actually sent to the data packets actually received by the destination. This is the best parameter to evaluate the performance of a network.



ii) End-to-End delay: The delay is the total latency experienced by a packet to traverse the network from the source to the destination. At the network layer, the end-to-end packet latency is the sum of processing delay, packetization, transmission delay, queuing delay, and propagation delay. The end-to-end delay of a path is the summation of the node delay at each node plus the link delay at each link on the path.



iii) Normalized Routing Overhead: This metric has two variants: packet overhead is the number of routing packets “transmitted” per data packet “delivered” at the destination, and byte overhead is the number of bytes of routing packets “transmitted” per data byte “delivered” at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.



V. CONCLUSION AND FUTURE SCOPE

In this paper, we compared the routing protocols based on significant performance metrics like Packet Delivery Ratio, End-to-end delay and Normalized Packet Overhead. After the simulation results it is observed that the packet delivery ratio is more in case of CBRP than that of DSR and AODV. But AODV outperform in end-to-end delay than that of CBRP and DSR. In the third performance metric DSR is best than both of the protocol. This work can be extended by nitty-gritty study of routing protocol and it would be significant to consider other performance parameters like throughput, energy consumption and number of hop counts etc.

VI. REFERENCE

[1] M. F. Juwad, and H. S. Al-Raweshidy, "*Experimental Performance Comparisons between SAODV & AODV*", IEEE Second Asia International Conference on Modelling & Simulation, 2008.

[2] Davide Cerri and Alessandro Ghioni, "*Securing AODV: The A-SAODV Secure Routing Prototype*", IEEE Communications Magazine, February 2008.

[3] L. Zhou and Z. Haas. "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security. Pages 24-30, November/December 1999.

[4] Lars Michael Kristensen, "An Introduction to Ad Hoc Networking" Department of Computer Science University of Aarhus.

[5] "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" Georgia Institute of Technology.

[6] Mario Gerla and Jack Tzu-Chieh Tsai. Multicluster, mobile, multimedia radio network. ACM-Baltzer Journal of Wireless Networks, 1(3):255–265, 1995.

[7] Martha Steenstrup. Cluster-based networks. In Charles E. Perkins, editor, Ad hoc networking, chapter 4, pages 75–138. Addison-Wesley, 2001.

[8] GloMoSim;Available on: htttp://pcl.cs.ucla.edu/projects/g;omosim.

[9] L. Bajaj, M.Takai, R. Ahuja, R. Bagrodia, and M. Gerla; "Glomosim: A scalable network simulaion environment"; Technical Report 990027, UCLA Computer Science Department; 1999; Available on: citeseer.ist.psu.edu/225197.html.

[10] Kuldeep Singh, Dr Anil Kr Kapil, Dr. Yudhvir Singh "Throughput, Collisions and Energy Consumption Comparision of MANET Routing Protocols", National Conference on Advances in Computing, Communication Networks & Electrical Systems (NCACCNES-2012) March 27-28, 2012 A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.