An Empirical Performance Evaluation of AODV and DSR using ALERT Protocol in MANET

Saloni Vashisht
Student
M.Tech, CSE
Lovely Professional University

Ankit Vashisht
Student
M.S, Telecom &Software Engg
Birla Institute of Tech & science

Sheveta
Assistant Professor
M.Tech, CSE
Lovely Professional University

ABSTRACT
Recent advances in portable computing and wireless technologies are opening up exciting possibilities for the future of wireless mobile networking. [1]A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links to exchange necessary information. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure and are a new wireless networking paradigm for mobile hosts. Analyzing and comparing the performance of routing protocol and doing some efforts for making these protocol performs much better is a wide area of research now a days. In this research work we implemented ALERT in AODV and DSR to provide the anonymity to the source, destination and routes in the network for the secure transmission by hiding node identities and routes from outside observers and compares the performance of those based on parameters such as throughput, packet delivery ratio, and packet delay This research achieves anonymity in AODV and DSR by using ALERT protocol without losing performance of AODV and DSR protocol in MANET. We are also Monitoring Loss at destination node using different traffic generator UDP/CBR in ALERT-AODV and ALERT-DSR for proposed work and TCP/FTP in normal AODV and DSR..

General Terms
MANET, routing, AODV, GPSR, ALERT, DSR, proto-cols, ns2, gnu plot

Keywords
Comparison, Performance

1. INTRODUCTION
A mobile ad hoc network is a collection of wireless mobile nodes [1] which dynamically forming a temporary mobile nodes without the aid of any established infrastructure or centralized administration. There are, furthermore, situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. It works in the absence of fixed infrastructure.[2] They provide fast and easy network deployment in circumstances where it is not possible otherwise. Mobile ad-hoc network is an autonomous system of mobile nodes which are connected by wireless links. In which every node operates as an end system and a router for all other nodes in the network. In present MANET is the most important research area for researchers for establishing the efficient ad-hoc network using available different routing schemes and analyzes this network with the help of different network simulation tools such as ns2.

In this paper we consider the most important routing scheme of the MANET named AODV (Ad-hoc On-demand Distance Vector) and DSR (Dynamic Source Routing) for our research. These two routing schemes are [6] Most important because they are capable of both unicast and multicast moreover they are on demand routing protocol. In our proposed work .we implemented ALERT in AODV and DSR to provide the anonymity to the source, destination and routes in the network for the secure transmission by hiding node identities and routes from outside observers and then analyzed the performance of ALERT-AODV and ALERT-DSR using the simulation tool ns2. Main aim of DSR scheme is to reduce the number of broadcasting packets by discovering the routes on demand maintains the route caches and route caching can further reduce route discovery overhead. AODV (Ad-hoc On-demand Distance Vector AODV discovers routes as and when Necessary and does not maintain routes from every node to every other GPSR Greedy Perimeter Stateless Routing is a responsive and efficient routing protocol for mobile wireless networks which uses greedy forwarding technique to forward packets to nodes. ALERT Anonymous Location-Based Efficient Routing Protocol dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route.

In particular, the section 2 describes the four protocols AODV, DSR, GPSR and ALERT in detail. section 3 describes our proposed work in which we implement the technique of ALERT in AODV and ALERT in DSR the section 4 shows the simulation results and performance analysis of ALERT-AODV ALERT-DSR and normal AODV and DSR to prove that the performance of normal AODV and DSR does not affect the performance when ALERT technique is applied on AODV and DSR all the simulation are based on network simulator ns2 and gun plot is used to draw the comparison graph and finally section 5 describes the conclusion of the work.

2. OVERVIEW OF PROTOCOLS USED IN RESEARCH: AODV, DSR, ALERT, GPRS
In this section we explained important details of protocols that will help in understanding the ides of this research.

2.1 AODV (Ad-hoc On-demand Distance Vector Routing)
AODV is a reactive protocol, in which routes are not predefined, and routes are created on demand of the source node. AODV mainly operates by two important functions, first is route discovery shown in the and second is route maintenance.[7]When source needs to send packet to

destination then protocols starts route discovery phase. After that source sends route request message to its neighbors then they broadcast the message to all their neighbors. Broadcasting is done via Flooding.[7]After this if any neighbor node has the information about the destination node, that node sends route reply message to the node from which it receives the route request message. This neighbor follows the same process. On the basis of this process a path is recorded in the intermediate nodes. As every node forwards route request message to all of its neighbors, more than one copy of the original route request message can arrive at a node. Due to this reason, a unique id is assigned with each message, when a route request message is created. When a node receives the message, it will check this unique id and the address of the initiator and it discarded the message if it had already processed that request.[7]When a route reply message reaches the initiator the route is ready and the initiator can start sending data packets. It Minimizes number of active routes between an active source and destination Packet in this process contains broadcast ID number and it gets incremented each time a source node uses route request.[3]AODV maintains the route information by creating a routing table at each node. In these tables it stores routing information as destination and next hop addresses as well as the sequence number of a destination. To prevent storing information and maintenance of routes that are not used anymore each route table entry has a lifetime. If during this time the route has not been used, the entry is discarded.

2.2 DSR (Dynamic Source Routing)

DSR is also referred to as on demand protocol. A node maintains initiates the route discovery process by sending a special route request packet to all neighboring nodes.[7]The route cache containing the routes it knows it includes route discovery on request and route maintenance when needed .DSR is quite simple algorithm in which a sending node must provide the sequence of all nodes through which a packet will travel. Each node maintains its own route cache, essentially a routing table, of these addresses. Source nodes determine routes dynamically only when needed there are no periodic broadcasts from routers.[10] A source node that wants to send a packet it first checks its route cache. If there is a valid entry for the destination, the node sends the packet using that route if no valid route is available in the route cache the source node request travels through the network, collecting the addresses of all nodes visited, until it reaches the destination node. This node in turn initiates the route reply process by sending a Special route reply packet to the originating node i.e. sender announcing the newly discovered route. The destination node can accomplish this using inverse routing or by initiating the route discovery process backwards.[4] The DSR algorithm also includes a route maintenance feature as AODV it is implemented via a hop-to-hop or end-to-end acknowledgment process the former includes error checking at each hop, while the latter checks for errors only on the sending and receiving sides. When the host encounters a broken link, it sends a route error (RERR) packet. Dynamic source routing is easy to implement, can work with asymmetric links, and involves no overhead when there are no changes in the network. DSR performs well because Route caching can further reduce route discovery overhead A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches and DSR has access to significantly greater amount of routing information.

2.3 GPSR (Greedy Perimeter Stateless Routing)

Greedy Perimeter Stateless Routing, GPSR, is a responsive and efficient routing Protocol for mobile, wireless networks. [5] GPSR exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. In regions of the network where such a greedy path does not exist *i.e.,* the only path requires that one move temporarily away from the destination GPSR recovers by forwarding in perimeter mode in which a packet traverses successively closer faces of a planar sub graph of full radio network Connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes.

2.4 Anonymous Location-based Efficient Routing Protocol

Mobile Ad Hoc Networks use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection. Anonymous communication protocol can provide untraceability to ensure the anonymity of the sender when the sender communicates with the receiver.

Routing Process of ALERT

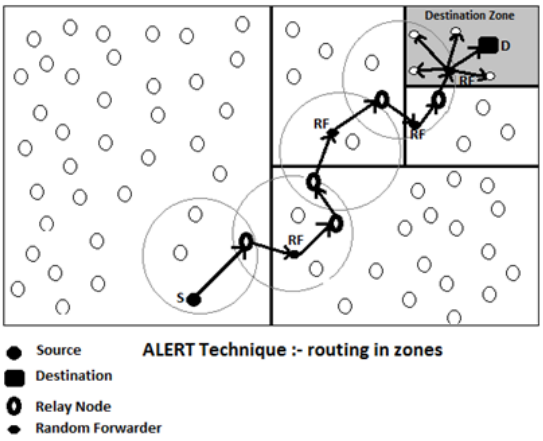
ALERT provides dynamic routing path, having no. of dynamically selected intermediate nodes.

1. Firstly it partitions given network area into two zones as horizontally or vertically.
2. Now, again split every partition into two zones as vertically or horizontally called as hierarchical zone partition.
3. After partitioning it randomly select a node in each zone at each step as an intermediate relay node, in this way ALERT provide dynamically creating an unpredictable routing path.

[9]When source wants to send the packet to the destination then source finds the destination is in the same zone then vertical partitioning will be done to differentiate from the destination. Then source randomly choose the node which is nearest to it in the other zone as a temporary destination called as random forwarder RF.After that source uses GPRS protocol to send the packet to the RF by using some relay nodes. These node can be selected randomly in every zone used for dynamically generating an unpredictable path for packet.RF then check if destination and itself are in same zone then it performs hierarchical partitioning to separate form destination and performs the same process as performed in first zone by go on till it reaches to the destination zone. The shaded part in the [9] figure 2.1 shows the destination zone, ZD. The zone in which the real destination is located with some nodes is called the destination zone, ZD, because to provide anonymity those nodes are chosen who have short distance to create a path from source to destination using formula given by:

$$Distance = \sqrt{((x_i - x_j)^2 + (y_i - y_j)^2)}$$

Partitioning is done first then to set up the path it takes the help of relay node and Random forward in the network to reach to the destination.



[9] Figure 2.1 Alert Techniques

Now, the next thing is how a node get to know that it is in the same zone as the destination. For that ALERT provides a formula i.e.,

$$H = log_2\left(\frac{\rho \cdot G}{k}\right),$$

Here H denotes the total number of partitions in order to produce destination zone. G is the size of the entire area of the network. ρ is the node density and k is the number of nodes in the destination zone.

3. PROPOSED WORK

In the proposed work we have implemented ALERT on AODV and ALERT on DSR.First, provide the anonymity protection to source, destination and route. Second to achieve anonymity in AODV and DSR by using ALERT protocol without losing performance of normal AODV and DSR protocol in MANET. Third to monitor the loss at destination using different traffic generator UDP/CBR in ALERT-AODV and ALERT-DSR for proposed work and TCP/FTP in normal AODV and DSR.

As we implemented ALERT on AODV and ALERT on DSR protocol the process is same when the connection is required it broadcasts a request for connection to the other nodes present in the network but the difference is in the path made between source and destination. The strategy is based on the ALERT protocol in which the links are created on the basis of their location in the region defined as well as the distance so that no one cannot find the location of destination ALERT broadcast the packet to all nodes in the network.

PROPOSED SYSTEM ARCHITECTURE

1. First distance is calculated between each and every node.
2. After that we set a variable named dismat and set it to 1 if distance is less than range set. This is the approach of GPSR.
3. After that we are defining the regions manually.
4. Now calculate the position of destination(x,y) and find it's region in which it is lying.
5. Now we are calculating the neighbor node position(x,y) and also find it's region in which it is lying.
6. After that all neighbors or nodes are compared against the dismat function where distance is less than the set range.
7. Now visit all the nodes where dismat is less than set range.
8. Now find that the node is in some region or not.
9. If in the region and dismat is less than set range than link is created by multicasting between these nodes.
10. This process is repeated until get a path from source to destination.

This proposed process is same for AODV and DSR Routing protocol which uses their own concepts to route a packet from source to destination. In this research comparison and analysis is done by implementing ALERT in AODV and ALERT in DSR without losing performance of normal AODV and DSR protocol in MANET. Minimum distance value creates the final path form source to destination. Because of multicasting and nodes being in different zones the actual location of destination cannot be determined by the attacker. Thus AODV and DSR can provide anonymity with the use of ALERT technique.

4. PERFORMANCE ANALYSIS BASED ON SIMULATION RESULTS

This section explains the simulation results of ALERT-AODV and ALERT-DSR and analyzes its performance with the performance of normal AODV and DSR protocol by simulating in NS2.

So, this part of the simulation proves that by implementing ALERT technique to provide the anonymity does not affect the normal performance of AODV and DSR.Different parameters such as throughput, packet delivery ratio, and packet delay are Performances are compared by using gnu plot AODV with the technique of ALERT and DSR with the technique of ALERT for different number of nodes. We compare both techniques on the basis of the results of their throughput, packet delivery ratio and packet delay. Simulation parameters are given below:

Table 4.1 Simulation Parameters

Parameter	Value
Protocols	AODV,DSR
No. of Nodes	50,60,70
Area Size	900*900
Traffic Type	UDP/CBR
Interface Queue Type	Drop Tail/PriQueue
Queue Length	50
Antenna Type	Omni Antenna
Simulation Time	10
MAC Layer Protocol	802.11

4.1 Performance Analysis of ALERT-AODV and ALERT-DSR

After doing the simulation graph has been plotted to show the performance of our proposed work i.e., implementation of AODV and DSR by using ALERT technique to provide anonymity protection and also analyzed how this system works when the no of nodes changes in the scenario.

The figure 4.1 shows that end to end delay between ALERT-AODV and ALERT-DSR. As the simulation results of end to end delay of normal AODV and DSR shown in the figure 4.4 proves that DSR has higher values as compares to the AODV which results into the better performance of AODV because it takes less time a packet to travel from source to destination node as comparative to DSR.So, this part of the simulation proves that by implementing ALERT technique to provide the anonymity it does not affect the normal performance of AODV and DSR.

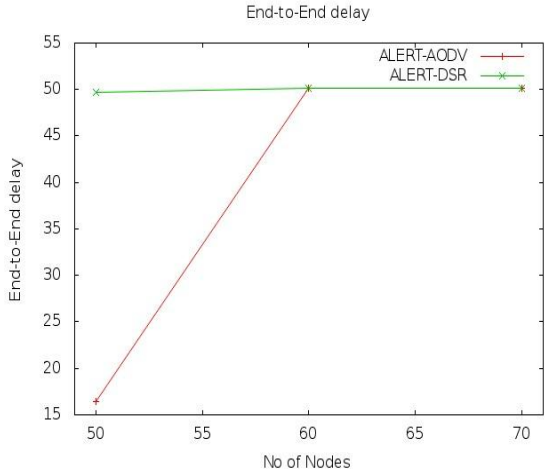


Figure 4.1 End to End Delay Vs No. Of nodes in ALERT-AODV-DSR

Similarly packet Delivery Ratio of ALERT-AODV is better than ALERT-DSR as the no of nodes increases in the scenario. Figure 4.2 shows the simulation results in the form of graphs. As discussed in the figure 4.5 i,e PDR(Packet Delivery Ratio) of normal AODV is better than DSR at maximum no of nodes taken into the taken into consideration. NS2 provides substantial support for simulation of TCP/UDP, routing, and multicast protocols. By implementing ALERT technique on AODV and DSR to provide the anonymity it does not affect the normal performance of AODV and DSR.

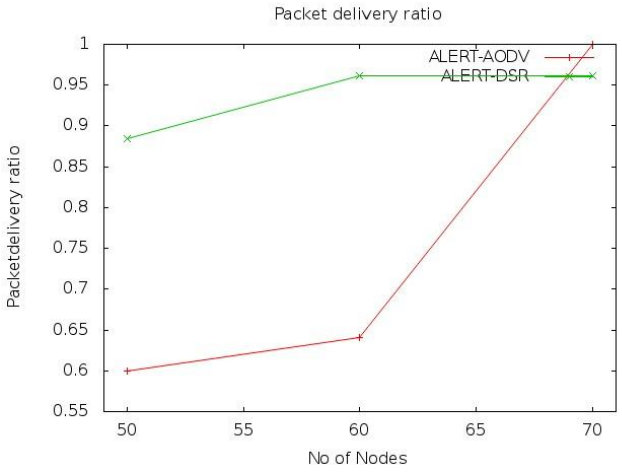


Figure 4.2 Packet Delivery Ratio Vs No of nodes in ALERT-AODV-DSR

Third parameter taken into consideration is throughput i,e average rate of successful message delivery over a communication channel. ALERT-AODV is better than ALERT-DSR as the no of nodes increases in the scenario.

Figure 4.3 shows the simulation results in the form of graphs. As discussed in the figure 4.6 i,e throughput of normal AODV is better than the DSR at maximum no of nodes taken into the scenario i,e 70. So, this parameter also proves that by implementing ALERT technique on AODV and DSR to provide the anonymity does not affect the normal performance of AODV and DSR

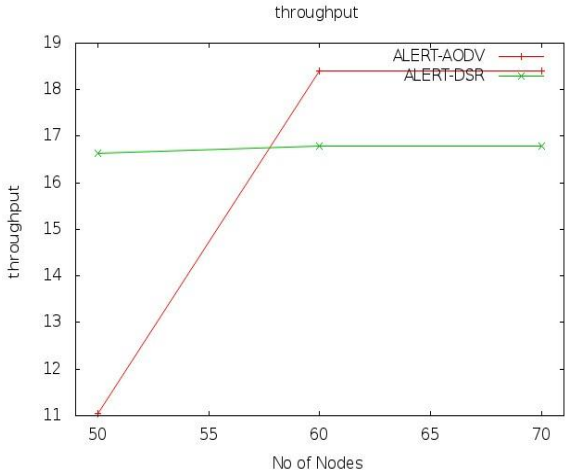


Figure 4.3 Throughput Vs no of nodes in ALERT-AODV-DSR

As Simulation results in the form of table is given in the table 4.2 and 4.3

Table 4.2 Performance Measurements of ALERT-AODV

Parameters	**For 50 nodes**	**For 60 nodes**	**For 70 nodes**
End to End Delay	16.469818779	50.1644914649	50.168544284
Packet Delivery Ratio	0.599999999	0.64102564	1.0
Throughput	11.0399999	18.39999999	18.399999999

End to end delay at node 50 in case of when ALERT technique is applied on AODV is 16.46 which is the minimum value and in case of when ALERT is applied on DSR value is 49.66 that shows that packets takes more time to deliver in ALERT-DSR

Packet Delivery Ratio of in case ALERT-AODV is at node 70 is 1.0 and .96 in case of ALERT-DSR that proves AODV is better than DSR after applying ALERT technique as well.

Table 4.3 Performance Measurements of ALERT-DSR

Parameters	**For 50 nodes**	**For 60 nodes**	**For 70 nodes**
End to End Delay	49.669836861	50.15996044	50.16502928
Packet Delivery Ratio	0.883928571	0.9615384615	0.9615384615
Throughput	16.63200	16.80001	16.80001

The Value of Throughput at node 70 is 18.39 in case of ALERT-AODV and 16.8 in ALERT-DSR that proves AODV is better than DSR when we apply ALERT technique on it which also does not effect on normal performance of AODV and DSR.

4.2 Performance Analysis of AODV and DSR

The simulation parameters considered in simulating the effect of varying the node density are shown in the table A flat area of 500*400 is chosen with Two Ray Ground as a propagation model by taking into consideration both direct and indirect paths between the communicating nodes. The analysis is based on varying the number of nodes from 50 to 70.

Table 4.4 Simulation Parameters

Parameter	Value
Protocols	AODV,DSR
No. of Nodes	50,60,70
Area Size	500*400
Traffic Type	TCP/FTP
Interface Queue Type	Drop Tail/Pri Queue
Queue Length	50
Radio Propagation Model	TwoRayGround
Antenna Type	Omni Antenna
Simulation Time	150sec

As shown in the figure 4.5 Packet delivery ratio of AODV is higher than DSR as the no of nodes increases. At node 70 value of AODV is higher than the value of DSR So, AODV

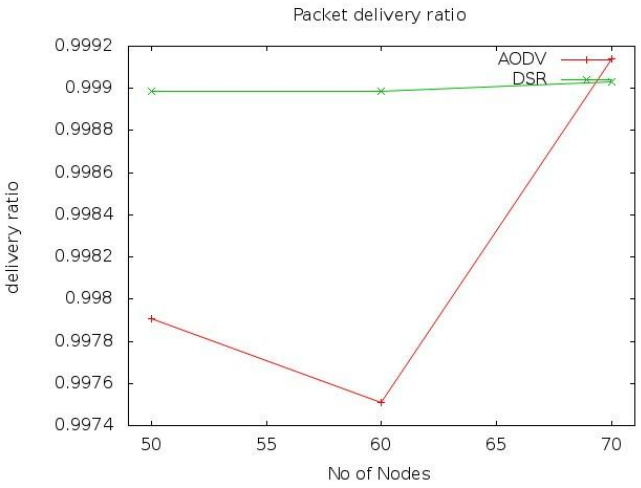


Figure 4.5 Packet Delivery Ratio Vs No. of nodes in AODV and DSR

performs well as compares to the DSR as he number of packets actually delivered to the destination to the number of data packets supposed to be received the better the packet delivery ratio, the more complete and correct is the routing protocol.

Average end to end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time this metric is useful in understanding the delay caused while discovering path from source to destination. As the graph shown in the figure 4.4 shows as the node density increases means at node 70 delay is higher in DSR as compared to the AODV which reveals the better performance of AODV as comparison to the DSR.

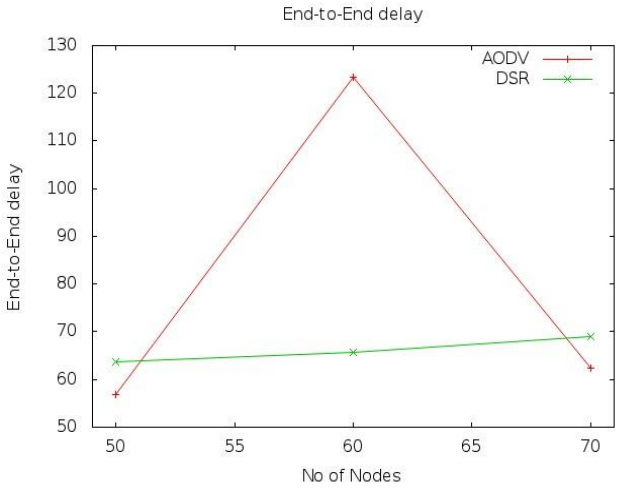


Figure 4.4 End to End Delay Vs no. of nodes in AODV-DSR

As we know throughput is the ratio of number of packets sent and total number of packet received which describes the average rate of successful message delivery over a communication channel. Graph shown in the Figure 4.6 shows that throughput in case of AODV is higher than DSR as the node density increases.So; AODV proves the efficient routing over the network.

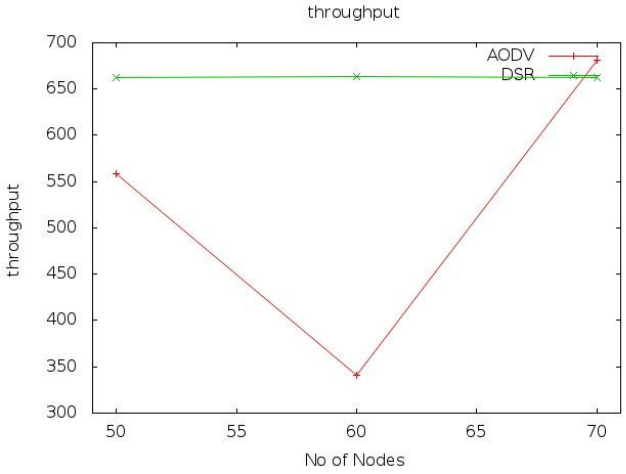


Figure 4.6 Throughput Vs No. of nodes in AODV-DSR

5. ACKNOWLEDGMENTS

A number of people have made this paper possible. In particular I wish to thank my husband Mr. Ankit Vashisht for providing much needed help and support, my Research guide Ms.Sheveta for their guidance. She gave me an opportunity to learn and conduct research. Her guidance helped me in all the time of research writing. I wish to thank my parents for teaching me never to give up on any endeavor.

6. CONCLUSION OF THE WORK

On combining the ALERT techniques with AODV and DSR protocol results efficient routing by providing anonymity protection to the source, destination node and route followed which helps in secure transmission of packets over the network and prevents the attack from outside observer. This research achieves anonymity in AODV and DSR by using ALERT protocol without losing performance of normal AODV and DSR protocol in MANET. The combination of

facts such as the extensive growth of network, So ALERT techniques is used for secret communication plays a important role. This paper provides an overview of the AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), ALERT (An Anonymous Location-Based Efficient Routing Protocol) and GPRS (Greedy Perimeter Stateless Routing) protocol which provides the efficient routing in the Ad hoc networks and also provides the comparison of normal AODV and DSR approach.

In future work one can analyze these techniques for a wide network by increasing the number of nodes greater than 200 or more and also for varying pause time.

7. REFERENCES

[1] Pravin Ghosekar, Girish Katkar and Dr.Pradip Ghorpade (2010), **"**Mobile Ad Hoc Networking: Imperatives and Challenges"IJCA Special issue on Mobile Ad Hoc Networks

[2] Imrich Chlamtac,Marco Conti and Jennifer J-N.Liu (2003) "Ad Hoc Network" 13-64

[3] Tuteja,A (2010)" Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2" Advances in Computer Engineering (ACE) IEEE

[4] Amandeep, Gurmeet kaur (2012) "Performance Analysis of AODV Routing Protocol in MANET" (IJEST) ISSN: 0975- 5462 Vol. 4

[5] Brad Karp and H.T Kung "Greedy Perimeter Stateless Routing for Wireless Networks"

[6] Carlos de Morais Cordeiro and Dharma P.Agrawal "Mobile Ad Hoc Networking"

[7] Shahjahan Ali and Abdul Wahid "Performance Evaluation of Routing Protocols under Wormhole Attack in Mobile Ad-Hoc Network"

[8] A.Rajeshkumar, J.Rajesh Kumar "Randomized Routing Protocols in Mobile Ad- Hoc Networks Using Alert"

[9] D.Pavun Kumar, Mr S.Sundar Raj "An Anonymous Authentication and Secure Communication Protocol in Ad-hoc Networks"

[10] Tanu Preet Singh, Neha, Vikrant Das "Multicast Routing Protocols in MANET"