A Session based Secured Communication for inter-networking environment in VANETs

R.Jeevitha[1], Dr.N.Sudha Bhuvaneswari[2]

[1] Research Scholar, Department of Computer Science, Dr.G.R.Damodaran College of Science, India.

[2]Associate Professor, Department of Computer Science, Dr.G.R.Damodaran College of Science,,
(India)

ABSTRACT

Vehicular Ad-hoc Network (VANET) is the subset of Mobile Ad-hoc NETwork (MANET). For the past few years, VANET evolved into VANET based cloud. Since the wireless communication takes place between vehicle to vehicle (V2V), vehicle to roadside units (V2R), security places a major role in vehicular network application. This paper mainly focuses on session based secured communications in VANET cloud using AODV, DSR and DSDV routing protocol. The performance metrics like Throughput, Jitter and Delay are analyzed with the help of NS2.

Keywords— Cloud, MANET, VANET, V2V, V2R

I.INTRODUCTION

1.1. Vehicular Adhoc Networks

Due to the increase in large number of vehicles, congestion on road and accidents are the major issue. VANET paves way for reduction of congestion on road and accident avoidance. Most widely used wireless access technologies in Vehicular Adhoc Networks are Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE). The VANET architecture comprises of three categories namely Vehicle to Vehicle Communication (V2V), Vehicle to Infrastructure Communication (V2I), and Inter Roadside Communication (VRC). In V2V communication, the vehicles communicate with each other without any infrastructure units. The vehicles can communicate with the Road Side Units (RSU) that are within its transmission range in V2I Communication. Inter Roadside Communication (VRC) comprises of both vehicle to vehicle communication as well as one RSU will communicate with other RSU. VANET applications are classified into two categories namely Safety applications and User Applications. [5][11]

1.2. Cloud

Cloud Computing is the latest technology that is being used all over the world. The resources can be retrieved from Internet through web-based tools and applications. Users need not be available in a specific place to gain access to it. Employees can work remotely. Users can access their email in any computer system and store files using Google Drive also. Cloud comprises of three services: Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). Cloud security still remains a big challenge in research. [9]

The paper is organized as follows. Section 2 focuses on VANET cloud environment. Section 3 provides the related works and reviews of securing communications in VANET cloud. Section 4 focuses on proposed work about how communication is secured in VANET cloud. Section 5 and 6 discusses on Simulation scenario and its results. Finally, concludes the paper in section 7.

II.VANET CLOUD ENVIRONMENT

Recent research involves the impact of Cloud computing on Vehicular Adhoc Networks. To improve the traffic safety and to provide computational services to road users, a new cloud computing model called VANET-Cloud is proposed. VANET cloud challenges include security and privacy issues that includes data integrity, data access, data loss and protecting the confidential data of users. The data centers in the cloud consume large amount of energy. So, alternative servers like onboard computers in vehicles can be used. Vehicles spend limited life time in cloud network. There should be continuous, efficient and secured communication between the VANET vehicles (nodes) as VANET Cloud entities. Efficient routing protocol should be developed to overcome the above issue. [9]

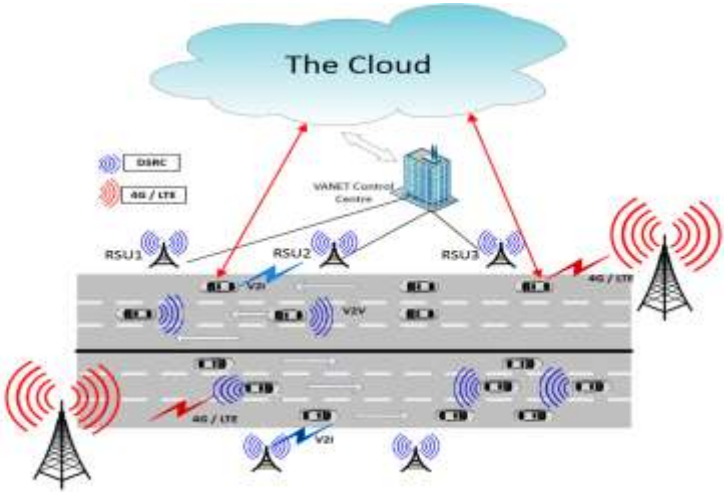

Fig. 1. Vehicular cloud environment [7]

Vehicles use DSRC radios to communicate with one vehicle to another vehicle and vehicle-to-infrastructure communication. The communication range of DSRC is between 300 and 1000 m. The connected vehicles would be able to share data through the cloud using 4G/LTE connectivity. The DSRC and 4G/LTE connectivity in vehicles can solve the bandwidth problem to give efficient, reliable, and secure information to the VANET users. [7]

III.RELATED WORKS

An efficient geographic location-based security mechanism for vehicular ad hoc networks is done by G. Yan and S. Olariu [4]. They proposed a concept in VANET named GeoEncrypt (Geolock). Secret key is generated using the geographic location of the vehicle. Messages are encrypted with the secret key, and the encrypted texts are sent to the receiving vehicles. The receiving vehicles can decrypt the message if it is present in a certain geographic region specified by the sender.

A secure and efficient Vehicle-to-Vehicle communication scheme using Bloom Filters is done by Su–Hyun Kim and Im-Yeong Lee [10]. According to them, Bloom filter is a data structure that can store large amount of data in a small space and it can search data quickly. Bloom filter reduces the overhead of group rekeying by an RSU in VANET if the number of vehicles present is high. Cloud is used as the medium of storage for the vehicles and RSU.

Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks is done by Rasheed Hussain and Heekuck Oh [8]. They suggested that the data generated from vehicles are considered to be big data with respect to the computing power of the individual vehicles. The data can be processed efficiently according to the desired results by using cloud resources.

IV.PROPOSED SCHEME

In this paper, we have selected throughput, end to end delay and jitter for 16 vehicles (nodes) in a session to check the performance of AODV, DSDV and DSR routing protocol. A session refers to interactive information exchange between the nodes. A session can be set up or it can be established at a certain point of time and later it can be torn down.

4.1. Routing Protocols

4.1.1. Ad-hoc On-Demand Distance Vector (AODV):

Reactive routing protocols discovers the routes only on demand. It builds the routes between nodes only as desired by source nodes. AODV builds the routes using a route request and route reply query cycle. Whenever the source nodes requires route to destination, it broadcasts Route Request packet (RREQ) across the network. The nodes that receive RREQ packet will update its information in source node by setting up backward pointers to the source node. The node that receives RREQ can send Route Reply (RREP) if it is the destination node or if it has the route to the destination node. Once the source nodes receives RREP, it starts forwarding packet to the destination node. When the source node stops sending the data packets, the links will time out. If a link break occurs when the route is active, a route error (RERR) message is sent to the source node to inform it of the now unreachable destination. After receiving the RERR by the source node and if it still desires the route, it can reinitiate route discovery. [3]

4.1.2. Dynamic Source Routing (DSR):

Dynamic source Routing depends on the strategy known as source routing. This protocol has two mechanisms namely Route Discovery and Route Maintenance. Route Discovery occurs when one node wants to send a packet to another node and the path is not really known. Route Maintenance occurs when the network topology has changed such that the route established after topological change results in an error. So the node can try a different route if it knows or route discovery occurs again. [3]

4.1.3. Destination Sequence Distance Vector (DSDV):

DSDV is a proactive routing protocol based on the Bellman-Ford routing algorithm. It provides solution for shortest path between two nodes and it is an enhancement of distance vector routing. DSDV solves Routing Loop problem. Sequence number is used for each routing table entry of entire network to avoid the formation of routing loops. It prevents nodes from saving battery power. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges. So, DSDV is not suitable for highly dynamic networks. [3]

4.2. Performance Metrics:

The metrics for routing protocols evaluation are as follows:

i) Throughput: Throughput is the total number of successful packets reached at the destination out of total transmitted packets. Throughput is calculated in data packets per second or bytes/sec.

ii) Jitter: Jitter is the mean deviation of the packets from source to destination for number of vehicles. Jitter is caused by delays and congestion in the network.

iii) End to End delay: Delay is the time taken for a packet to be transmitted across a network from source to destination.

V. SIMULATION SCENARIO

NS2 is open source which mainly used in wired and wireless researches. NS2 is developed as a collaborative environment and it is discrete event driven network simulator developed at UC Berkely written in C++ and OTcl. NS2 is useful for simulating local and wide area networks. [12]

Table 1.0 Simulation Parameters

Parameter	**Values**
Simulator	NS-2 (Version 2.34)
Channel	Wireless
Number of nodes	16
Routing protocols	DSR,AODV,DSDV
MAC layer	802.11
Mobility model	Random waypoint Model
Application Type	Constant Bit Rate (CBR)
Application packet size	512 bytes
Simulation Time	10 s

VI.RESULT AND ANALYSIS

OTCL script (.tcl file) has been created and the tcl Script (s1.tcl) is executed successfully using CYGWIN command shell. After the execution of tcl script, TRACE file (out.tr) and NAM file (out. nam) has been generated and the node movements are visualized using the Network Animator (NAM).

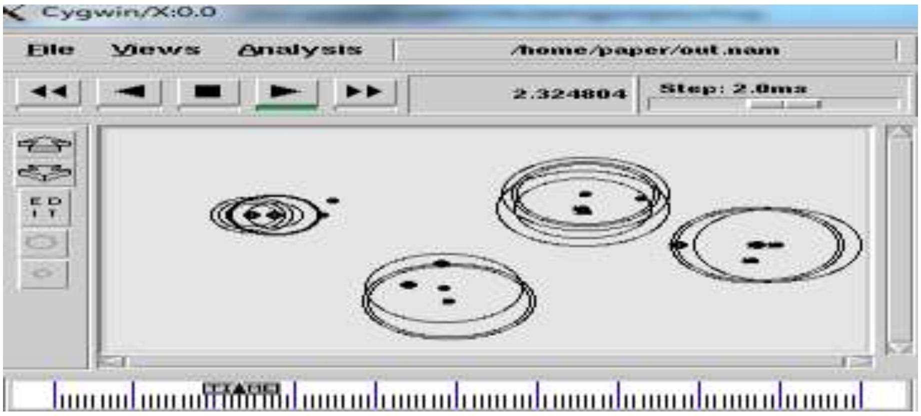

Fig. 2. A snapshot of the simulation scenario in NAM for 16 mobile nodes

The above figure shows the Simulation Scenario of the 16 nodes.

6.1. Throughput Analysis

When Throughput graph is plotted, time interval length option is used. To plot a Throughput graph, number of sent or received packets is calculated every time interval and divided by its length.'Throughput of sending' means throughput of sending or forwarding at current node.

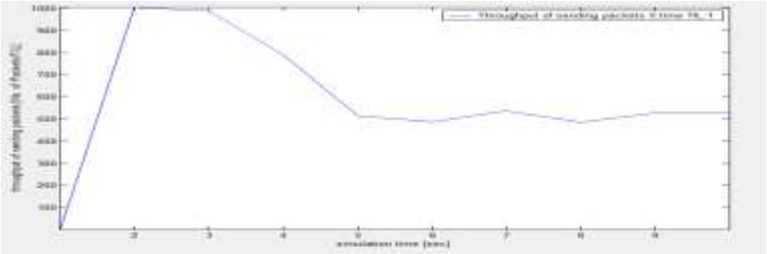

Fig. 3. AODV Throughput of sending packets

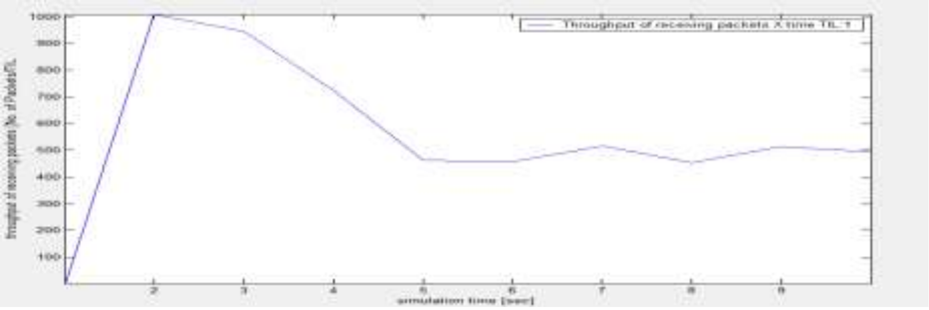

Fig. 4. AODV Throughput of receiving packets

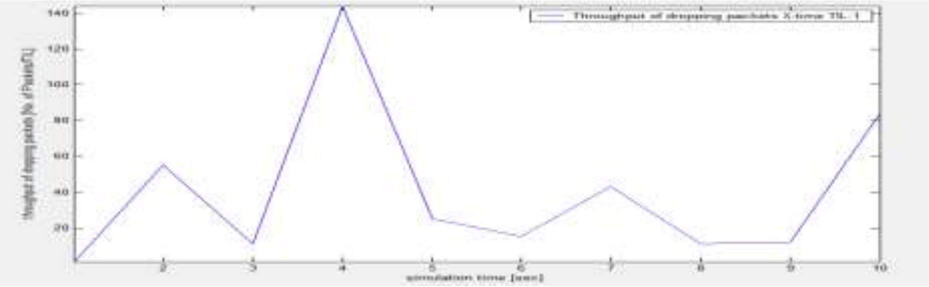

Fig. 5. AODV Throughput of dropping packets

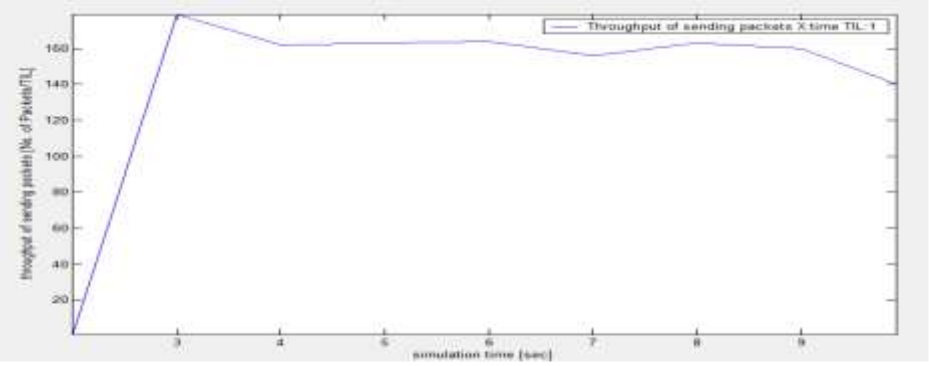

Fig. 6. DSR Throughput of sending packets

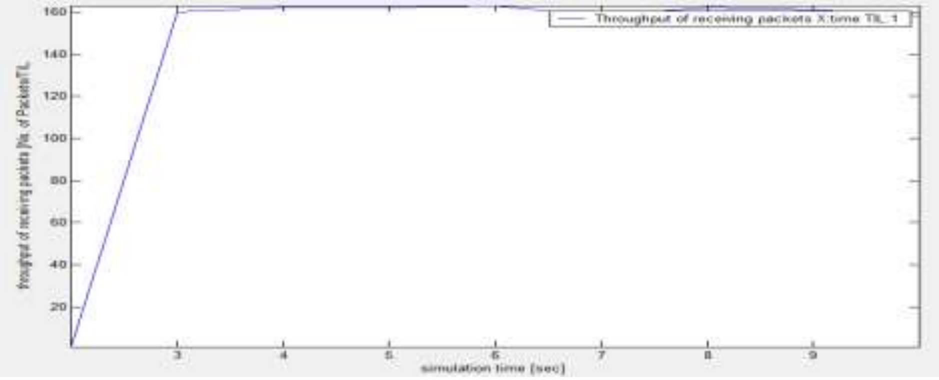

Fig. 7. DSR Throughput of receiving packets

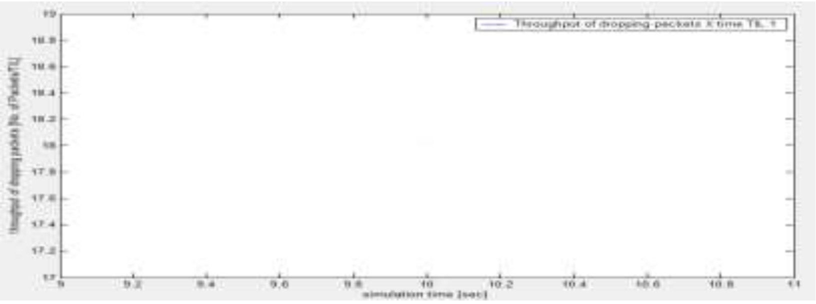

Fig. 8. DSR Throughput of dropping packets

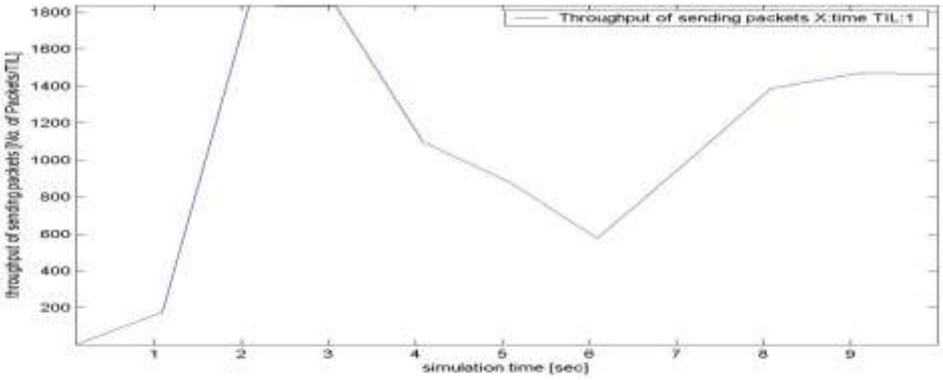

Fig. 9. DSDV Throughput of sending packets

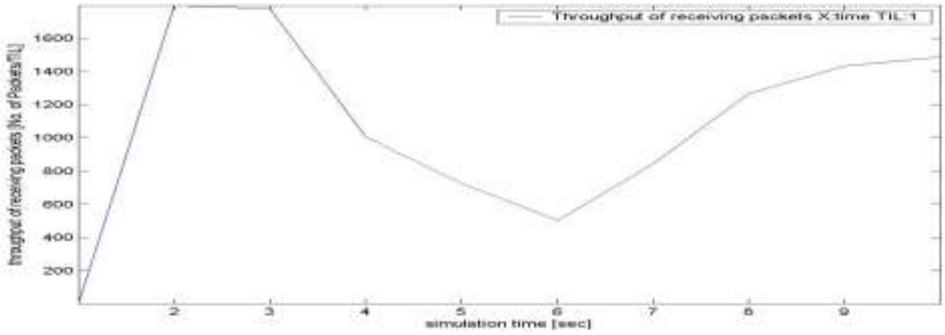

Fig. 10. DSDV Throughput of receiving packets

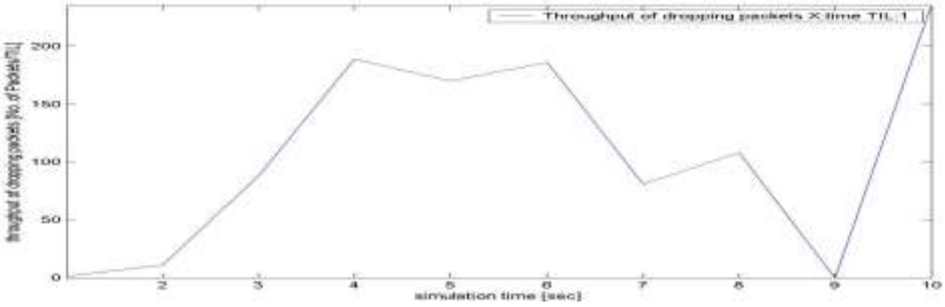

Fig. 11. DSDV Throughput of dropping packets

On observing the graphs from figure 3 to 11, we can observe that the dropping of packet is very less in DSR. So, the throughput of DSR network is constantly high during the simulation time compared to AODV and DSDV. AODV has high throughput next to DSR. In DSDV, the delay is caused in discovering the optimum route to the destination node

.

6.2. Jitter

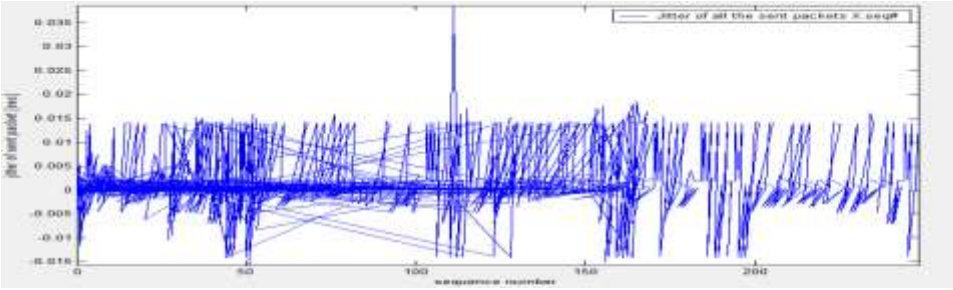

Fig. 12. AODV Jitter of all sent packets

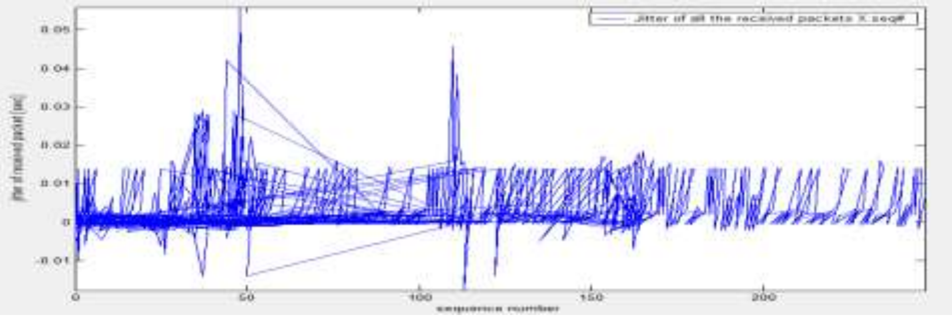

Fig. 13. AODV Jitter of all received packets

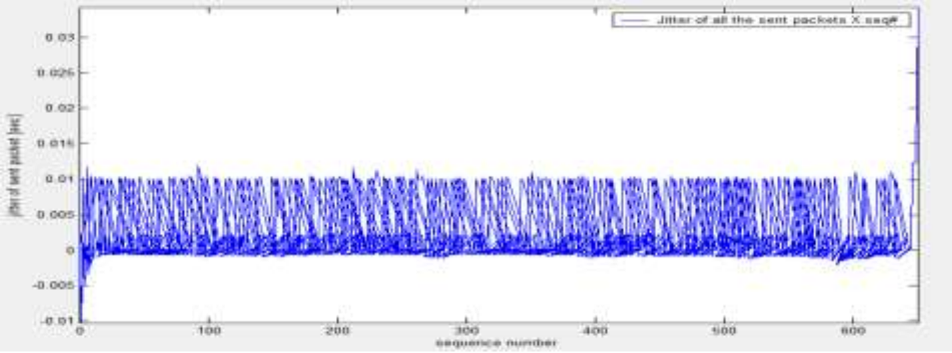

Fig. 14. DSR Jitter of all sent packets

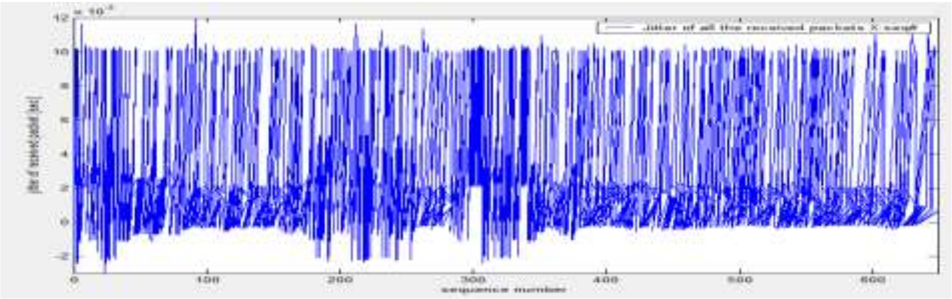

Fig. 15. DSR Jitter of all received packets

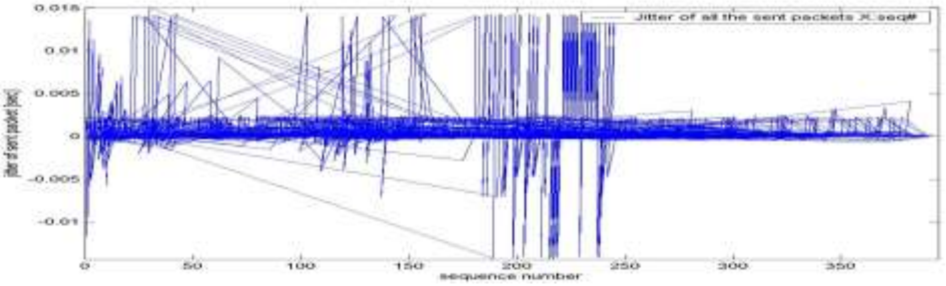

Fig. 16. DSDV Jitter of all sent packets

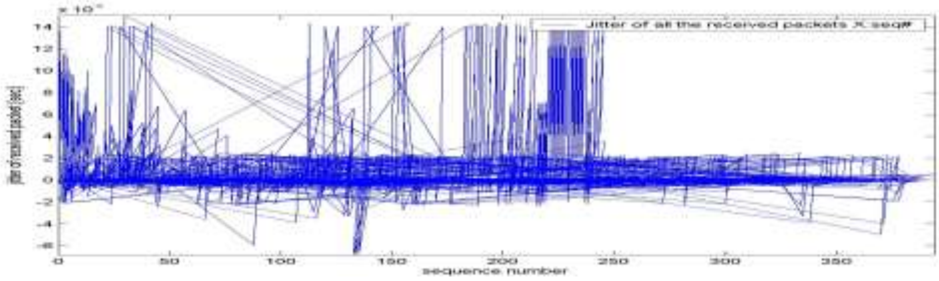

Fig. 17. DSDV Jitter of all received packets

Packets are sent in a continuous stream with the packets spaced evenly apart at the sending side. The delay between each packet vary due to network congestion, improper queuing, or configuration errors. Figures 12 to 17, depict the jitter of sent and received packets over the simulation time (sec) for AODV, DSR and DSDV. In DSR, the delay variation is much less and the overall jitter stabilizes faster in DSR. DSDV have highest delay variations in CBR traffic compared to AODV and DSR.

6.3. Average End To End Delay

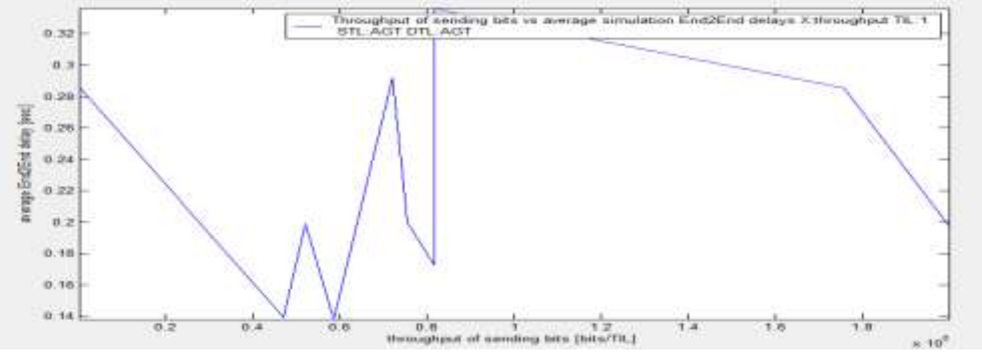

Fig. 18. AODV average end to end delay

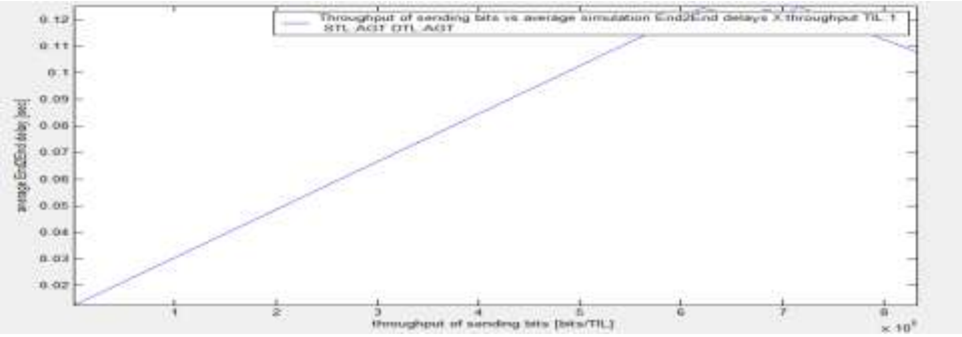

Fig. 19. DSR average end to end delay

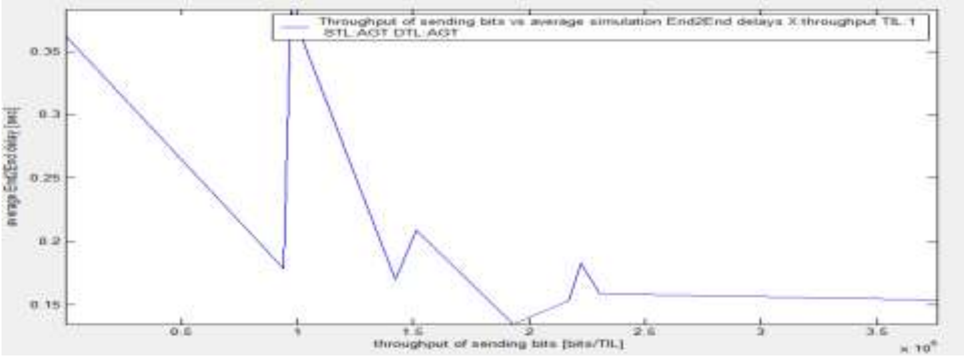

Fig. 20. DSDV average end to end delay

From figures 18 to 20, we can observe that average end to end delay in DSDV is better when compared to DSR and AODV. Next better routing protocol for average end to end delay is AODV in comparison with DSR.

VII. CONCLUSION

Though DSR routing protocol performs better in our simulation environment considering jitter and throughput, still it has some limitations like more delay in the network. In future, most of the vehicles have permanent Internet presence. Fog computing brings the cloud applications closer to the physical IoT devices at the network edge. Our future work would be to improve DSR routing algorithm so that these limitations can be removed and also testing the solution for more dense and populated network scenarios and to find the efficient routing protocol that works well in VANET cloud.

REFERENCES

[1] Bingyi Liu, Dongyao Jia, Jianping Wang, Kejie Lu, and Libing Wu “*Cloud-Assisted Safety Message Dissemination in VANET-Cellular Heterogeneous Wireless Network*”, IEEE Systems Journal, *Volume11, Issue 1*, 2017, pp. 128-139.

[2] Devhuti Vyas1,Gayatri s.pandi(jain), “*Reliable Service Provisioning In Vehicular Cloud Architecture*”, IJARIIE, *Volume 3, Issue 2*, 2017,pp.4839-4843

[3] Dilpreet Kaur, Naresh Kumar, —*Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks,‖* in International Journal of Computer Network and Information Security(IJCNIS)*, vol. 5, no.3*, pp.39, 2013.

[4] G. Yan and S. Olariu, "*An efficient geographic location-based security mechanism for vehicular ad hoc networks*," in Proc. IEEE Int. Symp. TSP, Macau SAR, China, Oct. 2009, pp. 804–809.

[5] Hari Krishna, Sandeep Kumar Arora, "*Review of Vehicular Ad Hoc Network Security*" , International Journal of Security and Its Applications *Vol. 11, No. 4*, 2017, pp.27-44

[6] Hatem M. Hamad, Alaaeddin B. AlQazzaz, "*Design a Cloud Security Model in VANET Communication: Design and Architecture*" ,International Journal of Computer Applications, *Volume 146 – No.3*, July 2016, pp. 38-48

[7] Kamran Zaidi, Muttukrishnan Rajarajan, "*Vehicular Internet: Security & Privacy Challenges and opportunities*", Future Internet ,*Volume 7, Issue 3*, 2015, pp.257-275

[8] Rasheed Hussain and Heekuck Oh, "*Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks*", Journal of Information Processing Systems,*Vol.10, No.1*, pp.103~118, March 2014

[9] Salim Bitam, Abdelhamid Mellouk, Sherali Zeadally, "*VANET-Cloud: A Generic Cloud computing model for Vehicular Ad hoc Networks*", IEEE Wireless Communications, 2015, pp. 96-102

[10] Su–Hyun Kim and Im-Yeong Lee," *A secure and efficient Vehicle-to-Vehicle communication scheme using Bloom Filter in VANETs*", International Journal of security and its Applications, Volume 8, Issue 2,2014,pp.9-24

[11] Vinita Jindal, Punam Bedi, "*Vehicular Ad-Hoc Networks: Introduction, Standards, Routing Protocols and Challenges*", IJCSI International Journal of Computer Science Issues, Volume 13, Issue 2, March 2016, pp.44-55

[12] http://www.isi.edu/nsnam/ns/