INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Performance Analysis Of ODV,OLSR,DSR And GRP Routing Protocols Of Adhoc Networks

Suchita Baxla
Dept. Electronics And Communication, Nri Institute Of Information Science & Technology, Bhopal (M.P) India
Rajesh Nema
Dept. Electronics And Communication, Nri Institute Of Information Science & Technology, Bhopal (M.P) India

Abstract*:*

A mobile ad hoc network(manet) consists of mobile wireless nodes. The communnication bet ween these mobile nodes is carried out without any centralized control.The ease of deployment and the infrastructure less nature of mobile ah hoc networks(manet) make them highly desirable for the preset day multi media communications.Tr additional routing protocols may not suffice for real time communications it depends upon the condition and our requirements.Though there has been considerable research in this area.In this paper we are analyzing the performance of routing protocol via increasing number of nodes. . Here we are observing performance of routing protocol by making a comparison between dcf (Distributed Coordination Function) and edcf (Enhanced Distributed Coordination Function) on the basis of following parameters :- delay,throughput, traffic sent and traffic received .Network simulation tool used in simulation is opnet modeler(ver.14)

Keywords*: :Manet, Aodv, Olsr, Grp, Dsr.*

1. Introduction

Manet represent a system of wireless mobile nodes that can freely and dynamically self organize in to arbitrary and temporary network topologies,allowing people and devices to communicate without any preexisting communication architecture.Each node in the network also acts as a router,forwarding data packets for other nodes.The absence of fixed infrastructure in a manet poses several types of challenges.The biggest challenges among them is routing.Routing is the process of selecting paths in a network along which to send data packets. An adhoc routing protocol is a convention or standard that controls how nodes decide which way to route packets between computing devices in a mobile adhoc network.In adhoc networks, nodes do not start out familiar with the topology of their network instead,they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors.Each nodes learns about nearby nodes and how to reach them and may announce that it can reach them too. Different protocols are then evaluated based on the packet drop rate,average routing load,average end-to-end delay and other measures.The proposed solution for routing protocols could be grouped in three categories-proactive(or table driven),reactive (or on demand)and hybrid protocols.

2. Manet Routing Protocols

Mobile adhoc network characterized by the mobility of its nodes each nodes can join and leave the network at any time,this means that the topology of the network also may changes at any time.These make the design of the mobile ad hoc network not an easy task and it become one of the most important manet challenges.There are different criteria for designing and classifying routing protocols for wireless adhoc networks.For example,what routing information is exchanged,when and how the routing information is exchanged, when and how routes are computed etc.Classification of routing protocols in manet`s can be done in many ways,but most of these are done depending on routing strategy and network structure.According to the routing strategy the routing protocols can be categorized as table-driven and on demand(source initiated),while depending on the network structure these are classified as flat routing,hierarchical routing and geographic postion assisted routing.both the table- driven and on demand protocols come under flat routing.One of the most popular methods to distinguish mobile adhoc network routing protocols is based on how routing information is acquired and maintained by mobile nodes.Using this method,mobile adhoc

network routing protocol can be divided into proactive routing,also called or table-driven routing protocol,reactive routing also called on demand routing protocols and hybrid routing.Hybrid routing protocols are proposed to combine the merits of both proactive and reactive routing protocols and overcome their short comings.

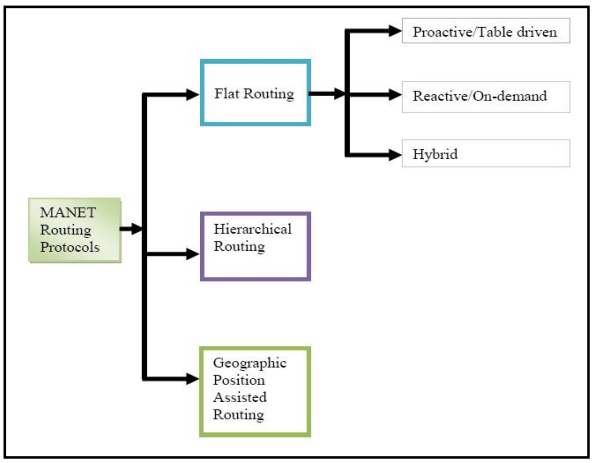

Figure 1:Shows The Classification Of Manet Routing Protocols

2.1Reactive routing protocol.

2.1.1Ad Hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance Vector routing protocol (AODV) is an improvement of the Destination-Sequenced Distance Vector routing protocol (DSDV). DSDV has its efficiency in creating smaller ad-hoc networks. Since it requires periodic advertisement and global dissemination of connectivity information for correct operation, it leads to frequent system-wide broadcasts. Therefore the size of DSDV ad-hoc networks is strongly limited. When using DSDV, every mobile node also needs to maintain a complete list of routes for each destination with inthe mobile network. The advantage of AODV is that it tries to minimize the number of required broadcasts. It creates the routes on a on-demand basis, as opposed to maintain a complete list of routes for each destination.

2.1.2 Path Discovery Process

When trying to send a message to a destination node without knowing an active route to it, the sending node will initiate a path discovery process. A route request message (RREQ) is broadcasted to all neighbors, which continue to broadcast the message to their neighbors and so on. The forwarding process is continued until the destination node is reached or until a intermediate

node knows a route to the destination that is new enough. To ensure loop-free and most recent route information, every node maintains two counters: sequence number and broadcast_id. The broadcast_id and the address of the source node uniquely identify a RREQ message. broadcast_id is incremented for every RREQ the source node initiates. An intermediate node can receive multiple copies of the same route request broadcast from various neighbors. In this case –if a node has already received a RREQ with the same source address and broadcast_id – it will discard the packet without broadcasting it furthermore. When an intermediate node forwards the RREQ message, it records the address of the neighbor from which it received the first copy of the broadcast packet. This way, the reverse path from all nodes back to the source is being built automatically. The RREQ packet contains two sequence numbers: the source sequence number and the last destination sequence number known to the source. The source sequence number is used to maintain "freshness" information about the reverse route to the source while the destination sequence number specifies what actuality a route to the destination must have before it is accepted by the source.

When using Destination-Sequenced Distance Vector routing, every mobile node in the network maintains a routing table where it lists all possible destinations within the network and the corresponding hop counts to them. The protocol requires periodic advertisement of the routing information throughout the entire network by using full dump and incremental packets. This potentially large amount of network traffic strongly limits the use of this protocol to small ad-hoc networks. A route is considered active if it has an entry in the routing table that is marked as valid. Active routes expire after a certain amount of time or on occurence of a link failure. Only active routes can be used to forward data packets When the route request broadcast reaches the destination or an intermediate node with a fresh

enough route, the node responds by sending a unicast route reply packet (RREP) back to the node from which it received the RREQ. So actually the packet is sent back reverse the path built during broadcast forwarding. A route is considered fresh enough, if the intermediate node's route to the destination node has a destination sequence number which is equal or greater than the one contained in the RREQ packet. As the RREP is sent back to the source, every intermediate node along this path adds a forward route entry to its routing table. The forward route is set active for some time indicated by a route timer entry. If the route is no longer used, it will be deleted after the specified amount of time. Since the RREP packet is always sent back the reverse path established by the routing of time. Since the RREP packet

is always sent back the reverse path established by the routing request, AODV only supports symmetric links. Maintaining Routes -If the source node moves, it is able to send a new RREQ packet to find a new route to the destination. If an intermediate node along the forward path moves, its upstream neighbor notices the move and sends a link failure notification message to each of its active upstream neighbors to inform them of the erasure of that part of the route . The link failure notification is forwarded as long as the source node is not reached. After having learned about the failure, the source node may reinitiate the route discovery protocol. Optionally a mobile node may perform local connectivity maintenance by periodically broadcasting hello messages.

2.1.3Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol based on source routing. In the source routing technique, a sender determines the exact sequence of nodes through which to propagate a packet. The list of intermediate nodes for routing is explicitly contained in the packet's header. In DSR, every mobile node in the network needs to maintain a route cache where it caches source routes that it has learned. When a host wants to send a packet to some other host, it first checks its route cache for a source route to the destination. In the case a route is found, the sender uses this route to propagate the packet. Otherwise the source node initiates the route discovery process. Route discovery and route maintenance are the two major parts of the DSR protocol.

2.1.4.Route Discovery

For route discovery, the source node starts by broadcasting a route request packet that can be received by all neighbor nodes within its wireless transmission range. The route request contains the address of the destination host, referred to as the target of the route discovery , the source's address, a route record field and a unique identification number. At the end, the source host should receive a route reply packet containing a list of network nodes through which it should propagate the packets, supposed the route discovery process was successful. During the route discovery process, the route record field is used to accumulate the sequence of hops already taken. First of all the sender initiates the route record as a list with a single element containing itself. The next neighbor node appends itself to the list and so on. Each route request packet also contains a unique identification number called request_id. request_id is a simple counter which is increased whenever a new route request packet is

being sent by the source node. So every route request packet can be uniquely identified through its initiator's address and request_id. When a host receives a route request packet, it is important to process the request in the order described below. This way we can make sure that no loops will occur during the broadcasting of the packets. 1. If the pair of source node address, request_id is found in the list of recent route requests, the packet is discarded.2. If the host's address is already listed in the request's route record, the packet is also discarded. This ensures removal of later copies of the same request that arrive by using a loop.

3. If the destination address in the route request matches the host's address, the route record field contains the route by which the request reached this host from the source node. A route reply packet is sent back to the source node containing a copy of this route.

4. Otherwise, add this host's address to the route record field of the route request packet and re-broadcast the packet. A route reply is sent back either if the request packet reaches the destination node itself, or if the request reaches an intermediate node which has an active route to the destination in its route cache. The route record field in the request packet indicates which sequence of hops was taken. If the node generating the route reply is the destination node, it just takes the route record field of the route request and puts it into the route reply. If the responding node is an intermediate node, it appends the cached route to the route record and then generates the route reply. Sending back route replies can be accomplished in two different manners: DSR may use symmetric links, but it is not required to. In the case of symmetric links, the node generating the route reply just uses the reverse route of the route record. When using unidirectional (asymmetric) links, the node needs to initiate its own route discovery process and piggyback the route reply on the new route request.

2.1.5.Route Maintenance

Route maintenance can be accomplished by two different processes:

• Hop-by-hop acknowledgement at the data link layer

• End-to-end acknowledgements

Hop-by-hop acknowledgement at the data link layer allows an early detection and retransmission

of lost or corrupt packets. If the data link layer determines a fatal transmission error (for example, because the maximum number of retransmissions is exceeded), a route error packet is being sent back to the sender of the packet. The route error packet contains two parts of

information: The address of the node detecting the error and the host's address which it was trying to transmit the packet to. Whenever a node receives a route error packet, the hop in error is removedfrom the route cache and all routes containing this hop are truncated at that point.

End-to-end acknowledgement may be used, if wireless transmission between two hosts does not work equally well in both directions. As long as a route exists by which the two end hosts are able to communicate, route maintenance is possible. There may be different routes in both directions. In this case, replies or acknowledgements on the application or transport layer may be used to indicate the status of the route from one host to the other. However, with end-to-end acknowledgement it is not possible to find out the hop which has been in error.

2.2.Proactive Routing Protocols

2.2.1OLSR

Optimized Link State Routing (OLRS) is a topologybased, neighbor selection protocol, in which each node only maintains a subset of network topology information. OLRS is a proactive protocol, because it exchanges the topology information with other nodes regularly to maintain information required for routing. OLRS reduces the cost of distributing network-scale link-state information by two ways. First, it uses multipoint relays (MRP) to reduce redundant rebroadcasting during flooding operation. That is the key concept of the protocol. MRPs are selected nodes, which forward broadcast messages during the flooding process. Secondly each node only broadcast the state of nodes in its own multi-point relay set. That is a method to reduce the contents of the control messages. A node's multipoint relay set is the minimal subset of its one-hop neighbors, which must rebroadcast a message so that it is received by all of its two-hop neighbors. When a node sends a broadcast message, all of its neighbors receive and process the data. However, only those neighbors, which belongs to the source node's MPR set and have not previously received the message re-broadcast it. This reduces the number of broadcast messages needed to flood a message through the network. Since each node selects its MPR set independently, it must know the topology of its two-hop neighborhood, but additional inter-nodal coordination is not required. In the OLSR protocol, each node uses this flooding technique to distribute the link-state of its own MPR set. This is done periodically. The update period is in its minimum when there is detected a change and when the network is in its stabile state there is a updates only between refresh intervals. Each node uses the attained topology information to construct its routing tables. For the neighbor

sensing purposes the OLSR uses HELLO-messages, because each node should detect the neighbor interfaces with which it has a direct and symmetric link. OLSR supposes bi-directional links and so the connectivity must be checked in both directions. HELLO-messages are broadcast to all one-hop neighbors, but are not relayed to further nodes. OLSR is well suited to large and dense mobile networks, as the optimization achieved using the MRPs works well in this context. The larger and more dense the network, the more optimization can be achieved. OLSR is well suited for networks, where traffic is random and sporadic between several nodes rather than being almost exclusively between a small specified set of nodes.

2.2.2 GRP (Gathering-based Routing Protocol)

Gathering-based Routing Protocol combines the advantages of Proactive Routing Protocol (PRP) and of Reactive Routing protocol(RRP). PRP are suitable for supporting the delay sensitive data such as voice and video but it consumes a great portion of the network capacity. While RRP is not suitable for real-time communication, the advantage of this approach is it can dramatically reduce routing overhead when a network is relatively static and the active traffic is light. However, the source node has to wait until a route to the destination can be discovered, increasing the response time. The function of Gathering-based Routing Protocol (GRP) for mobile ad hoc network is to gather network information rapidly at a source node without spending a large amount of overheads. It offers an efficient framework that can simultaneously draw on the strengths of Proactive routing protocol (PRP) and reactive routing protocol (RRP) collects network information at a source node at an expense of a small amount of control overheads. The source node can equip promising routes on the basis of the collected information, thereby continuously transmitting data packets even if the current route is disconnected, its results in achieving fast (packet) transfer delay without unduly compromising on (control) overhead performance.

3. Experimental set up

The main interest is to analyse and compare the performance of routing protocol between dcf and edcf routing protocol.Here we are observing performance of routing protocol on the basis of following parameters:-delay,throughput,traffic sent and traffic received . The

simulations were performed with 20and60 numbers of nodes, .Network simulation tool used in simulation is OPNET modeler(ver.14). In this comparison we are using triangular mobility model.

4. Performance Metrics

The following four metrics have been chosen to compare the protocols:

Traffic Sent :data packet sent to receiver

Traffic Received:data pacekt received from the source.

Delay: The delay is the time taken by a packet from the movement it is transmitted on the network by the source node to reach the destination node.

Throughput: The average network throughput is simply the number of data packet received by all destinations over the duration of the simulation

5. Performance Analysis

The simulation is performed for 20 nodes and 60 nodes using triangular mobility.The proposed model is evaluated for its efficiency considering comparative analysis with the prior research work conducted in comparison of routing protocols in mobile adhoc network.

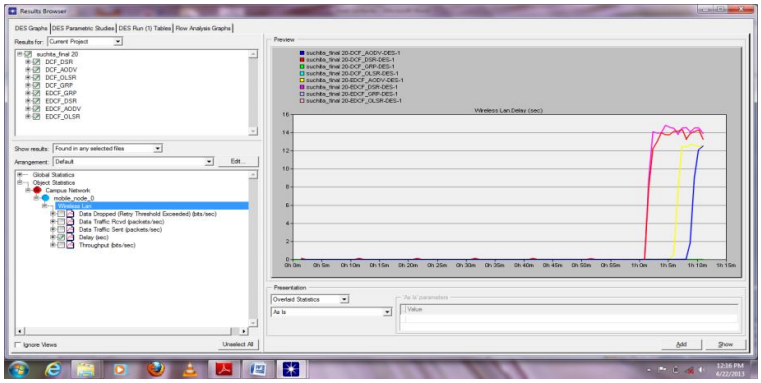

Figure 2: Delay For 20 Nodes

The fig.2 shows the performance ananlysis when conducted for delay by using 20 nodes.The proposed system shows that edcf routing protocol performs better than dcf routing protocol.

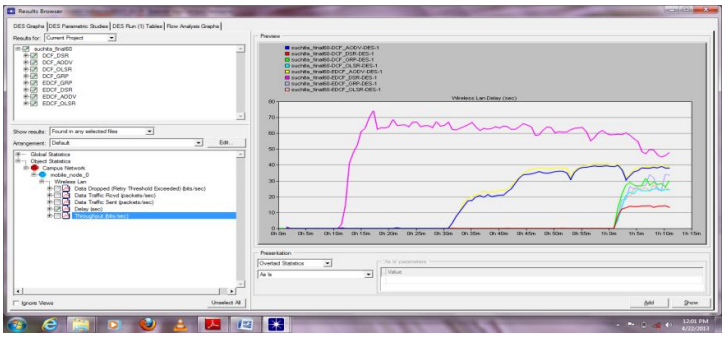

Figure 3: Delay For 60 Nodes

Fig.3 shows the performance of 60 nodes for delay and it also shows that edcf performance well with respect to dcf

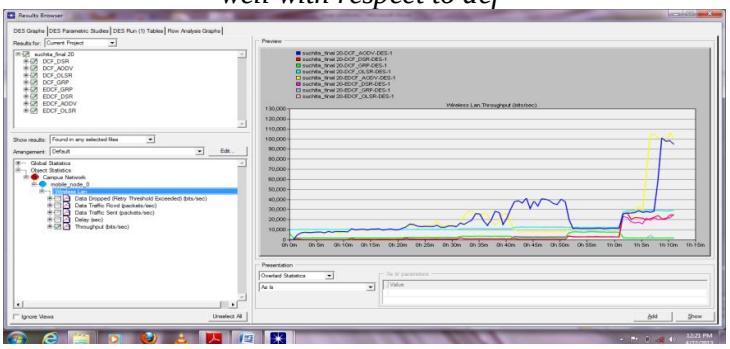

Figure 4: Throughput For 20 Nodes

Fig.4 shows the throughput for 20 nodes,here edcf has performed better than dcf

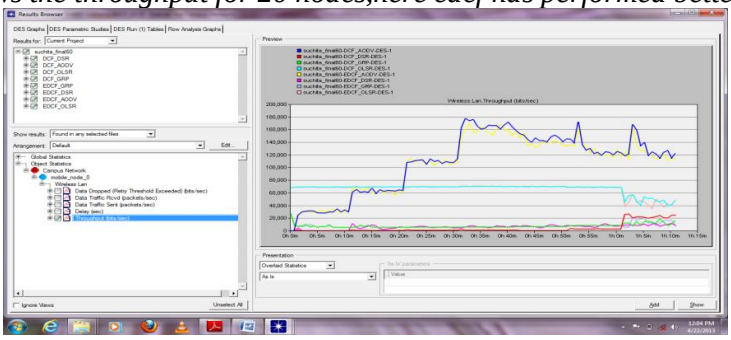

Figure 5: Throughput For 60 Nodes

Fig.5 shows the performance analysis for throughput by taking 60 nodes resulting in dcf superior than edcf.

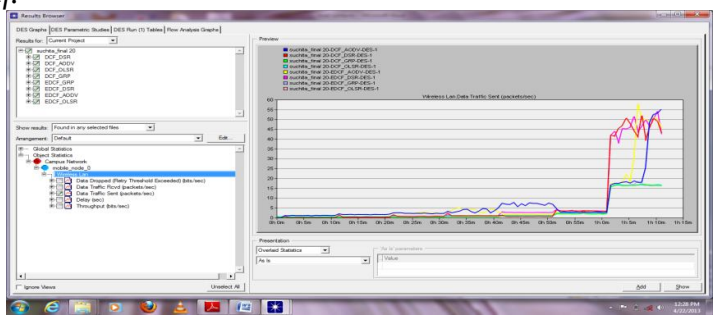

Figure 6: Traffic Sent For 20 Nodes

Fig.6 present the performance for traffic sent by using 20 nodes and it shows that edcf performs better than dcf

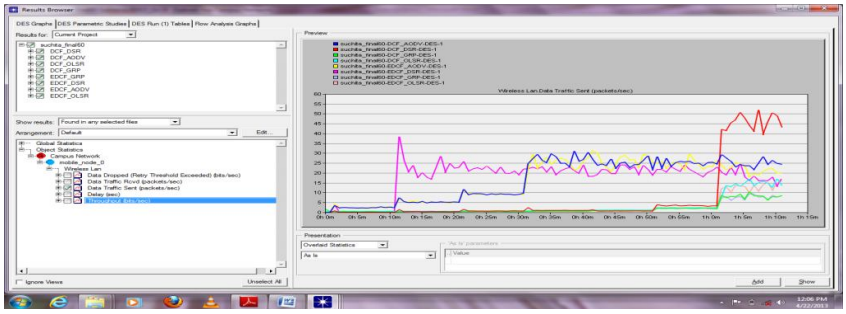

Figure 7: Traffic Sent For 60 Nodes

Fig.7 gives the result that when nodes are increased dcf performs better than edcf

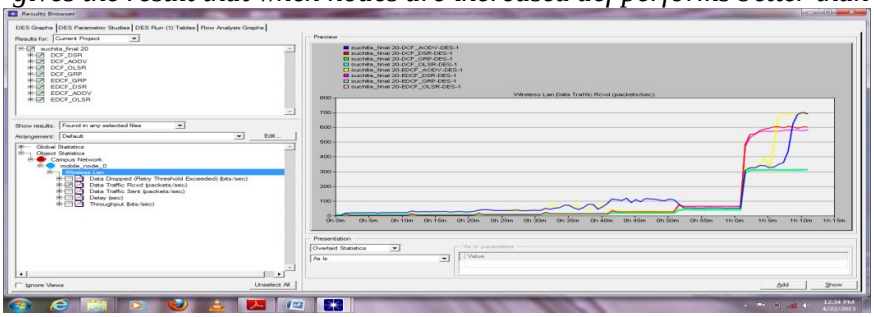

Figure8: Traffic Received For 20 Nodes

Fig.8 shows the performance analysis of traffic received for 20 nodes which shows that dcf is slightly superior than edcf.

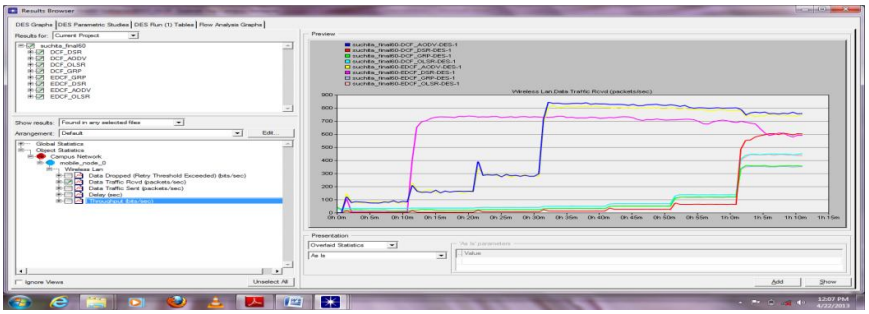

Figure 9: Traffic Received For 60 Nodes

Fig.9 illustrates that traffic received for 60 nodes in which the performance of dcf is greater than edcf.

6. Conclusion

In this work ,performance evaluation of triangular mobility models on four routing protocols olsr ,grp,aodv and dsr is done on the basis of four different performance metrics that is throughput,delay,traffic sent,traffic received.The simulation results shows that throughput of edcf in case of 20 nodes is better than dcf,while there is reverse case in terms of 60

nodes.Delay of edcf is better than dcf in both the cases that is 20 nodes and 60 nodes.The performance of edcf is greater than dcf in case of 20 nodes where as dcf perfoms better in case of 60 ndes for traffic sent.Traffic received of dcf perfoms better than edcf in both the cases that is 20 and 60 nodes.

7. Reference

1. Anil g.n ,dr. a venugopal reddy ,semantic probabilistic modeling of novel routing protocol with implication of cumulative routing attack in mobile adhoc network, International Journal of Computer Applications Volume 9– No.1 january 2012.
2. Sherif m.badr , a framework for integrated routing protocols for mobile ad hoc network, International Journal of Computer Applications (0975 – 8887) Volume 60– No.9, December 2012.
3. Rashmi rohankar ,rinkoo Bhatia,vi neet shrivastava,Deepak kumar Sharma,performance analysis of various routing protocols(proactive and reactive) for random mobility models of adhoc networks.cof. on recent advances in information technology rait-2012.
4. Avnikhatkar,yudhvir singh,performance evaluation of hybrid routing protocols in mobile adhoc networks, 2012 second international conference on advanced computing & communication technologies.
5. Ashish bagwari, raman jee,pankaj joshi sourabh bisht,performance of aodv routing protocol with increasing the manet nodes and it`s effects on qos of mobile ad hoc networks, 2012 international conference on communication system and network technologies.
6. Ramandeep kaur nagra ,jasmeet singh gurm, gurpreet singh grewal,simulation based analysis of aodv,babel and puma protocols for adhoc network.
   International conference on recent advances and future trends in information technology.(irafit2012)
7. D.Suresh kumar, K.Manikandan, M.A.Saleem Durai, Secure On-Demand Routing Protocol for MANET using Genetic Algorithm, International Journal of Computer Applications (0975 – 8887) Volume 19– No.8, April 2011
8. Zahra Moradi, Mohammad Teshnehlab, Intrusion
   Detection Model in MANETs using ANNs and ANFIS, 2011 International Conference on Telecommunication Technology and Applications Proc .of CSIT vol.5 (2011)