ISSN:0975-9646

K S R Murthy et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3210-3218

Based on Packet Delivery Performance Review for Route Discovery in Reactive Routing Protocols (AODV, AOMDV, DSDV)

K S R Murthy [#1], **Dr Samuel VaraPrasad Raju** [*2],

[#] *Research scholar,CSSE ,Andhra University College of Engineering, AP,india*
[*] *Professor, Andhra University, AP.*

Abstract:The objective of this research paper is to find a multifold security solution by developing a new on-demand stable and secure routing protocol, using five performance metrics for packet delivery fraction, average end to end delay, network throughput, and normalized routing load and packet loss. According to this we know the various kinds of attacks as it based on the assumption that all nodes must cooperate and without their cooperation no route can be established. In addition, when the malicious nodes enter into the network, various performance metrics begin the efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc. the ultimate goal for ad-hoc network security is to develop a multifold security solution that results in in-depth protection that offers multiple lines of defense against both known and unknown security threats.

Keywords: Wireless Sensor networks, Design issues, Routing protocols, Applications

INTRODUCTION

Mobile Ad-hoc network (MANET) is a collection of mobile nodes by wireless links forming a dynamic topology without any network infrastructure such as routers, servers, access points/cables or centralized administration. Each mobile node functions as router as well as node. The most important characteristics of MANET are;

i) Dynamic topologies
ii) Bandwidth constrained links
iii) Energy constrained operation and
iv) limited physical security

Routing protocols play a vital role in MANET to find routes for packet delivery and make sure that the packets are delivered to the correct destinations. These protocols are classified as:

(i) Pro-active,
(ii) Re-active, and
(iii) Hybrid.

Proactive Routing Protocols

Routes to all destinations are maintained by sending periodical control messages. There is unnecessary bandwidth wastage for sending control packets. Proactive routing protocols are not suitable for larger networks, as it needs to maintain route information every node's routing table. This causes more overhead leads to consumption of more bandwidth. Ex: OLSR, DSDV [10, 11].

Reactive Routing Protocols

Routes are found when there is a need (on demand). Hence, it reduces the routing overhead. It does not need to search for and maintain the routes on which there is no route request. Reactive routing protocols are very pleasing in the resource-limited environment. However the source node should wait until a route to the destination is discovered. This approach is best suitable when the network is static and traffic is very light. Ex: DSR, AODV. [15, 16].

Hybrid Routing

The Ad Hoc network can use the hybrid routing protocols that have the advantage of both proactive and reactive routing protocols to balance the delay and control overhead (in terms of control packages). The difficulty of all hybrid routing protocols is the complexity of organizing the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption.

AODV PROTOCOL

AODV protocol allows mobile nodes to quickly obtain routes for new destinations, and it does not require nodes to maintain routes to destinations that are not in active communication. Also, AODV routing permits mobile nodes to respond link breakages and changes in network topology in a timely manner. The main objectives of the protocol is quickly and dynamically adapt to changes of conditions on the network links, for example, due to mobility of nodes the AODV protocol works as a pure on-demand route acquisition system. Control messages [8, 9] used in AODV is:

• Route Request Message (RREQ)

Among these protocols, the reactive category is widely used because they find routes whenever needed (i.e., on-demand). We present a simulation-based performance study of the two types of widely used reactive protocols such as AODV, AOMDV, DSR, OLSR . Moreover, the performance comparison of both AODV and AOMDV is carried out with varying network load and pause time.

• Route Reply Message (RREP)
• Route Error Message (RERR)
• Route Reply Acknowledgment (RREP-ACK) Message
• HELLO Messages

Algorithm 1: Implemented in Intermediate Node
If (Node listen a RREQ**)**
{
If (same as forwarded in near past)
{
Discard**;**
}
Else //This is a new RREQ
{
Calculate RSSI
If (RSSI < RSSI_Thr1) then
Drop packet P
Return
End If
Else
Entry for Reverse Route // (Route from node to originator of this RREQ message)
{ // update the sequence no. ,
// Set the valid flag for route,
// Change the life time for route to originator.
//Update the routing table entries for
//originator IP address;

Increase the hop count by one in RREQ packet; **}**
IF (TTL > 1)
{
Decrease the TTL field by one;
If [(Node is Destination for this RREQ**) OR (**Node has route to destination**)]**
{
Send RREP;
Discard RREQ**;**
}
Else
{
Broadcast RREQ**;**
}
}
}
}

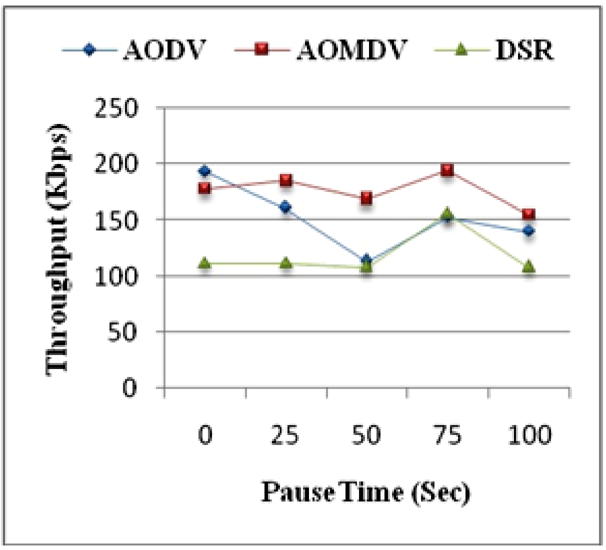
Route discovery:
When a source node desires to send a message to some destination node, and doesn't have a valid route to the destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) control packet to its neighbours, which then forward the request to their neighbours, and so on, either the destination or an intermediate node with a new route to the destination is located. The AODV protocol utilizes destination sequence numbers to ensure that all routes contain the most recent route information. Each node maintains its own sequence number. During the forwarding process the RREQ intermediate nodes record the address of the neighbour from which the first copy of the broadcast packet is received in their route tables, thereby establishing a reverse path. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or the intermediate node responds by unicasting a route reply (RREP) control packet back to the neighbour from which first received the RREQ [6,7].

B) Route Maintenance
A route discovered between a source node and destination node is maintained as long as needed by the source node. 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 predecessor nodes. This process continues until the source node is reached. When RERR is received by the source node, it can either stop sending the data or reinitiate the route discovery mechanism by sending a new RREQ message if the route is still required[9,10].

Network Scenarios:
In the ad hoc network, we have simulated the following 3 different scenarios:
(a) Pause Time
(b) Offered Load (number of source destination pairs)
(c) Node Speed

In each of the scenario, unless otherwise specified, simulation settings are same

(a) Pause Time
Pause time refers to the rest time of the node. The RWMM includes pause times between changes in direction and/or speed. A node begins by staying in one location for a certain period of time (i.e. a pause time). Once this time expires, the node chooses a random destination in the simulation area and a speed that is uniformly distributed between [MIN SPEED, MAX SPEED]. The node then travels towards the newly chosen destination at the selected speed. Upon arrival the node pauses for a specified time period before starting the process again. In our simulation, we considered 10 m/s as an average node speed, 10 SDPs as offered load, random waypoint as mobility model and 0,500,1000,1500,1800 seconds as pause time. Where, 0s pause time represent the continuous node mobility and 1800s pause time represents static network environment.



(b) Offered Load (Number of SDPs)

Offered load refers to the number of source destination pairs engaged in data transfer. For example, with 10 SDPs amongst 50 nodes, 10 source nodes and 10 destination nodes (i.e. 20 nodes in total) will be engaged in data transfer. However, during this data transfer process, all of the 50 nodes (including the above 20 nodes) will operate in the background for providing necessary support (i.e. routing/forwarding) to the ongoing communication process in the network. In our simulation we considered 10 m/s as an average speed and 0s pause time with offered load (i.e. number of SDPs) varied as 10,20,30,40 pairs.

(c) Node Speed

Node speed refers to the average speed with which nodes move in the simulation area. We have used random waypoint mobility model (RWMM), as it is widely used in MANET simulations [23]. In RWMM, nodes move at a speed uniformly distributed in [MIN SPEED, MAX SPEED]. In our simulation, we have considered 10 SDPs for data transfer and average node speeds considered are 5, 10, 15, 20, 25 m/s. Each node begins the simulation by moving towards a randomly chosen destination. Whenever a node chooses a destination, it rests for a pause time. It then chooses a new destination and moves towards the same. This process is repeated until the end of the simulation time. In this scenario, however, pause time is set at 0s (i.e. nodes move continuously throughout the simulation period). This is done to study the impact of continuous node mobility (i.e. worst case scenario) on the network performance.

In this section, we present the results obtained via simulations followed by analysis. Packet delivery ratio, average end-to-end delay, throughput, routing message overhead are the metrics used to evaluate and analyze the performance of reactive (AODV,DSR) and proactive (WRP) routing protocols under different types of traffic like CBR, FTP, TELNET.

MANET ROUTING PROTOCOL (10)

Here we are described three Manet routing protocol these are (DSR) reactive, (ZRP) hybrid and (STAR) Proactive protocols in brief.

A. Reactive (on demand) Routing Protocols

In this routing information is acquired on-demand. Reactive routing protocols use two different operations to Route discovery and Route maintenance operation. Route maintenance is the process of responding to change in topology that happen after a route has initially been created, Route Maintenance is used to handle route breaks [6]. Examples: ANODR, AODV, DSR, DYMO, LAR1 etc.

1) Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing (DSR) [10] is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender unambiguously lists this route in the packet.s header,identifying each forwarding ¡°hop¡± by the address of the next node to which to transmit the packet on its way to the destination host. It also computes the routes when necessary and then maintains them. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use.

1.1) Route Discovery

Route Discovery [6] is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it already contains a route to the destination. If the source finds a valid route to the destination, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message. The route request message contains the address of the source and the destination, and a unique identification number. An intermediate node that receives a route request message searches its route cache for a route to the destination. If no route is found, it appends its address to the route record of the message and forwards the message to its neighbors. The message propagates through the network until it reaches either the destination or an intermediate node with a route to the destination. Then a route reply message, containing the proper hop sequence for reaching the destination, is generated and unicast back to the source node.

1.2) Route Maintenance

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. [6]

B***. Hybrid Routing Protocol***

Hybrid routing protocols are a new generation of protocol, which are both are Proactive and Reactive in nature. Most hybrid protocols proposed to date are zone based, which means that the network is partitioned or seen as a number of zones by each node. Normally, Hybrid routing protocols for MANETs exploit hierarchical network architectures [7] [10]

Zone Routing Protocol (ZRP)

The hybrid approach combines the table-driven and source-initiated on-demand driven approaches such that the overhead incurred in route discovery and maintenance is minimized while the efficiency is maximized. The Zone Routing Protocol (ZRP) [10] partitions the network implicitly into zones, where a zone of a node includes all nearby nodes within the zone radius defined in hops. It applies proactive strategy inside the zone and reactive strategy outside the local zone. Each node may potentially be located in many zones. ZRP consists of two sub-protocols. The proactive intra zone routing protocol (IARP) is an adapted distance-vector algorithm. When a source has no IARP route to a destination, it invokes a reactive inter-zone routing protocol (IERP), which is very similar to DSR.

C. Proactive (Table Driven) Routing Protocol

Proactive routing protocols maintain information continuously. Typically, a node has a table containing information on how to reach every other node and the algorithm tries to keep this table up-to-date. Change in network topology is propagated throughput the network [8]. Examples: RIP STAR, RIPng, IGRP, OLSR INRIA, OLSRV2 etc.

Source tree adaptive Routing (STAR)

The STAR [16] protocol is based on the link state algorithm. Each router maintains a source tree, which is a set of links containing the preferred paths to destinations. This protocol has significantly reduced the amount of routing overhead disseminated into the network by using a least overhead routing approach (LORA) to exchange routing information. It also supports Optimum routing approach (ORA) if required. This approach eliminated the periodic updating procedure present in the Link State algorithm by making update dissemination conditional. As a result the Link State updates are exchanged only when certain event occurs. Therefore STAR will scale well in large network since it has significantly reduced the bandwidth consumption for the routing updates while at the same time reducing latency by using predetermined routes. However, this protocol may have significant memory and processing overheads in large and highly mobile networks, because each node is required to maintain a partial topology graph of the network. (It is determined from the source tree reported by its neighbors), which change frequently may as the neighbors keep reporting different source trees [8].

D. Different Traffic and Energy Consumption Modes

1) Traffic Model

Traffic model used in the simulation is (CBR) constant bit rate [10][11]. CBR represents constant-bit-rate traffic. It is generally used to either fill in background traffic to affect the performance of other applications being analyzed, or to simulate the performance of generic network traffic. The CBR model collects the following statistics:

1. Time when source to destination node session is started
2. Time when source to destination node session is closed
3. Number of bytes sent
4. Number of bytes received Throughput

2. Battery Power Consumption Model

The Battery power consumption of the mobile devices depends on the operating mode of its wireless network interfaces. Considering a broadcast transmission between the nodes of the active network, then wireless interfaces can be assumed to be in any of the following operating modes:[10][11][12]

1. transmit: source node packet transmitting,
2. receive: source to destination nodes packets received,
3. idle: in this mode the node is ready to transmit or receive packets,
4. Sleep: it is the low power consumption
5. mode state when a node cannot transmit or receive until woken up.

3. Power Consumption Model

The mobile nodes in Manet are connected between sources to destination nodes. These nodes are free to transmit (Tx) and receive (Rx) the data packet to or from other nodes and require energy to such activity. The total energy [7] [13] of nodes i s used up in following modes: These modes of power consumption are described as:

(1) Transmission Mode
(2) Reception Mode
(3) Idle Mode.

3.1) Transmission Mode

A node is supposed to be in transmission mode when it communicate data packet to other nodes in network. These nodes need energy to transmit data packet, such energy is called Transmission Energy (Tx) of that node. [17], [14] Transmission energy is depended on size of data packet which is transmitted (in Bits), if the size of a data packets is increased the required transmission energy is also increased. The amount of energy spent in transmitting and receiving the packets is calculated by using the following equations:

Energy Tx = (330*Packet Size)/2*106
Energy Rx= (230*Packet Size)/2*106

where , Packet size is specified in bits, Tx is transmission Energy.

3.2) Reception Mode

When a node communicates and receives a data packet from other nodes then it is called Reception Mode and the energy taken to receive packet is called Reception Energy (Rx), [15], [17]. Then Reception Energy can be given as:

Rx= (230* Packet Size)/2*106

And PR= Rx/ Tr, Where Rx is Reception Energy, PR is Reception Power, Tr is time taken to receive data packet.

Performance Evaluation Metrics:

To evaluate the performance of routing protocols various quantitative metrics are practiced [118]. In our research study six different quantitative metrics have been used to compare the performance of routing protocols against mobility of the nodes and traffic load conditions. The six important performance metrics are considered for evaluation of these routing protocols are as follows

Throughput :

Throughput is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet [119].

Throughput = Pr/Pf

Where Pr is the total number of Received Packets and Pf is the total number of Forwarded Packets.

3. ***Packets Dropped or loss*** :

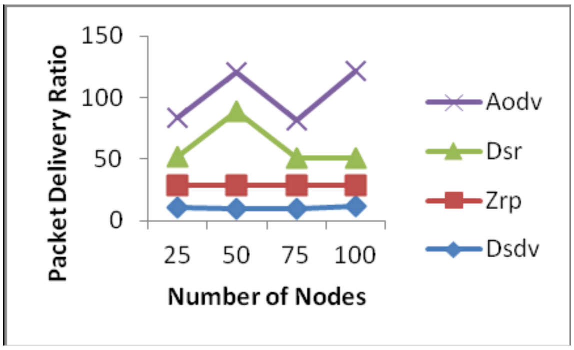
Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

Packet Loss % = (1-Pr/Ps)*100

Where Pr is total number of Received Packets and Ps is total number of Sent Packets.

4. Packet Delivery Ratio :

The ratio of the data packets delivered to the destinations to those generated by the CBR sources. It is the fraction of packets sent by the application that are received by the receivers [66].

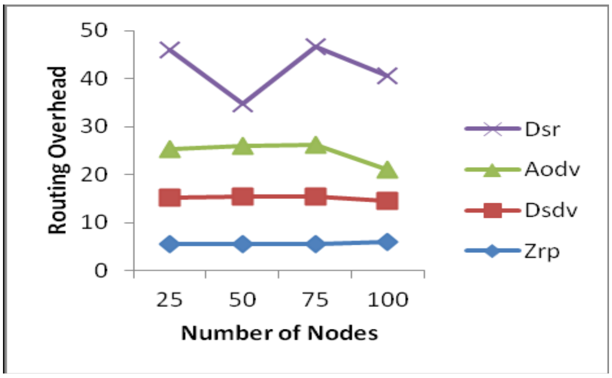


PDF = (Pr/Ps)*100

It is calculated by dividing the number of packet received by destination through the number packet originated from source. Where Pr is total Packet received & Ps is the total Packet sent.

Normalized Routing Overhead :

The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. The routing overhead describes how many routing packets for route discovery and route maintenance need to be sent in order to propagate the data packets [67].



Overhead = number of RTR packets (or)

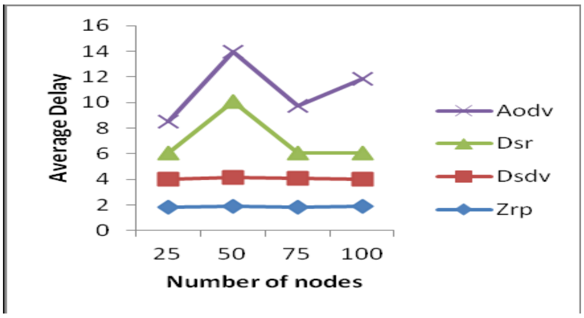
NRL = Routing Packet/Received Packets

5. ***End-to-End Delay –***

End-to-End delay indicates how long it took for a packet to travel from the source to the application layer of the destination. [65]. i.e. the total time taken by each packet to reach the destination. Average End-to-End delay of data packets includes all possible delays caused by buffering during route discovery, queuing delay at the interface, retransmission delays at the MAC, propagation and transfer times.

D = (Tr –Ts)

Where Tr is receive Time and Ts is sent Time.



SIMULATION ENVIRONMENT:

NS-2 (Network Simulator-2):

The NS-2 [3] is functions of a Network Simulator [9] to create the event scheduler, to create a network, for computing routes, to create connections, to create traffic. It is also useful for inserting errors and tracing can be done with it. Tracing packets on all links by the function trace-all and tracing packets on all links in nam format using the function namtrace-all.

Simulation environment is as follows:

Parameter Values	**Parameter Values**
Traffic type	CBR
Simulation time	100 seconds
Number of nodes	100
Pause time	0, 25, 50, 75 and 100 second
Maximum connections	15, 30 and 45
Maximum speed of nodes	10 meter per second
Transmission rate	10 packets per second
Area of the network	800m X 800m

Parameters	**Value**
Routing Protocols	AODV, DSDV, OLSR
MAC Layer	802.11
Packet Size	512 bytes
Terrain Size	1000m * 1000m
Nodes	50
Mobility Model	Manhattan Grid Mobility Model
No. of Horizontal Streets	3
No. of Vertical Streets	3
Data Traffic	CBR, TCP
No. of Source	10, 40
Simulation Time	900 sec.
Maximum Speed	0-60 m/sec (interval of 10)

Parameter	**Value**
Simulator	NS 2.34
MAC Type	802.11
Simulation Time	100 seconds
Channel Type	Wireless Channel
Routing Protocol	AODV,AOMDV
Simulation Area	1520 m x 1520 m
Traffic Type	CBR
Data Payload	512 bytes/packet
Network Loads	4 packets/sec
Interface Queue Length	50
Interface Queue Type	DropTail/PriQueue
Number of nodes	25
Pause Time	0,10,20,40,60,80,100 sec
Mobility Model	Random Way point Mobility

Parameter	Value
Protocols	AODV, DSR and DSDV
Traffic Type	CBR
Simulation Duration	100 seconds
Packet Size	512 bytes
Simulation Area	800 m x 800 m
Number of mobile nodes	20,50,75,100,125
Pause Time	20 sec
Maximum speed	30 m/s
Sending Rate	4 packets/sec
Mobility model	Random way point

No. of Nodes	200
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	80 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point
Propagation model	Two Ray ground
Packet Rate	5 pkts/s

Parameters	Values
Simulator	NS-2.34
Protocol	AODV, DSR, DSDV, OLSR
Simulation Time	500 s
Simulation Area	500x500
Transmission Time	500 s
Traffic Type	UDP, TCP
Data Payload	0.01Mbps
No of Connections	8 connections
Mobility Model	Random Way Point

Parameter Name	Value
Speed of node	0 to 20 m/s
Density of node	5 to 200
Number of CBR sources	10
Speed of CBR link	10 packets per second
Packet Size	512 bytes
Wireless Radio	802.11
Transmission Range	50 m
Transmission rate	1 Mbps
Area of simulation	1500m x 1500m
Simulation time	300 seconds

Scenario for Simulation of DSDV and AODV:

Parameter	Values
Number of nodes	1st case 10 nodes 2nd case 20 nodes 3rd case 30 nodes 4th case 40 nodes 5th case 50 nodes
Simulation Time	100
Pause Time	2 s
Environment Size	700 x 400
Packet Size	512 bytes
Maximum Speed	10 m/s
Queue Length	50
Mobility Model	Random Waypoint Mobility

No. of nodes	Packet Delivery Ratio (%)	Throughput (kbps)	Routing Overhead
10	99.12	47.05	2.03
20	99.18	47.74	2.19
30	97.79	42.10	2.48
40	98.10	48.58	2.23
50	98.54	58.12	2.02

Performance of AODV Routing Protocol in various numbers of Nodes with 20 connections fixed

Parameter Name	Value
Topology	800×800, 1000×1000, 2450×2450 and 3500×3500 (m)
No. of Nodes	50, 100, 250 and 500
Mobility Model	Two Ray ground
Simulation Time	50 Seconds
Pause Time	5
No. of Connections	20
Buffer length	60
MAC Protocol	IEEE 802.11
Packet Size	512 Bytes
Traffic Type	Cbr
Mobility Speed	5 m/s
Traffic Rate	4 Packets/Second

No. of nodes	Packet Delivery Ratio (%)	Throughput (kbps)	Routing Overhead
10	98.41	43.47	2.31
20	98.21	41.69	2.72
30	96.84	44.76	2.67
40	97.73	45.20	2.63
50	97.97	57.57	2.14

EXPERIMENTAL RESULTS :

The simulation results are routing protocol under various conditions was evaluated at random for five samples in terms of five performance metrics, routing load, delivery packet ratio, packet drop, end-to-end delay and throughput. In our simulation structure we used 10 numbers of loss dependent parameters and retrieve maximum as well as minimum dependent parameters. For that purpose here we define two level of simulation as follows. Experimental Parameters and their Levels

Parameter	Level1	Level2
Terrain Size(A)	800*800	1000*1000
No of Nodes(B)	50	100
No of Source Nodes(C)	5	10
Transmission rate(D)	5	20
Node Speed (E)	2	10
Pause time(F)	50	150
Queue Size(G)	50	10
Transmission range(H)	500	600
Antenna height(I)	1.0	1.5
Receiving Power(J)	20	10

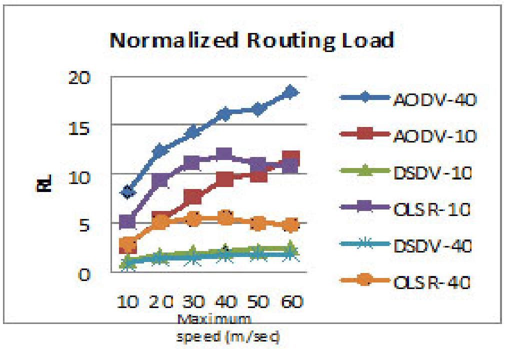
Calculated values:

Parameter	Level1	Level2
1	2.6533	1.7886
2	2.2585	2.0105
3	2.6852	1.0203
4	2.7709	1.7102
5	2.1671	2.1018
6	1.9947	2.2276
7	1.2203	3.0487
8	0.2928	2.7897
9	1.6735	2.4418
10	1.4746 2	.7943

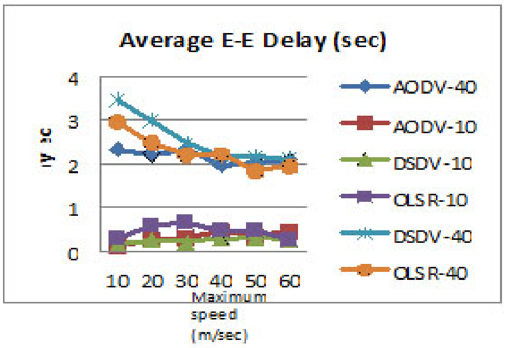
Simulator	Ns-2.35
Protocols	AODV,DSDV,DSR
Simulation duration	600 seconds
Simulation area	600 m*600 m
Movement model	Gauss Markov
MAC Layer Protocol	IEEE 802.11
Traffic type	CBR
Data payload	512 bytes/packet
Pause time	0.2 s

75 nodes for AODV and ZRP protocol

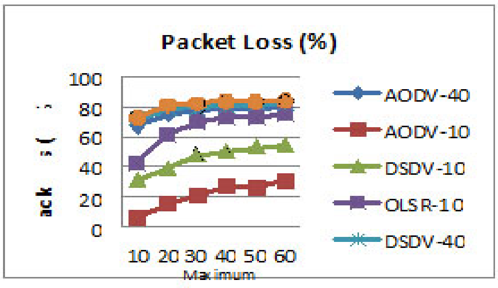
Parameter	Value
Number of Nodes	25, 50, 75, 100
Traffic	CBR
Network Size	1200 x 1200
Simulation Time	10 sec
Path loss Model	Two- Ray Propagation Model
Protocol	802.11
Data Link Layer	MAC 802.11



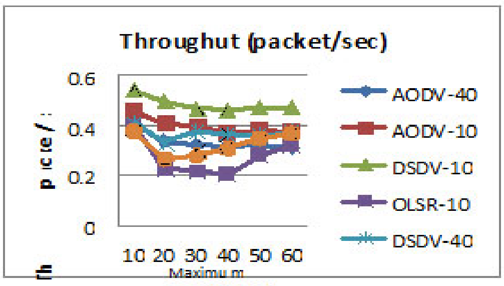
NRL vs Speed



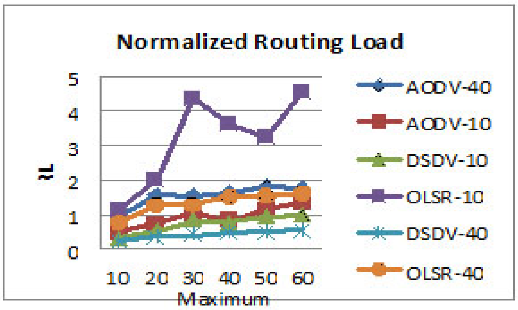
Avg. E-E Delay vs Speed



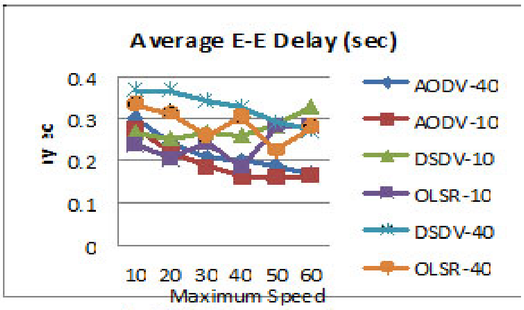
Packet Loss vs Speed



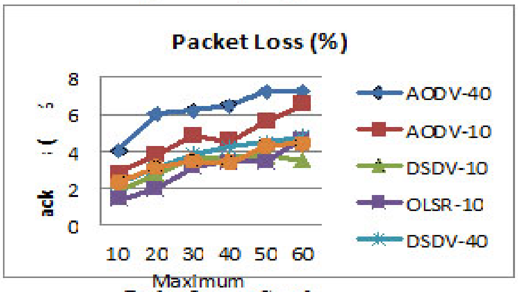
Throughput vs Speed



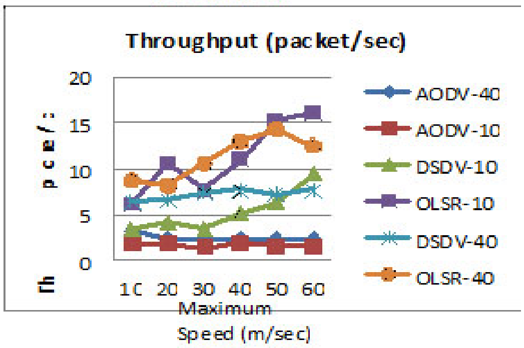
NRL vs Speed



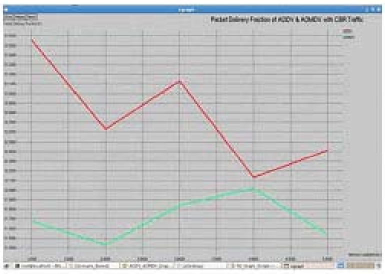
Avg. E-E delay vs Speed



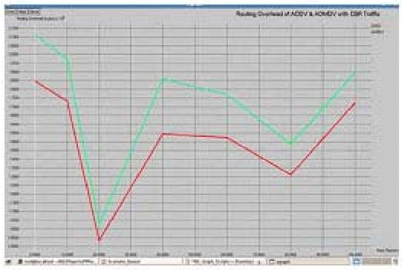
Packet Loss vs Speed



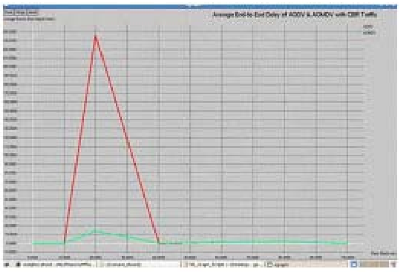
Throughput vs Speed



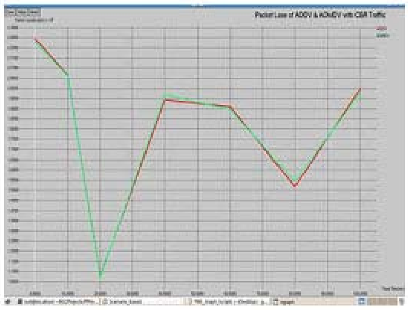
Packet Delivery Ratio



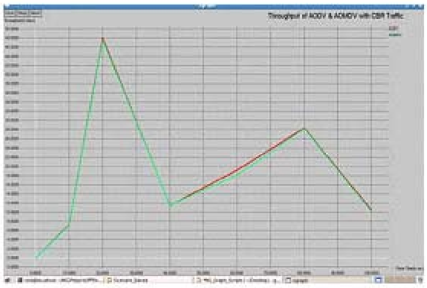
Routing over head



End to End Delay



packet Loss



Throughput

Increasing nodes and loss

CONCLUSIONS AND FUTURE WORK

The protocols are compared in terms of the variation in pause time and network load in CBR traffic under RWM. Due to randomness in mobility, the RWM and CBR are selected as scenario parameters. The AOMDV protocol is giving better performance than the AODV protocol for most of the performance parametric measures. The ROH and NROH parameters are comparatively high for AOMDV protocol which h can be reduced by the reduction of control packets. The future work of the research will focus on the reduction of the usage of control packets in routing.

REFERENCES

[1] Sapna S. Kaushik, P.R.Deshmukh, “Comparison of effectiveness of AODV, DSDV and DSR Routing Protocols in Mobile Ad hoc Networks”, International Journal of Information Technology and Knowledge Management, Vol. 2(2), pp.499-502, 2009.

[2] V.C.Patil, Rajashree, V.Biradar, R.R. Mudholkar, S.R.Sawant, “On-Demand Multipath Routing Protocols for Mobile Ad Hoc Networks Issues and Comparison”, International Journal of Wireless Communication and Simulation, Vol. 2(1), pp. 21-38, 2010.

[3] Elizabeth M. Royer, C-K Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications, pp.46-55, April 1999.

[4] S.Corson, J.Macker, “Routing Protocol Performance Issues and Evaluation Considerations”, RFC2501, IETF Networking Group, January 1999.

[5] R.L.Lagendijik, J.F.C.M.de Jongh, “Multipath Routing in Mobile Ad Hoc Networks”, Traineeship Report, Version 1.2, TU- Delft/TNO, 2003.

[6] Mohd Izuan Mohd Saad, Zuriati Ahmad Zukarnain, “Performance Analysis of Random-based Mobility Models in MANET Protocols”, European Journal of Scientific Research, Vol. 32(4), pp. 444-454,2009.

[7] Thomas Clausen, Philippe Jacquet, Laurent Viennot, “Comparative study of CBR and TCP Performance of MANET routing protocols”, Technical report, Project HiPERCOM, INRIA Rocquencourt, 2002.

[8] Vikas Singla, Parveen Kakkar,“Traffic Pattern based performance comparison of Reactive and Proactive protocols of Mobile Ad-hoc Networks”, International Journal of Computer Applications, Vol. 5(10), pp.16-20,2010.

[9] Harminder S. Bindra1, Sunil K. Maakar, A. L.Sangal , “Performance Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model”, IJCSI International Journal of Computer Science Issues, Vol. 7(10), pp.38-43, 2010.

[10] C.P.Agrawal, O.P.Vyas, M.K.Tiwari, “Evaluation of varying mobility models & network loads on DSDV protocol of MANETs”, International Journal of Computer Science and Engineering,Vol. 1(2), pp. 40-46, 2009.

[11]The Network Simulator ns-allinone-2.34,http://www.isi.edu/nsnam/ns/

[12] Kevin Fall, K. Varadhan, "The ns Manual",University of Southern California, InformationSciences Institute (ISI), http://www.isi.edu/nsnam/ns/ns-documentation.html.
[13] NS-2 with Wireless and Mobility Extensions,http://www.monarch .cs.cmu.edu.
[14] The Bonn Motion, http://bonnmotion.cs.unibonn.de/
[15] A.Valarmathi, RM.Chandrasekaran, “Congestion Aware and Adaptive Dynamic Source Routing Algorithm with Load Balancing in MANETs”,International Journal of Computer Applications, Vol. 8(5), pp.1-4, 2010.
[16] Anuj K. Gupta, Harsh Sadawarti, Anil K. Verma,“Performance analysis of AODV, DSR & TORA Routing Protocols”, IACSIT International Journal of Engineering and Technology, Vol. 2(2), pp.226-231,2010.
[17] S. R. Das, R. Castaeda, J. Yan, “Simulation-based performance evaluation of routing protocols for mobile ad hoc networks”, Mobile Networks and Applications, Vol. 5, pp.179–189, 2000.
[18] Sujata V.Mallapur, Sujata .Terdal, Enhanced, “Ad-Hoc on Demand Multipath Distance Vector Routing Potocol (EAOMDV)”, International Journal of Computer Science and Information Security, Vol. 7(3), pp.166-170, 2010.
[19] Mahesh K. Marina and Samir R.Das, “On-Demand Multipath Distance Vector Routing in Ad-hoc Networks”, In proceedings of the IEEE International Conference on Network Protocols, 2001 pp 14-23.
[20] Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment, by Nor Surayati Mohamad Usop, Azizol Abdullah, IJCSNS International Journal of Computer Science and Network Security, 9, No.7, July 2009.
[21] H. S. Bindra, S. K. M aakar and A. L. San gal, “Performan ce Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model”, IJCSI (Internal journ al of Computer Science Issues, Vol. 7, Issue. 3, No 10, May 2010.
[22] N. Adam, M. Y. Ismail, J. Abdullah, “Effect of Node Density of Performances of Three MANET Routing Protocols”, Dep artment of Science Phy sics, Dep artment of Communication Eng., Faculty of Science and Technology, Fac. of Electrical and Electronic Eng., University of Malaysia Terengganu, University of Tun Hussein Onn Malaysia 2010, P 321-325.
[23] V.C. Patil, R.V. Biradar, R.R. Mudholkar and S.R. Sawant, On-demand multipath routing protocols for mobile ad hoc networks issues and comparison, International Journal of Wireless Communication and Simulation 2 (1) (2010), pp.21–38.
[24] N. Jaisankar and R. Saravanan, An extended AODV protocol for multipath routing in MANETs, International Journal of Engineering and Technology 2 (4) (2010).
[25] S.S. Tyagi and R.K. Chauhan, Performance analysis of proactive and reactive routing protocols for ad hoc networks, International Journal of Computer Applications 1(14) (2010).

AUTHORS PROFILE

Mr K S R Murthy an Assistant professor of the Department of Infotrmation Technology Sreenidhi Institute of science and technology ,Hyderabad , A..P, India. He is an active Research Scholar at Andhra University in the areas of Ad hock networks Network Security, Cryptography and Mobile Computing, Data Mining.

Dr. G. Samuel Vara Prasada Raju received the M.Tech degree in CSE from Andhra University in 1993. He received PhD degree from Andhra University in 1996. From 1994 to 2003 worked as Asst. Professor in the Dept. of CS&SE in Andhra University College of Engineering. From 2003 onwards worked as Associate Professor and Director of the CS&SE Department for School of Distance Education of Andhra University College of Engineering His research interest includes ecommerce, Network Security, Cryptography and Data Mining. He has more than 20 years experience in Academics and Research