Performance Evaluation of routing protocols with and without malicious nodes

Snehal Mendadkar [1,*], and Poornima *Talwai*[1]

[1]Department of Electronics Engineering, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, 400 706, India

Abstract. Vehicular adhoc networks (VANETs) are made by applying the standards of mobile adhoc networks (MANETs)-the unconstrained making of a remote network of cell phones to the area of vehicles. VANETs were first referenced and presented in 2001 under "vehicle to-vehicle specially appointed versatile correspondence and systems administration" applications, where networks can be shaped and data can be handed-off among vehicles. It was shown that vehicle-to- vehicle and vehicle-to-road side exchange designs will exist together in VANETs to give street security, route, and other side of the road administrations. VANETs are a vital piece of the intelligent transportation frameworks (ITS) system. At times, VANETs are known as Intelligent Transport Networks. They are perceived as having advanced into a more extensive "Web of vehicles". Which itself is relied upon to eventually advance into a "Web of self-sufficient vehicles". The vehicles send some data about street status and traffic. But sometimes the information send from one vehicle to another can be malicious. This malicious information is added by the intruders to cause problem in vehicular network so that accident can occur. In this report, we will analyse the throughput, packet delivery ratio and end to end delay in sending information from vehicle to vehicle when the network is attacked by some malicious nodes.

1 Introduction

Recently, the streets have seen a huge expansion in the quantity of vehicles, which brought about an increment in auto collisions and traffic clog on the streets. [1-3] Due to these, it got important to give security and comfort to the driver on the street. Thus, the requirement for a network named VANET came into existence. Vanet is an invention which utilizes
Vehicles as mobile nodes to set up a remote association between them without the need of any focal base station or any regulator. It permits the vehicles sending and receiving data between one another and the climate encompassing them.

Vanet can be utilized for security, well-being applications such as improved route, area based administrations like finding the nearest fuel station or cafe, entertainment hubs, access to internet on go, vehicle security.[4] From the last decade, mobile adhoc networks have changed the car business by giving whenever anyplace correspondence between various gadgets. This simplicity of correspondence permits trade of significant data between gadgets simply in a hurry. The
Consistent exchange of data on on-going bases has ended up becoming another worldview in the business. Correspondingly, the advances in the data innovation and correspondence have effortlessly upheld the possibility of correspondence between mobile devices. [6]

2. Vehicular Adhoc Routing Protocols

2.1 *Ad-hoc On Demand Distance Vector Routing Protocol (AODV)*

It is on demand convention in which every hub keeps up the routing information by using steering table which is kept up at every hub of the organization. In routing table, target area, next jump IP address and target progression number is taken care of. Course interest (RREQ), Hello message, Route answer (RREP) and Route Error (RERR) are the four kinds of messages used in AODV framework. Hi message is used to screen associates, each organization in network broadcast the Hello Message, and this invite message will be received by all neighbour hubs. Invalid Links are recognized if hub fails to get any of the control or data information message. Course Request is used when a source S needs to send data to Destination ID, this allure is imparted to neighbours. All of the widely appealing hubs among source and target transmission the requesting in two cases, one they don't get the allure already or second
It's everything except the goal hub. If momentary is the target or it having the course to objective, it will reply to source in jump by hopping. [7-9]

2.2 Dynamic source Routing Protocol (DSR)

It is an On-Demand routing protocol in which the sequence of nodes through which a packet needs to travel is calculated and maintained as an information in packet header. Every mobile node in the network needs to maintain a route cache where it

* Corresponding author: snehalmendadkar69@gmail.com

caches source routes that it has learned. When a packet is sent, the route-cache inside the node is compared with the actual route needs to be covered. If the result is positive, the packet is forwarded otherwise route discovery process is initiated again. [10]

2.3 Destination Sequenced Distance Vector (DSDV)

DSDV is table driven routing protocols using Bellman Ford Algorithm to determine a way. As DSDV uses proactive philosophy all hubs in the organization understands a course to every single Hub in the organization going before correspondence. Hence every hub in the organization broadcast HELLO information at typical range to get information about the neighbour hubs, course available to show up at the neighbour hub and to recognize the real or invalid association. A routing table is kept up at every hub to store every one of this information. Every objective course is connected with a characteristic of progression number. [11]

3. Problem Statement

1. The goal of the work is to think about the exhibition of the three routing protocols dependent On-Demand Behaviour, for example AdHoc On-Demand Distance Vector (AODV), Dynamic Source Routing(DSR) and Destination-Sequenced Distance Vector routing, for remote adhoc networks dependent on the presentation and examination has been made based on their properties like the throughput, packet drop ratio (PDR), Average end-to-end delay and packet data loss regarding various situations one by fluctuating the number of nodes, changing the speed of the vehicles with constant number of nodes in the network.

2. The second significant issue in utilizing the VANET network as ITS innovation and its execution in reality is the security and protection of the application. As a wireless network, VANET is vulnerable to few attacks. For instance, an aggressor can infuse false data into the network by sending traffic data that doesn't exist. Mistaken traffic data can make traffic be redirected starting with one street then onto the
Next. The results can cause traffic sticks surprisingly more terrible on the off chance that it's anything but a mishap. The network will be analysed on what results after the malicious nodes enter the network.

4 Methodologies

In this report, we use network test system NS-2 which is a discrete test system and item situated dependent on both C++ and OTcl. Ns-2 additionally plays out the reproduction on the foundation of two sort of document C++ and TCL. It is utilized for both wired and remote conventions and furthermore support
Client expanded conventions with IP convention. Ns-2 has numerous other reasonable highlights like a channel for remote, routing along different ways etc. The Simulations
were performed utilizing Network Simulator NS2.35. At first, situation and traffic records are created. These documents are utilized as contribution for TCL script. After execution of TCL script two records are made for example NAM document and trace file. Trace file are utilized to break down the conduct of network. Trace file is dissected utilizing AWK
scripts. Following steps are performed to run the simulation
1. Select performance parameters. (Throughput, delay, packet delivery ratio and
packet loss ratio).
2. Generate scenario using NSG2.1 and topology files using cbrgen and setdest commands.
3. Create TCL script with .tcl extension.
4. Execute TCL script (Use ns Command)
5. Generate Trace and NAM file.
6. Execute AWK script to measure performance.

5. Simulation Assumptions

The simulations were performed using Network Simulator 2 (NS-2.35). The traffic sources are Constant Bit Rate (CBR). The source destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' in a rectangular field of 500m x 500m with 20 nodes to 100 nodes. For the simulation we consider five different scenarios by varying packet size, varying number of nodes and spedd of the nodes.

6. Performance Metrics

To evaluate the evalauation of both proactive and responsive protocols different estimations measurements like: Throughput, start to finish delay, packet delivery ratio, number of dropped packets, number of sent packets, number of received packets has been surveyed.

4.4.1 Packet Delivery Ratio

Packet Delivery Ratio is a crucial factor to evaluate the display of routing protocol in any organization. The show of the protocol depends upon various limits picked for the simulation. The critical limits are parcel size, no of hubs, transmission range and the development of the organization. The Packet delivery ratio to be acquired from the hard and fast number of information packets displayed at objective isolated by the full scale information packets sent from sources. As such Packet Delivery Ratio is the extent of number of packets got at the objective to the amount of parcels sent from the source. The show is better when parcel Delivery Ratio is high. Mathematically it will in general be shown as

$$PDR = \frac{Total\ packets\ received\ by\ all\ destination\ node}{Total\ packets\ send\ by\ source\ nodes} \quad (1)$$

4.4.2 Average End to End Delay

Normal End-to-end delay is the time taken by a packet to course through the network from a source to its objective. The typical beginning to end delay can be procured enlisting
the mean of beginning to end deferral of all viably passed on messages. Consequently, beginning to end delay midway depends upon the parcel conveyance extent. As the distance among source and objective grows, the probability of parcel drop increases. The typical beginning to end postpone recalls all possible deferrals for the association for instance buffering course revelation torpidity, retransmission delays at the MAC, and creating and transmission delay. Mathematically it will in general be shown as

$$D = \frac{1}{n} \sum_{1}^{n} (Tri - Tsi) * 1000[ms] \quad ---(2)$$

Where D = Average E2E Delay
i = packet identifier
Tri= Reception time
Tsi = Send time
n = Number of packets successfully delivered

4.4.3 Packet loss

Packet Loss is the proportion of the quantity of packets that never arrived at the destination to the quantity of packets started by the source. Numerically it tends to be displayed as follows.

$$PL = \frac{(nSentPackets - nReceivedPackets)}{nSentPackets} \quad -- (3)$$

where nReceivedPackets = Number of recieved packets
nSentPackets = Number of sent packets

4.4.4 Packet Loss Ratio

Packet Loss Ratio is the proportion of the quantity of packets that never arrived at the destination to the quantity of packets started by the source. Numerically it very well may be displayed as follows

$$PLR = \frac{(nSentPackets - nReceivedPackets)}{nSentPackets} * 100 \quad -(4)$$

Where nReceivedPackets = Number of received packets
nSentPackets = Number of sent packets

4.4.5 Throughput
The end-to-end network throughput measures the number of packets per second received at the destination. It is considered here as an external measure of the effectiveness of a protocol.

$$\text{Throughput} = \frac{(recvdSize)}{(stopTime - startTime)} * \frac{8}{1000}$$

Where recvdSize = Store received packet's size
stopTime = Simulation stop time
startTime = Simulation start time

7 Simulation Results

The simulations were performed using Network Simulator 2 (NS-2.35). The traffic sources are Constant Bit Rate (CBR). The source destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' in a rectangular field of 500m x 500m with 20 nodes to 100 nodes. For the simulation we consider five different scenarios by varying packet size, varying number of nodes and speed of the nodes.

Scenario1:- The nodes are moving with a constant speed of 20m/s. The simulation time is taken to be 600ms. The number of nodes are varying from 20, 40, 60, 80 and 100 with constant packet size of 512Mb.

PARAMETER	VALUES
PROTOCOLS	AODV, DSDV, DSR
NUMBER OF NODES	20,40,60,80,100
TRAFFIC TYPE	CONSTANT BIT RATE(CBR)
TRANSMISSION RANGE	250M
MOBILITY MODEL	RANDOM WAY POINT
SIMULATION AREA	500*500m
NODE SPEED	20m/s
PACKET SIZE	512MB
RADIO PROPAGATION MODEL	TWO RAY GROUND

Table 1;- Constant packet size of 512Mb with variable number of nodes

No of nodes	AODV	DSDV	DSR
20	0.1685	0.6428	1
40	0.0448	0.0491	0.0403
60	0.056	0.0493	0.0482
80	0.0743	0.0968	0.068
100	0.0746	0.0897	0.0586

Table 2:- Packet loss

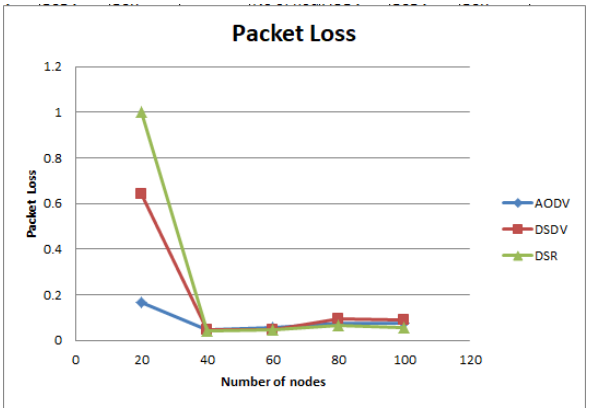
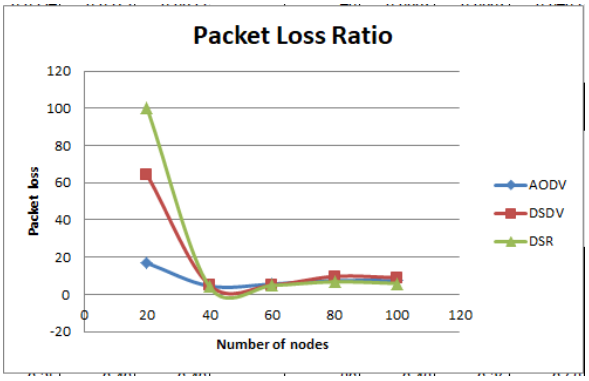


Figure 1:- Packet loss

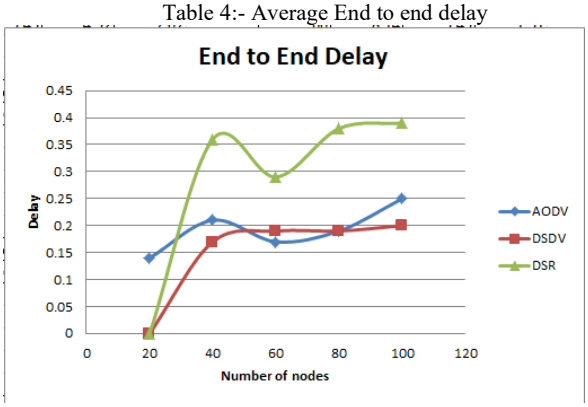
No of nodes	AODV	DSDV	DSR
20	16.85	64.28	100
40	4.48	4.91	4.03
60	5.6	4.93	4.82
80	7.43	9.68	6.8
100	7.46	8.97	5.86

Table 3:- Packet Loss Ratio



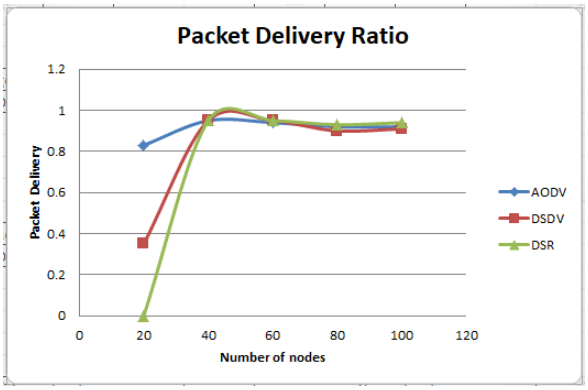
No of nodes	AODV	DSDV	DSR
20	0.14	0	0
40	0.21	0.17	0.36
60	0.17	0.19	0.29
80	0.19	0.19	0.38
100	0.25	0.2	0.39

Table 4:- Average End to end delay



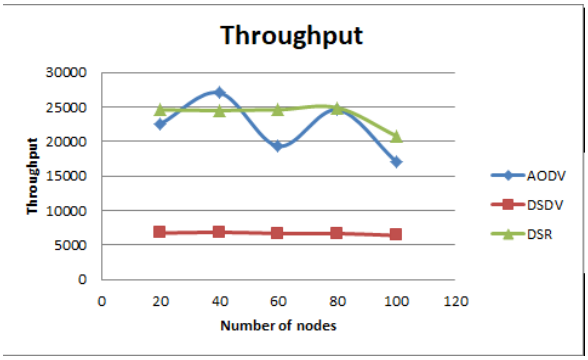
No of nodes	AODV	DSDV	DSR
20	0.83	0.35	0
40	0.95	0.95	0.95
60	0.94	0.95	0.95
80	0.92	0.9	0.93
100	0.92	0.91	0.94

Table5:- Packet delivery Ratio



No of nodes	AODV	DSDV	DSR
20	22546	6765	24596
40	27052	6881	24496
60	19328	6709	24600
80	24592	6709	24897
100	17085	6402	20812

Table 6:- Throughput



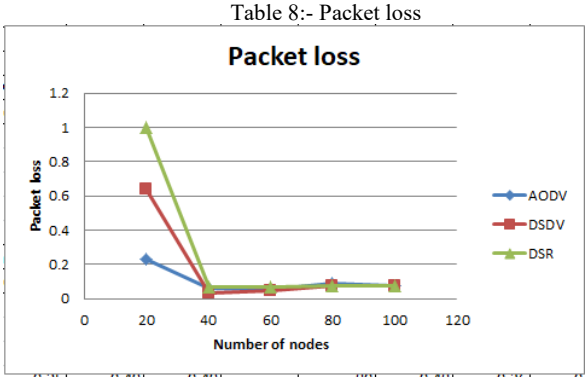
Scenario2:- The nodes are moving with a constant speed of 20m/s. The simulation time is taken to be 600ms. The number of nodes are varying from 20, 40, 60, 80 and 100 with constant packet sie of 1024Mb.

PARAMETER	VALUES
PROTOCOLS	AODV, DSDV, DSR
NUMBER OF NODES	20,40,60,80,100
TRAFFIC TYPE	CONSTANT BIT RATE(CBR)
TRANSMISSION RANGE	250M
MOBILITY MODEL	RANDOM WAY POINT
SIMULATION AREA	500*500m
NODE SPEED	20m/s
PACKET SIZE	1024MB
RADIO PROPAGATION MODEL	TWO RAY GROUND

Table7 :- Constant packet size of 1024 Mb with variable number of nodes

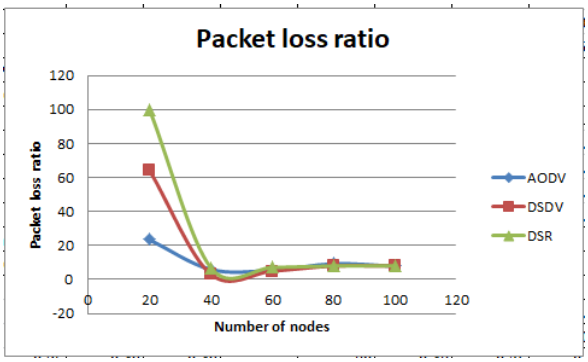
No of nodes	AODV	DSDV	DSR
20	0.2343	0.6428	1
40	0.0594	0.0315	0.0695
60	0.0545	0.0492	0.0707
80	0.0926	0.0795	0.0795
100	0.0782	0.0797	0.0797

Table 8:- Packet loss



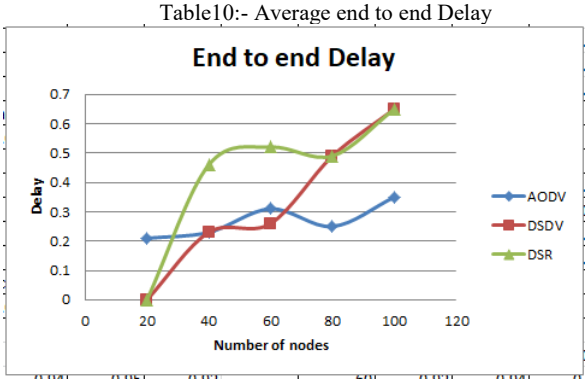
No of nodes	AODV	DSDV	DSR
20	23.43	64.28	100
40	5.94	3.15	6.95
60	5.45	4.92	7.07
80	9.26	7.95	7.95
100	7.82	7.97	7.97

Table 9:- Packet loss ratio



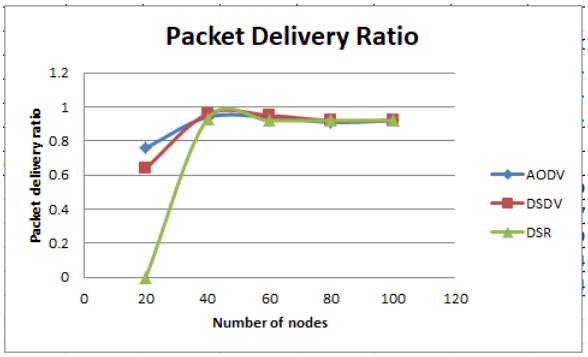
No of nodes	AODV	DSDV	DSR
20	0.21	0	0
40	0.23	0.23	0.46
60	0.31	0.26	0.52
80	0.25	0.49	0.49
100	0.35	0.65	0.65

Table10:- Average end to end Delay



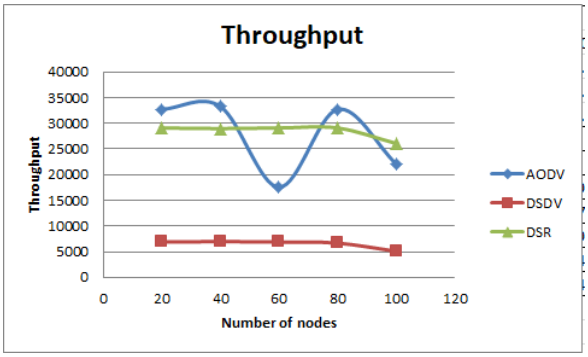
No of nodes	AODV	DSDV	DSR
20	0.76	0.64	0
40	0.94	0.96	0.93
60	0.94	0.95	0.92
80	0.91	0.92	0.92
100	0.92	0.92	0.92

Table11:- Packet Delivery ratio



No of nodes	AODV	DSDV	DSR
20	32723	6891	29091
40	33255	6991	28973
60	17547	6891	29091
80	32723	6687	29091
100	22084	5092	26076

Table12:- Throughput



Scenario3:-The nodes are moving with a constant speed of 20m/s. The simulation time is taken to be 600ms. The number of nodes are varying from 20, 40, 60, 80 and 100 with constant

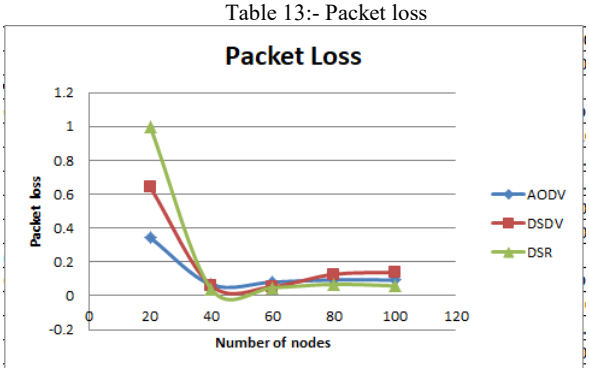
packet sie of 2048Mb.

PARAMETER	VALUES
PROTOCOLS	AODV, DSDV, DSR
NUMBER OF NODES	20,40,60,80,100
TRAFFIC TYPE	CONSTANT BIT RATE(CBR)
TRANSMISSION RANGE	250M
MOBILITY MODEL	RANDOM WAY POINT
SIMULATION AREA	500*500m
NODE SPEED	20m/s
PACKET SIZE	2048MB
RADIO PROPAGATION MODEL	TWO RAY GROUND

Table 11:- Constant packet size of 2048 Mb with variable number of nodes

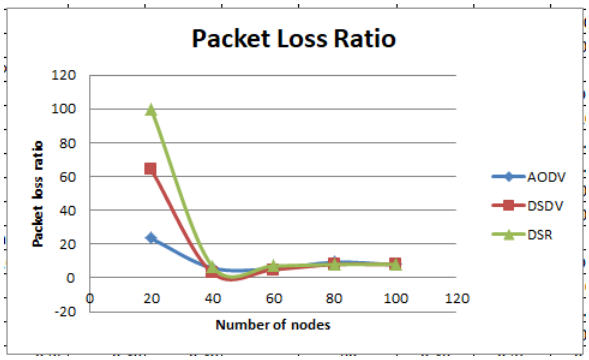
No of nodes	AODV	DSDV	DSR
20	0.3444	0.6428	1
40	0.0662	0.0602	0.0403
60	0.0814	0.0545	0.0482
80	0.0942	0.1273	0.068
100	0.0932	0.1378	0.0586

Table 13:- Packet loss



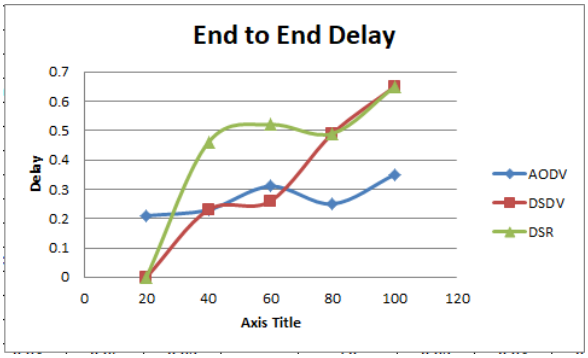
No of nodes	AODV	DSDV	DSR
20	23.43	64.28	100
40	5.94	3.15	6.95
60	5.45	4.92	7.07
80	9.26	7.95	7.95
100	7.82	7.97	7.97

Table 14:- Packet loss ratio



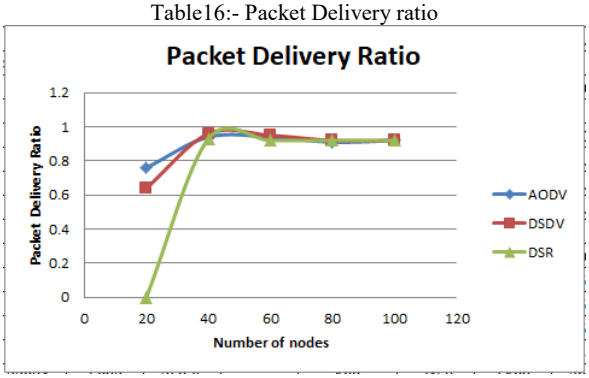
No of nodes	AODV	DSDV	DSR
20	0.21	0	0
40	0.23	0.23	0.46
60	0.31	0.26	0.52
80	0.25	0.49	0.49
100	0.35	0.65	0.65

Table 15:- Average End to End Delay



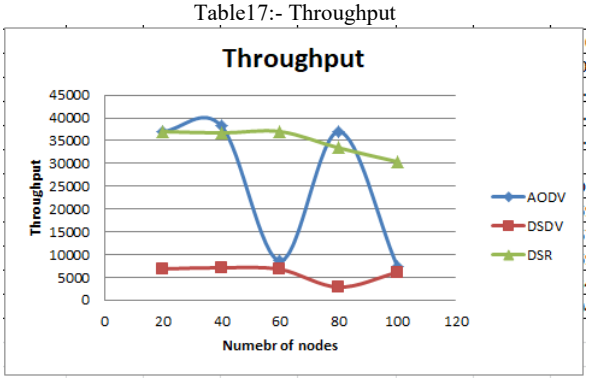
No of nodes	AODV	DSDV	DSR
20	0.76	0.64	0
40	0.94	0.96	0.93
60	0.94	0.95	0.92
80	0.91	0.92	0.92
100	0.92	0.92	0.92

Table16:- Packet Delivery ratio



No of nodes	AODV	DSDV	DSR
20	36993	6871	36998
40	38186	7137	36700
60	8631	6776	36998
80	36993	2872	33418
100	7458	6109	30400

Table17:- Throughput



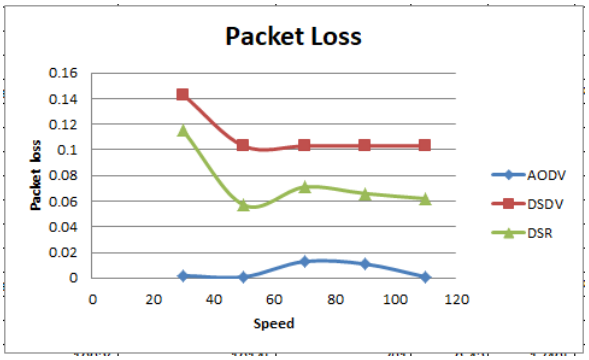
Scenario4:- The nodes are moving with variable speed of 30m/s, 50m/s, 70m/s, 90m/s and 110m/s. The simulation time is taken to be 600ms. The number of nodes are kept constant i.e
100 nodes with a packet size of 2048Mb.

PARAMETER	VALUES
PROTOCOLS	AODV, DSDV, DSR
NUMBER OF NODES	100
TRAFFIC TYPE	CONSTANT BIT RATE(CBR)
TRANSMISSION RANGE	250M
MOBILITY MODEL	RANDOM WAY POINT
SIMULATION AREA	500*500m
NODE SPEED	30m/s, 50m/s, 70m/s, 90m/s and 110m/s
PACKET SIZE	2048MB
RADIO PROPAGATION MODEL	TWO RAY GROUND

Table 18:- Varying speed of 100 nodes

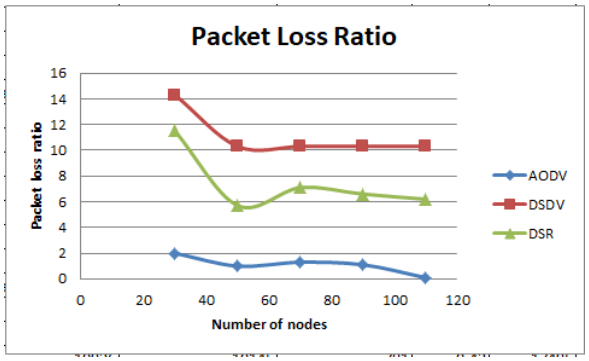
Speed	AODV	DSDV	DSR
30	0.002	0.143	0.115
50	0.001	0.103	0.057
70	0.013	0.103	0.071
90	0.011	0.103	0.066
110	0.001	0.103	0.062

Table 19:- Packet loss



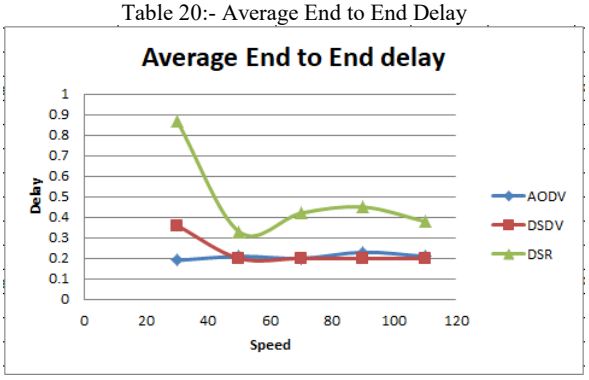
Speed	AODV	DSDV	DSR
30	2	14.3	11.5
50	1	10.3	5.7
70	1.3	10.3	7.1
90	1.1	10.3	6.6
110	0.1	10.3	6.2

Table 20:- Packet loss ratio



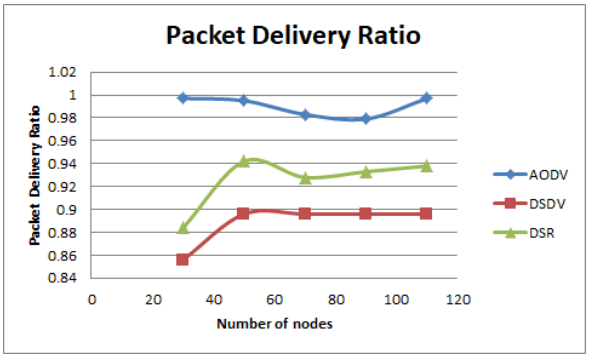
Speed	AODV	DSDV	DSR
30	0.19	0.36	0.87
50	0.21	0.2	0.33
70	0.2	0.2	0.42
90	0.23	0.2	0.45
110	0.21	0.2	0.38

Table 20:- Average End to End Delay



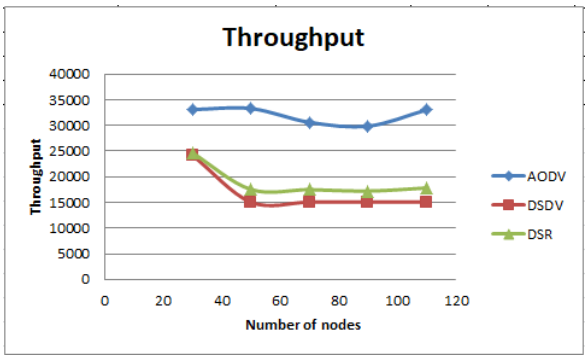
Speed	AODV	DSDV	DSR
30	0.997	0.856	0.884
50	0.995	0.896	0.942
70	0.983	0.896	0.928
90	0.979	0.896	0.933
110	0.997	0.896	0.938

Table 21:- Packet Delivery Ratio



Speed	AODV	DSDV	DSR
30	33082	24217	24669
50	33297	15069	17541
70	30605	15069	17495
90	29861	15069	17218
110	33035	15069	17833

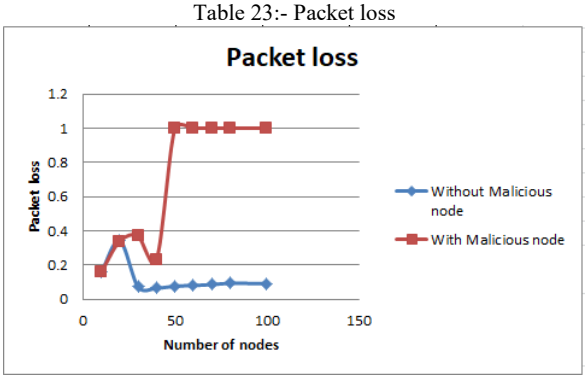
Table 22:- Throughput



Scenario5:- In this situation, the number of nodes are varied as 10, 20, 30, 40, 50, 60, 70, 80 and 100. The packet size of the data is kept constant to be 2048Mb.

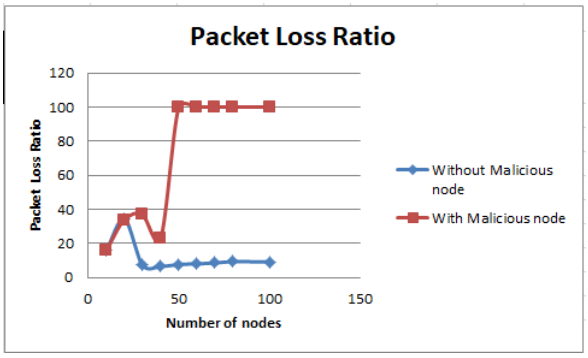
Total number of nodes	Without Malicious node	With Malicious node
10	0.16	0.16
20	0.3444	0.34
30	0.074	0.37
40	0.0662	0.23
50	0.078	1
60	0.0814	1
70	0.087	1
80	0.0942	1
100	0.0932	1

Table 23:- Packet loss



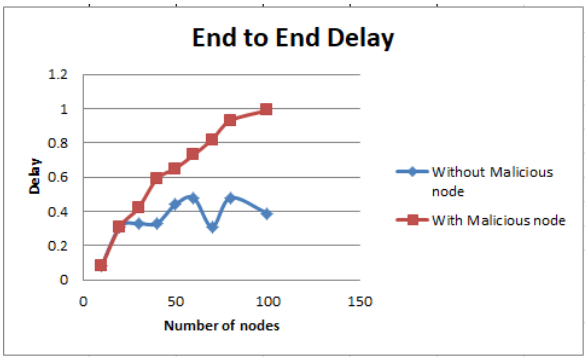
Total number of nodes	Without Malicious node	With Malicious node
10	16	16
20	34.44	34
30	7.4	37
40	6.62	23
50	7.8	100
60	8.14	100
70	8.7	100
80	9.42	100
100	9.32	100

Table 24:- Packet loss ratio



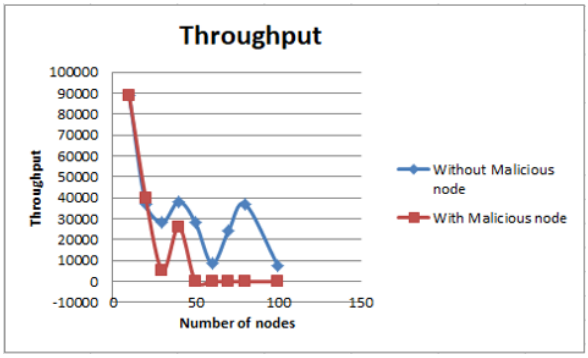
Total number of nodes	Without Malicious node	With Malicious node
10	0.08	0.08
20	0.31	0.31
30	0.33	0.42
40	0.33	0.59
50	0.44	0.65
60	0.48	0.73
70	0.31	0.82
80	0.48	0.93
100	0.39	0.99

Table 25:- Average End to End Delay



Total number of nodes	Without Malicious node	With Malicious node
10	88539	88539
20	36993	39698
30	28152	5359
40	38186	26120
50	28152	0
60	8631	0
70	24292	0
80	36993	0
100	7458	0

Table 26:- Throughput



8. Analysis and Results

The simulations were performed using Network Simulator 2 (NS-2.35). The traffic sources are Constant Bit Rate (CBR). The source destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' in a rectangular field of 500m x 500m with 20 nodes to 100 nodes. For the simulation we consider five different scenarios by varying packet size, varying number of nodes and speed of the nodes.

Scenario1:- In this situation, the number of nodes are varied as 20,40,60,80 and 100. The packet size of the data is kept constant to be 512kB. The packet loss and Packet Loss Ratio is less in AODV as compared to DSDV and DSR. Packet delivery ratio is high in AODV. DSR has high End to End Delay whereas AODV and DSDV has less delay. DSR shows constant line of throughput ghraph whereas DSDV has low Throughput. So we can say that, AODV and DSR show best performance in this scenario.

Scenario2:- In this situation, the number of nodes are varied as 20,40,60,80 and 100. The packet size of the data is kept constant to be 1024Mb. The packet loss and Packet Loss Ratio is less in AODV as compared to DSDV and DSR. Packet delivery ratio is almost same in AODV, DSDV and DSR. DSR has high End to End Delay whereas AODV shows less delay. DSR shows constant line of throughput ghraph whereas DSDV has low Throughput. So we can say that, AODV and DSR show best performance in this scenario.

Scenario3:- In this situation, the number of nodes are varied as 20,40,60,80 and 100. The packet size of the data is kept constant to be 2048Mb. The packet loss and Packet Loss Ratio is less in AODV as compared to DSDV and DSR. Packet delivery ratio is almost same in AODV, DSDV and DSR. DSR has high End to End Delay whereas AODV shows less delay. DSR shows constant line of throughput graph whereas DSDV has low Throughput. So we can say that, AODV and DSR show best performance in this scenario.

Scenario4:- In this situation, the number of nodes is kept constant to be 100. The speed of the vehicles is changed from 30m/s, 50m/s, 70m/s, 90m/s and 110m/s. The packet size of the data is kept constant to be 512kB. As the speed of the vehicles is increasing, the packet loss and Packet Loss Ratio is less in AODV as compared to DSDV and DSR. Packet delivery ratio is high in AODV. DSR has high End to End Delay whereas AODV shows less delay. AODV shows high Throughput whereas DSDV has low Throughput. So we can say that, AODV and DSR show best performance in this scenario.

Scenario5:-In this situation, the number of nodes are varied as 10, 20, 30, 40, 50, 60, 70, 80 and 100. The packet size of the data is kept constant to be 2048Mb. The packet loss and Packet
Loss Ratio is more as the number of malicious nodes are increased in the network. Packet delivery ratio is lowest in AODV when malicious nodes are introduced in the network.
Average End to End Delay increases whereas throughput graph shows decreasing trend. This shows that when the network is infected by malicious nodes, the throughput and packet delivery ratio becomes the least where as the end to end delay and packet loss increases with the increase in malicious nodes.

When the network is moving without any malicious nodes, the performance matrics show different behaviour in each scenario. The packet loss, packet loss ratio is less and packet delivery ratio is more in each case. But when malicious nodes are introduced in the network, they degrade the performance of the network. Packet loss and packet loss ratio increases as the number of malicious nodes increase in the network. As packet loss increases, packet delivery ratio decreases. Packet delivery reduces as the malicious nodes drop the packets in the network. Throughput is dependent on the packets received and the time taken to receive the packets. The malicious nodes do not allow the packets to reach to the destination, hence reducing the throughput and efficiency of the network and increases the end to end delay of the packets reaching the destination node.

9. Conclusion

AODV performs best in the event of packet delivery ratio without malicious nodes in the network. As the number of malicious nodes enter the network, they degrade the network with respect to throughput, packet delivery ratio and End to End delay in the network. Analysis of malicious nodes shows that with malicious node and without malicious node the output of parameters are different. From the graph it is shown that
malicious nodes have less accuracy then malicious-less networks. Therefore security of MANET becomes fragile in presence of malicious nodes.

10. References

[1]Jakubiak, J.,Koucheryavy, Y. (2008, January). State of the art and research challenges
for VANETs. In 2008 5th IEEE Consumer Communications and Networking
Conference (pp. 912-916). IEEE.
[2] Youse_, S., Mousavi, M. S., Fathy, M. (2006, June). Vehicular ad hoc networks
(VANETs): challenges and perspectives. In 2006 6th International Conference on ITS
Telecommunications (pp. 761-766). IEEE.
[3] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N., Nemoto, Y. (2007).

A stable routing protocol to support ITS services in VANET networks. IEEE Transactions
on Vehicular technology, 56(6), 3337-3347.
[4] Abdullah, A., Ramly, N., Muhammed, A., Derahman, M. N. (2008). Performance comparison
study of routing protocols for mobile grid environment. IJCSNS International
Journal of Computer science and Network security, 8(2), 82-88.
[5] Mahmood, Z., Nawaz, M. A., Iqbal, M., Khan, S., Haq, Z. U. (2015). Varying pause
time e_ect on AODV, DSR and DSDV performance. Int. J. Wirel. Microwave Technol,
1, 21-33.
[6] Ripan, K., Verma, A. K. (2007). Performance Comparison of AODV and DSR Routing
Protocols in MANETs (Doctoral dissertation
[7] F□u_ler, H., Mauve, M., Hartenstein, H., K□asemann, M., Vollmer, D. (2002). A comparison
of routing strategies for vehicular ad hoc networks. Technical reports, 2.
[8] Johnson, D. B., Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless
networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.
[9] Li, F., Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. IEEE
Vehicular technology magazine, 2(2), 12-22.
[10] Henderson, T. (2011). Radio Propagation Models. Information Sciences Institute,
University of Southern California.[Online] Available: http://www. isi.
edu/nsnam/ns/doc/node216. html.
[11] Siraj, M., Kanrar, S. (2012). Performance of Modeling wireless networks in realistic
environment. arXiv preprint arXiv:1201.0842.
[12] Sto_ers, M., Riley, G. (2012, August). Comparing the ns-3 propagation models. In
2012 IEEE 20th International Symposium on Modeling, Analysis and Simulation of
Computer and Telecommunication Systems (pp. 61-67). IEEE.
28
[13] Abdullah, A., Ramly, N., Muhammed, A., Derahman, M. N. (2008). Performance
comparison study of routing protocols for mobile grid environment. IJCSNS International
Journal of Computer science and Network security, 8(2), 82-88.
[14] Perkins, C. E., Bhagwat, P. (1994). Highly dynamic destination-sequenced distancevector
Routing (DSDV) for mobile computers. ACM SIGCOMM computer communication
Review, 24(4), 234-244.
[15] Ab Rahman, R., Kassim, M., Yahaya, C. K. H. C. K., Ismail, M. (2011, June). Performance
analysis of routing protocol in WiMAX network. In 2011 IEEE International
Conference on System Engineering and Technology (pp. 153-157). IEEE.
[16] Nikam, S., Jadhav, B. T. (2016). Analysis of AODV Protocol against Pause Time
Using NS2. 34.
[17] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., Jetcheva, J. (1998, October). A
performance comparison of multi-hop wireless ad hoc network routing protocols. In
Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing
and networking (pp. 85-97).
[18]
The Network Simulator ns-2. http://www.isi.edu/nsnam/ns/index.html.