Performance Analysis of AODV, DSR, OLSR Routing Protocol in Ad hoc Networks

Jitesh Dhankar[1], Lakhan Singh[2], Ashok Yadav[3]
JB Institute of Technology, Dehradun
jitesh87.electronics@gmail.com,singh.lakhan313@gmail.com,ashok71986@gmail.com

Abstract—

In this paper, an effort has been made to examine and compare the performance of the reactive and proactive ad-hoc routing protocols by employing OPNET Simulator according to increasing number of failed nodes in the network. In current study, a comparison of reactive routing protocols such as Distance Vector Routing (DSR), Ad Hoc On-Demand Distance Vector Routing(AODV) and proactive routing protocols such as Optimized Link State Routing(OLSR) has been done in terms of delay, throughput and network load, by increasing amount of failed nodes in the network. Three routing protocols are being examined on the above specified parameters and had been found that OLSR performance is better as compared to AODV and DSR on persisting node failure in the network

Keywords: AODV, DSR, OLSR, MANET, OPNET

1 INTRODUCTION

Mobile ad hoc networks (MANET) are standards for mobile communication [1] [2] in which mobile nodes are arbitrarily and dynamically positioned in such a way that interaction between nodes does not depend on any fundamental fixed network infrastructure. Since no static infrastructure or centralized management exists, these networks are self-configured and end-to-end communication may need routing information through various intermediary nodes. Every device in a MANET is free to proceed independently in any direction, and will thus modify its connections to other devices immediately. The main issue in constructing a MANET is fitting every device to continuously manage the information needed to suitably propagate traffic [10]. There are various factors which causes the reduction of the network's performance. Among others, signal attenuation, node failure [3], and high bit error rate are causes to performance reduction in term of packet drop and obtained good throughput.

In specific way, dealing with node failure is a problem in wireless ad hoc environments. The employed device may work out of battery or move causing the disruption of the ongoing communication. The MAC layer is slow to determine these types of failures and to invoke the routing protocol to see for a new route to the destination node. In this paper, the simulation has been carried out to compare the performance measurement and comparison of three different routing protocols in terms of three different parameters i.e. delay, throughput and network load. This work offers a comparative study, by simulation, of three routing protocols i.e. AODV, DSR and OLSR for MANETs by utilizing the well-known network simulator OPNET Simulator [9].

1.1 Dynamic Source Routing (DSR)

DSR [4] is an on-demand reactive routing protocol planned to limit the bandwidth consumed by control packets in wireless networks by removing the periodic table update messages needed in the table-driven method. The basic strategy of this protocol (and all other on-demand routing protocols) during the route establishment step is to construct a path by broadcasting Route Request packets across the network. The destination node, on obtaining a Route Request packet, reply by sending a Route Reply packet in return to the source node, which holds the path traversed by the Route Request packet obtained. Source routing prompts the source node to construct an ordered list of intermediary nodes which would consists the complete path to the destination.

Every transmitted packet is then propagated having the complete path in its header. Since the route is detected in the packet, this routing approach exempts intermediary nodes from keeping routing information to propagate packets. The protocol composed of two route-regarding processes: the route discovery process and the route maintenance process. Every node keeps a route cache. Whenever a source node wants to send a packet, firstly it examines its route cache for a path to the destination node. In case it is found, the node utilizes that one found. In case the node does not discover any right path to the destination, it begins the route discovery process. In the route discovery process, the source node floods a Route Request (RREQ) packet, which is broadcasted via intermediary nodes. Nodes without path to the destination add their addresses to the RREQ packet and again flood it until it reaches the destination node or an intermediary node with a right path to the destination node. Then, it neglects the RREQ packet obtained. The destination node (or the intermediary node with a valid path), upon obtained the RREQ packet, routes a Route Reply (RREP) packet to the source node. It consists the complete path from the source node to the destination node.

1.2 Ad-hoc on demand distance vector (AODV)

Ad-hoc On-demand distance vector (AODV) [5] [6] [11] is another distance vector routing algorithm, a combination of both DSR [4] and DSDV [8]. It shares DSR's on-demand features hence find paths whenever it is required by a same route discovery process. However, AODV follows conventional routing tables; one entry per destination node which is opposite to DSR that keeps multiple route cache entries for every destination. AODV has other important features. Whenever a path exists from source node to destination node, it does not append any overhead to the packets. Since, route discovery process is only started when paths are not utilized and/or they died and immediately removed. This method decreases the impacts of state routes as well as the requirement for route maintenance for unused paths. Another important feature of AODV is the capability to offer multicast, unicast and broadcast communication. AODV utilizes a broadcast route discovery algorithm and then the unicast route reply massage.

1.3 Optimized Link State Routing (OLSR)

OLSR [6] is proactive hop by hop routing protocol. It is a modular protocol which contains an always needed core, and a collection of auxiliary functions. It is a proactive method, so it continuously attempts to discover paths to all possible destinations in the network. Proactive and link state nature could increase congestion in the network because of the routing traffic produced. However, because of its proactive nature, it has the benefit of having paths quickly available whenever they are needed. In order to decrease the amount of routing traffic created by the protocol and therefore optimize the algorithm to fulfill the needs of a mobile WLAN, OLSR presents Multipoint Relays (MPR). A MPR is a collection of chosen nodes which sends messages during the broadcasting process. Only nodes chosen as MPR members can forward control traffic and routing. Employing this method traffic produced at the broadcasting process is highly decreased, making this method a sort of selective broadcasting. A node chooses its MPR node members out of its neighboring nodes positioned at one hop distance from it. A node which chooses another node as a MPR node member is also known as MPR Selector of that node. Adopting these guidelines, neighbors of a provided node not involved in its MPR set receive and process control messages, but do not send them. MPR set deals with all nodes positioned two hops from the node. Generally, the smaller a MPR set, the lower control traffic produced in the network.

2 OPNET SIMULATOR

Simulator is commercial network simulation framework for network simulation and modeling. It permits the users to plan and analyze communication networks, protocols, devices and applications with scalability and flexibility. It models the network diagrammatically and its graphical editors reflect the structure of network components and actual networks.

3 SIMULATION ENVIRONMENT

this section the efficiency of the Ad-hoc routing protocols have been examined and verified by employing OPNET simulator [8] [12]. The calculation platform utilized is a desktop (2.5 GHz, 2GB RAM). Fig 1 indicates a network considered for this study. It is composed of 50 mobile nodes which a raw packet creator is transmitting packets over IP and WLAN, one static FTP server node with server applications running. This node provides support to one fundamental IEEE 802.11 connection at 1 Mbps or 2 Mbps. The operational speed is decided by the associated link's data rate application configuration which describes the kind of application executing in the network.

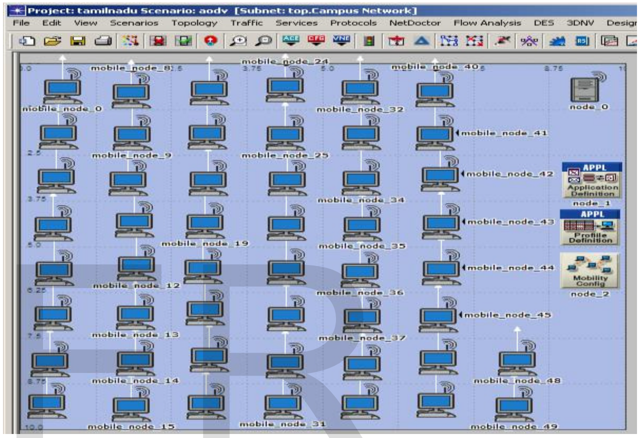

Fig. 1 MANET Scenario

The study has been carried out for the case when the whole network is healthy and the other when many of its nodes fail. Network's performance based on load in the network has been examined on the basis of the network throughput.

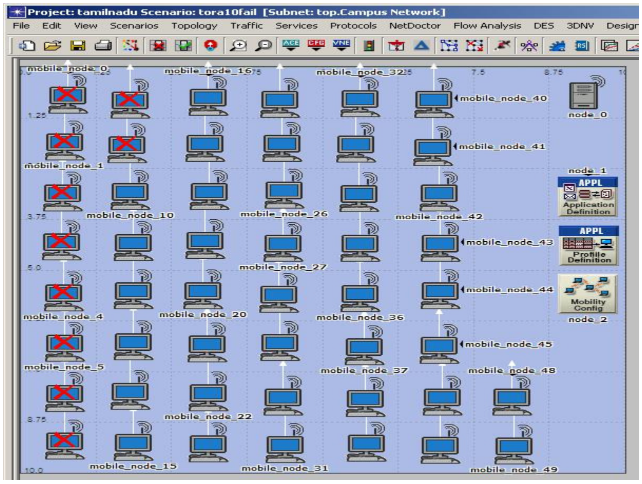

Fig 2 MANET scenario with ten nodes failed

Fig 2. describes the network under the situation of node failures. Random waypoint model [12] of mobility has been analyzed where nodes go moving until they reach at a random destination computed by the algorithm
Main features of the scenarios are shown in the Table 1.

Table 1: Simulation Parameters

Statistic	Value
Scenario Size	10*10 km
Simulation Time	1 h
Nodes	50
802.11 data rate	11 Mbps
Mobility Model	Random Waypoint

A. *Traffic Modeling*
This simulation environment is composed of 50 wireless nodes making an ad-hoc network, moving over about 10 x 10 kilometer area for about 1 hr of simulated time.

B. *Performance Matrices*
The parameters depends on which the protocols are formulated are the default parameters of the protocols. There are various metrics employing which one can compare these three protocols. In this work following performance metrics are utilized for design and analysis work.

Throughput can be defined as the average rate of successful message delivery over a communication medium. The time it considers by the receiver to obtain the last message is known as throughput [13]. Throughput is measured as bytes or bits per sec (byte/sec or bit/sec). Some factors influence the throughput as; if there are various configuration changes in the network, limited bandwidth available, unreliable communication among nodes, and restricted energy [13]. A high throughput is absolute selection in each network. Throughput can be defined numerically as in equation specified below:

$$\text{Throughput} = \frac{\text{No. of delivered packets*packet size*8}}{\text{Total duration of Simulation}}$$

Delay can be defined as time considered to push the packet's bits onto the connections. The delay of a network describes how long it consumes for a bit of data to move from one node to another node over the network.

Network load can be defined as the total number of packets transmitted per second.

4 RESULTS

Throughput is the ratio of the total data arrives a receiver from the sender. The network throughput for many routing protocols i.e. DSR, AODV and OLSR in successful operation of the network without any node breakage is described in Fig. 3. The network throughput as measured is maximum for OLSR and minimum for DSR and throughput of AODV lies between the two.

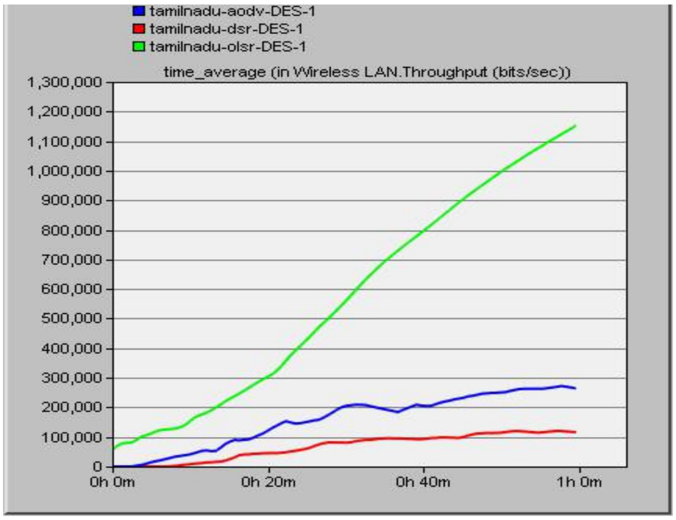

Fig 3 Simulation time v/s throughput (without node fail)

Fig. 4, 5and 6 shows the throughput of the network with 10, 20 and 30 failed nodes respectively. When node failure occurs, the network throughput for several routing protocols is examined. The network throughput for OLSR is better in comparison of DSR and AODV.

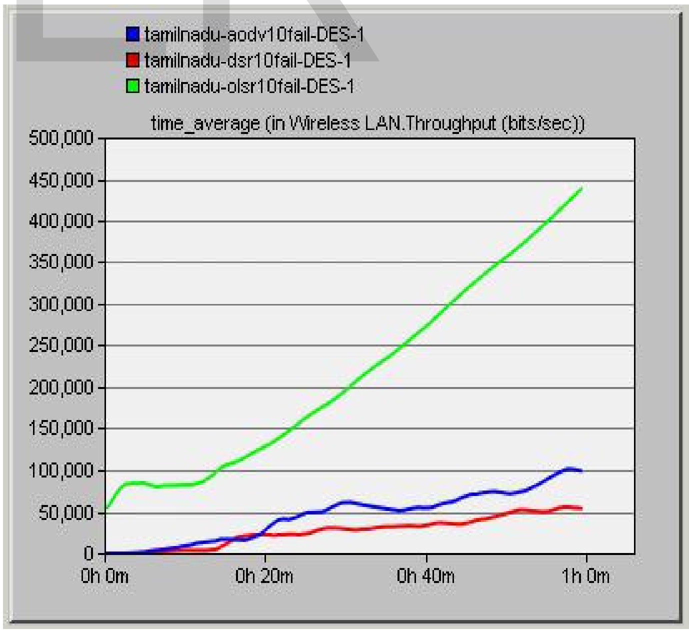

Fig 4 Simulation time v/s throughput (10 node fail)

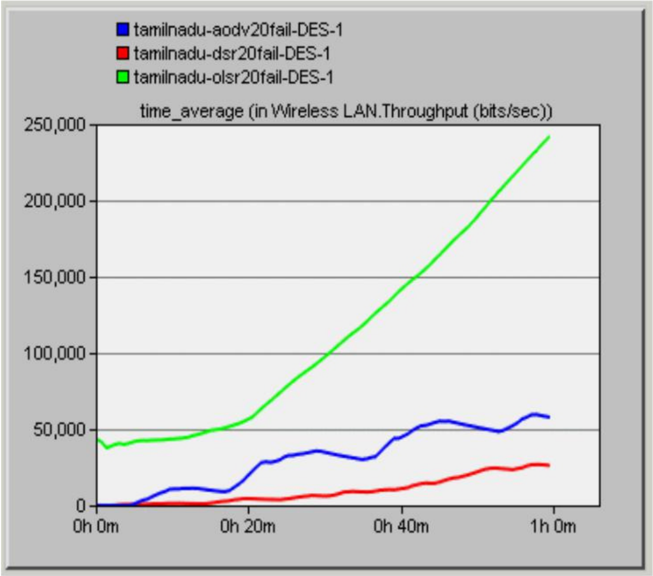

Fig 5 Simulation time v/s throughput (20 node fail)

Fig 7 shows the network delay for many routing protocols i.e. DSR, AODV and OLSR in successful operation of the network without any node failure. As depicted in fig 7, the network delay in condition of DSR is maximum and that for OLSR is least and for AODV it lies between the two. When the network is subjected to node failure, the network delay for the several routing protocols is examined. The simulation is executed and network is examined for various number of failed nodes. The impact of node failure is depicted in Fig 8, 9 and 10 respectively. When subjected to node failure the network delay in case of DSR is maximum and that for OLSR is least.

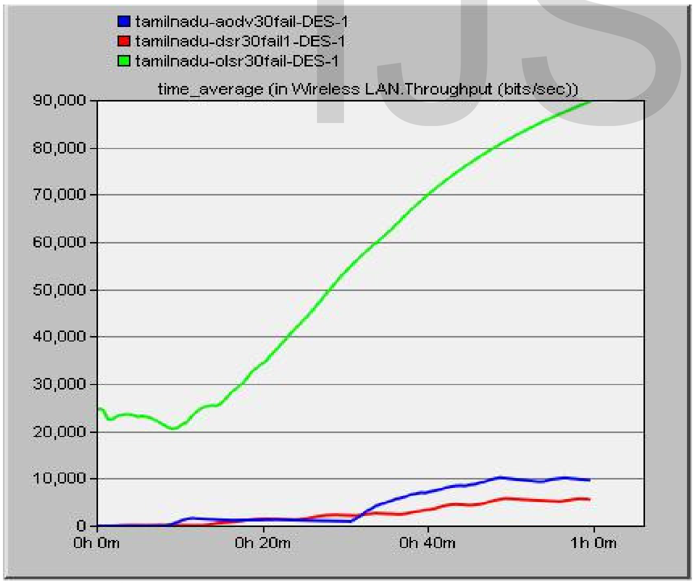

Fig 6 Simulation time v/s throughput (30 node fail)

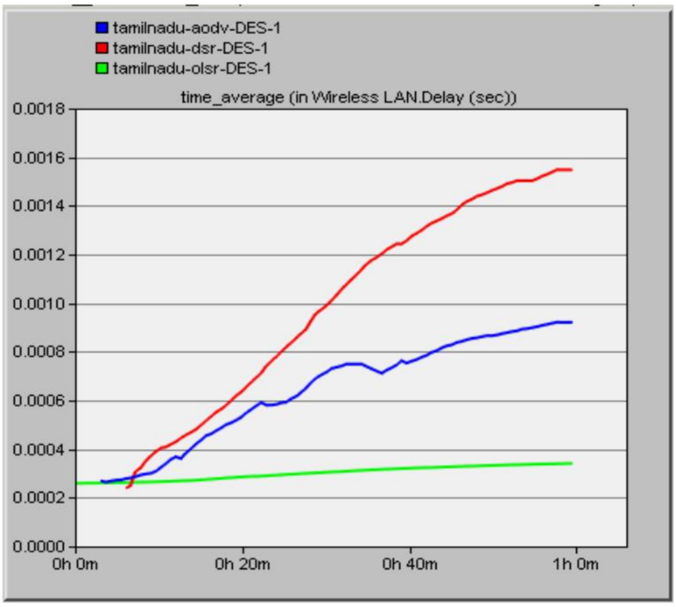

Fig 7 Simulation time v/s delay (without node fail)

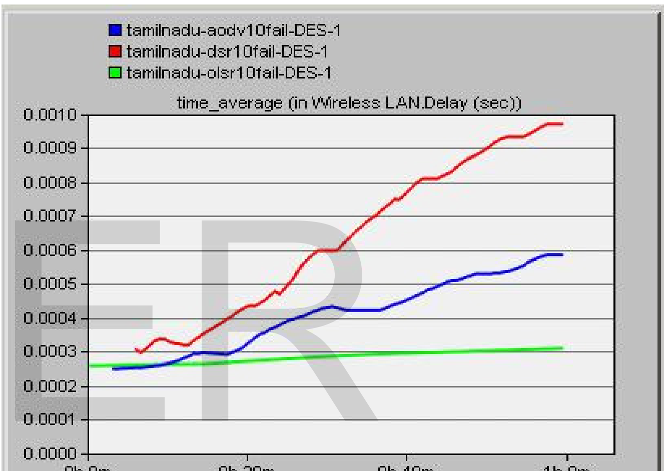

Fig 8 Simulation time v/s delay (10 node fail)

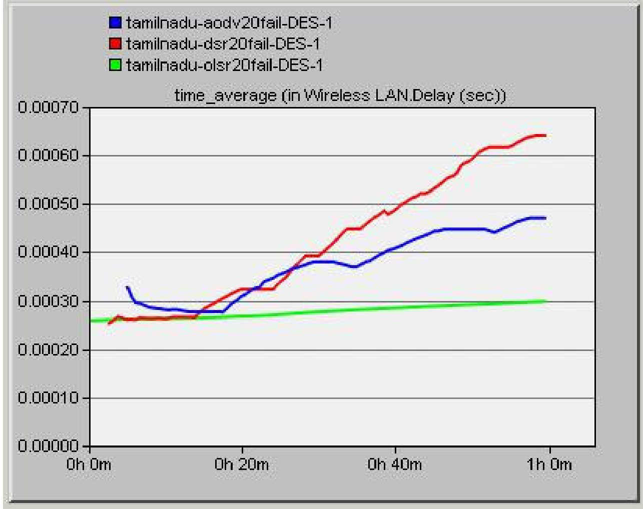

Fig 9 Simulation time v/s delay (20 node fail)

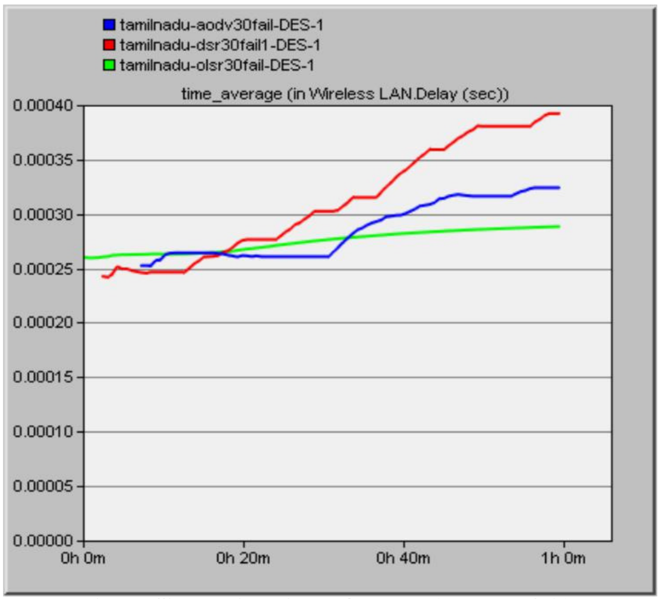

Fig 10 Simulation time v/s delay (30 node fail)

Fig 11 shows the network load for several routing protocols i.e. AODV, DSR and OLSR in successful operation of the network without any node failure. As shown in Fig 11, the network load in case of OLSR is maximum and that for DSR is least and for AODV lies between the two. When the network is subjected to node failure, the network delay for the several routing protocols is examined. The impact of node failure is depicted in Fig 12, 13 and 14 respectively. When subjected to node failure the network load in case of DSR is least and that for OLSR is maximum.

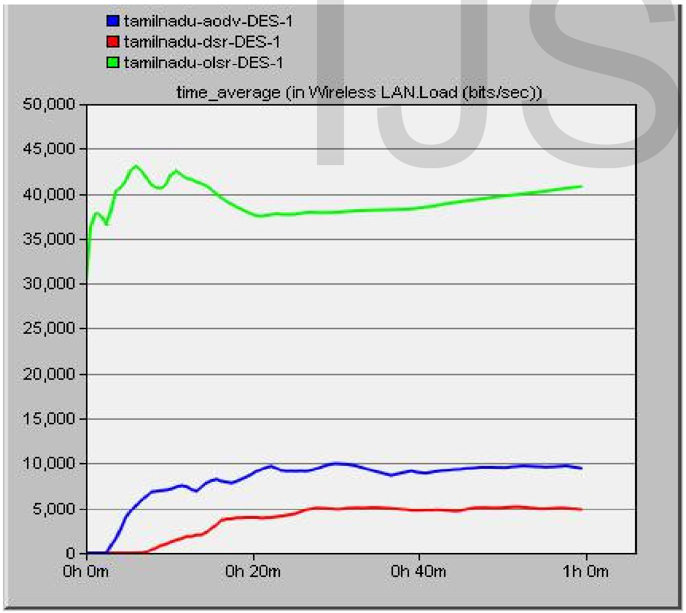

Fig 11 Simulation time v/s load (without node fail)

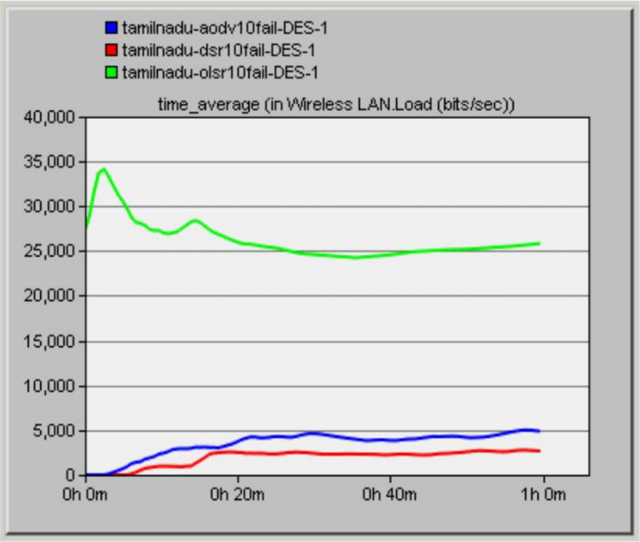

Fig 12 Simulation time v/s load (10 node fail)

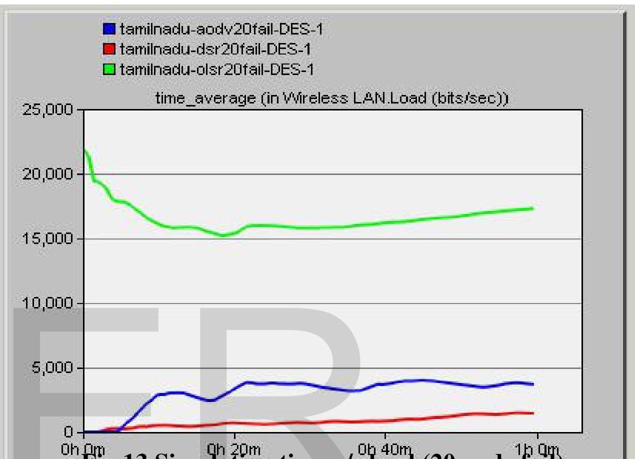

Fig 13 Simulation time v/s load (20 node fail)

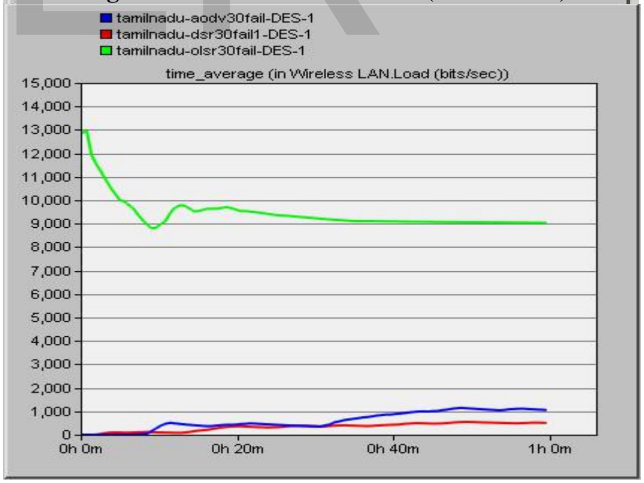

Fig 14 Simulation time v/s load (30 node fail)

5 CONCLUSION

The simulation study of this work has been performed for three different protocols AODV, DSR and OLSR deployed over MANET utilizing FTP traffic examining their behavior in terms of delay, throughput and network load. Objective of performing this simulation was to examine the performance of these three different routing protocols in MANET in usual operating situations as well as on the happening of node failure based on above specified parameters, as the choice of effective and reliable protocol is a serious issue. From the above analysis it is observed that OLSR performs best as compared to DSR and AODV protocols in terms of delay and throughput. While in terms of network load AODV and DSR are better. The throughput of OLSR is better in comparison of AODV and DSR in both usual operating conditions as well as in situations of node failure. This is due to the proactive nature of OLSR because of which it continuously attempts to discover paths to entire possible destinations in the network. Thus it has the benefit of having paths instantly available whenever they are needed and same scheme is followed in situation of node failure. This is the cause for its excellent performance. Whereas in case of AODV and DSR, they find paths whenever it is required due to their reactive nature. This causes undesirable delay in the network which in turn decrease the total network performance.

6 REFERENCES

[1] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[2] Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" , IEEE Transactions on Parallel and Distributed Systems, 2012

[3] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN:

[4] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on* , vol., no., pp.611,615, 8-10 Aug. 2012

[5] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," *Communications Surveys & Tutorials, IEEE* , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[6] Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," *Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1,4, 12-14 Oct. 2008.

[7] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan," *Vehicular Ad hoc Networks(VANET):Status, Results, Challenges*". Springer Science, Business Media.2010

[8] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan*Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.*

[9] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[10]Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011

[12] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal Processing (ICCSP), 2013 International Conference on* , vol., no., pp.1170,1174, 3-5 April 2013

[13] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013

[14] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," *ELEKTRO, 2014* , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," *Computing for Sustainable*