COOPERATIVE DATA SHARING WITH SECURITY IN VEHICULAR AD-HOC NETWORKS

Deepa B[1] and Dr. S A Kulkarni[2]

[1]IV Sem M. Tech, Dept of CSE, KLS Gogte Institute of Technology, Belagavi
deepa.bangarshetru@gmail.com
[2]Professor and HOD of ISE, KLS Gogte Institute of Technology, Belagavi
shri1_kulkarni@yahoo.com

ABSTRACT

Vehicles download the data when passing through a drive through the road (RSU) and then share the data after travelling outside the coverage of RSU.A key issue of downloading cooperative data is how effectively data is shared among them self. Developing an application layer data exchange protocol for the coordination of vehicles to exchange data according to their geographic locations. Coordinated sharing can avoid medium access control (MAC) layer collisions and the hidden terminal effect can be avoided in the multi-hop transmission. A salient feature of the application layer data exchange protocol, in the voluntary services, Vehicles purchase the requested data from service provider via RSUs. In this project, we propose a cooperative data sharing with secure framework for voluntary services in special vehicles networks (VANETs). We also concentrate on security in the process of downloading data and sharing. Applicants to ensure exclusive access to data applied and security of the vehicles involved in the implementation.

KEYWORDS

VANET, RSU, Security, Data Sharing & Voluntary Services.

1. INTRODUCTION

VANET- Vehicular networks is likely to develop in the upcoming years and thus become the most applicable form of ad hoc networks. Vehicular Ad hoc Network (VANET) consists of the imperative elements of Intelligent Transportation System (ITS) in which vehicles are arranged with several short-range and medium-range wireless communications. In VANET two kind's communication are possible. One is vehicle-to-vehicle (V-2-V) communication; the other is roadside-to-vehicle communications (V-2-R).By V-2-V communication, people can obtain more information and use the shared information to improve road safety. By V-2-R communication, people can communicate with RSU to access internet for downloading and updating files or inquire neighbourhood location information. Thus, compared with the traditional pure infrastructure-based network, the hybrid of V-2-V and V-2-R communications is promising since

David C. Wyld et al. (Eds) : ACITY, DPPR, VLSI, WiMNET, AIAA, CNDC - 2015
pp. 53–62, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.51305

it can not only overcome the disadvantages of infrastructure-based network, but can also overcome the disadvantage of non-infrastructure-based network.

In recent years, VANETs- vehicular ad hoc networks have gained much attention in the world of automobiles and Research. One reason is interest in an increasing number of applications designed for safety of passengers such as traffic jam detection and cooperative driving and also for emergency braking, As well as in applications for the comfort of passengers like games, chat-rooms and distribution of vehicle data (eg CarTorrent). The increased use of software has not only affected the automotive guarantee costs, but has also made most difficult to car repairs. Data downloading is a practical and prominent application in VANETs-vehicular ad hoc networks, which can bring comfort and entertainment to users. In data downloading, vehicles send service requests and then get the data stream from the current or the next roadside units (RSU). In the downloading application, the amount of data a vehicle can download at a drive-through of a RSU is very limited due to the short connection time. Cooperative download is a promising scheme in which vehicles download the data when passed through a RSU and then share data when traveling outside the scope of the communications of RSU. Thus, the total amount of data that can download a particular vehicle will increase.

A key issue in cooperative download is how vehicles share data with others. There are some existing studies on data exchange in VANETs [1]. However, existing exchange protocols are limited to issues of medium access control (MAC) layer of the collisions, limited applicability to multiple data exchange units, and there is no guarantee of receipt of complete data.

We propose an application layer protocol for data exchange with the assumption that each vehicle knows the positions of the own and neighboring vehicles (which can be obtained through global positioning system (GPS) and related security messages transmitted regularly by neighboring vehicles [2]). In the proposed protocol, vehicles used for coordination channel to coordinate relay transmissions in VANETs for data exchange based on GPS vehicle location. With such cooperative exchange, collisions and MAC layer hidden terminal effect can be avoided in the data channel. In addition, Design a stylish selection of relay vehicles mechanism for the space between the two RSU can be completely exploited for data exchange. A prominent feature of the proposal exchange protocol is that it can ensure the receipt of the data for each applicant vehicle pass an RSU. Security is also critical issue.

Characteristics of voluntary services require exclusive access to applicant's data.

In summary, develop a framework for cooperative secure data sharing with the following contributions.

1. Designed an application layer protocol for data exchange to facilitate data sharing with the coordinated transmission. With such coordinated sharing can avoid medium access control (MAC) layer collisions and the hidden terminal effect can be avoided in the multi-hop transmission.
2. Security protocol for voluntary services VANETs are developed, which can ensure applicants exclusive access to data applied and also ensures security of the vehicles involved in the implementation.

1.1 Features and challenge

To develop this system we come across some of the difficulties

- Vehicles are moving faster and therefore lifetimes of the communication links are shorter; therefore, the links are facing rapid changes in the network topology.
- Vehicles are high mobile and are usually constrained with layout of the road, speed limits, traffic and vehicle destination. If the vehicle is in exceeding the speed limit then it results in receiving an incomplete data. This requires the intelligent file transfer.
- The existing sharing protocols constrained with issues of medium access control (MAC) layer collisions, limited applicability to sharing multiple data units, and no guarantee of complete data receiving.

2. LITERATURE SURVEY

S. Ahmed and S. S. Kanhere in [1] proposed a co-operative content distribution scheme based on novel network coding called VANETCODE for Content distribution in Vehicular Ad-Hoc Networks (VANET) is challenging due to the high mobility, rapidly topology changing and intermittent connectivity observed in these type of networks. Using VANETCODE, leverages of the wireless medium of the broadcasting nature to accelerate the distribution of encoded blocks amongst neighboring one-hop neighbors and is completely independent of routing.

X. Lin et. al proposed a secure data downloading protocol with preserving privacy in VANETs - vehicular ad hoc networks [2]. Which Enables vehicles to download data from RSUs Securely With Their privacy protection under one or Even When multiple RSUs are compromised .This protocol give the guarantees for vehicles to exclusive access their requested data while eavesdroppers cannot obtain any private information of the vehicles.

K. Sampigethava et. al describe techniques used for privacy-preserving and secure protocol based on identity (ID)-based and group signature [3]. This protocol gives the guarantee the requirements of privacy and security of the each vehicle. But it can also give the each vehicle desired traceability in the event that the ID of the sender message must be revealed by the authority for any disputes of an event.

Y. Hao et. al give details of how the problem involved in controlling of unauthorized vehicle tracking based on their broadcast communications media, in order to improve user location privacy in VANET. [4] AMOEBA provides location privacy by utilizing the location group navigation of vehicles. By using vehicle groups for anonymous access to applications location-based services in VANET, for privacy protection of user. The robustness of privacy of the user provided is considered under various attacks.

J. Byers et. al describe fully scalable and ideal protocol for the applications such as reliable distribution of bulk data for that we call a digital fountain [5]. In this many number of heterogeneous receivers at times of their choice to procure content with maximum efficiency. Here, no feedback channels are required in order to ensure the reliable delivery, even when the face of high loss rates.

3. SYSTEM ARCHITECTURE

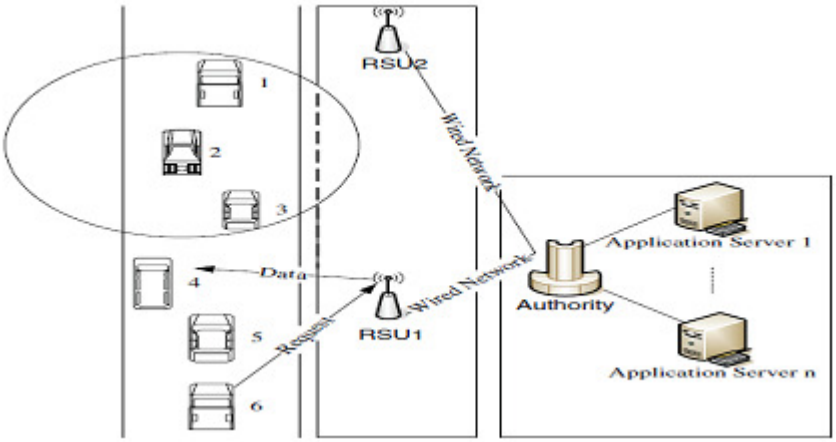

Figure 1: System Architecture

Applicant vehicle download the data from the application server via RSU. Initially applicant vehicle send request for data to RSU, then RSU will forward that request to authority. Authority is responsible for selection of downloading vehicle based on geographic information and also check the identity of the vehicle whether it is valid to purchase the data or not from application server. If vehicle is valid to purchase the data then it will download the data from the server and that will send to RSU. Finally RSU sends data to the Applicant vehicle.

The application authority and application servers: These are responsible for the management and provision of service data, respectively. The authority knows all the keys and is in charge of programming service. They can be kept either by the authority or third party operators.

Road side infrastructure: Consisting of RSUs deployed at the edges of the roads that are responsible for forwarding request and response. RSUs communicate with authority via wired network.

Nodes: These are ordinary vehicles on the street and highway road that can communicate with each other and RSUs through radio.

3.1 Vehicle Classification

Classifies the vehicle into three categories i.e Applicant Vehicle and Downloading Vehicle and Relay Vehicle.

Applicant Vehicle: These are the vehicle they are likely to purchase the data.
Downloading Vehicle: These vehicle download the data from the RSU for applicants. These are assigned by the authority according to geographic positions.
Relay Vehicle: These are responsible for forwarding data to buyers which are more than one hop away from downloading vehicles

4. ANALYSIS AND RESULTS

The experiment was conducted for 50, 55, 60, so on number of sent packets. The comparison between ADOV & ADOV_DES is made. In figure 6 we show the transmission of message to the v which is conducted in NS-2 and also shows the transmitted packets to vehicles from RSU (Road Side Unit). The RSU broadcasts the message any vehicle in the range will receive the message. The message transmission to the nearest vehicle, Without providing security and with providing security is shown in the following figures.

Title:-Run simrun.tcl for 50 packets, Without providing security (AODV) total number of sent packets will be 50 and number of received packets will be 49 and with delay was 13.0747. Consider 73 as applicant vehicle receives data from application server via RSU (67) are shown in the figure 2 and figure 3.

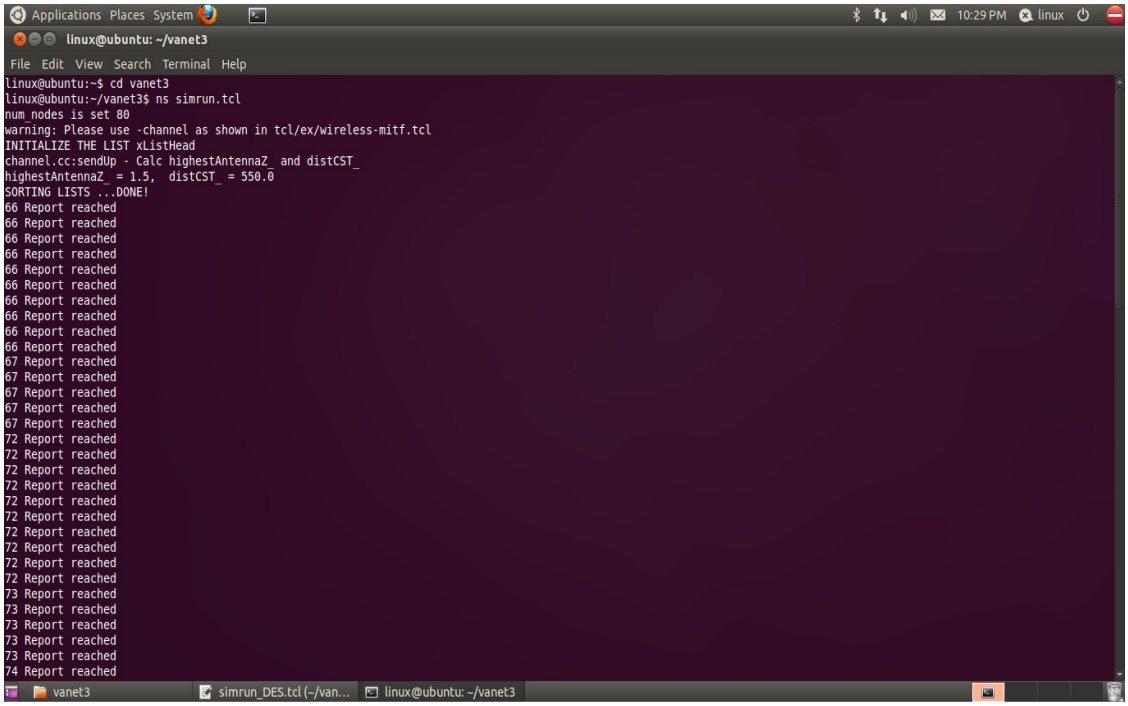

Figure 2: Run simrun.tcl for 50 packets

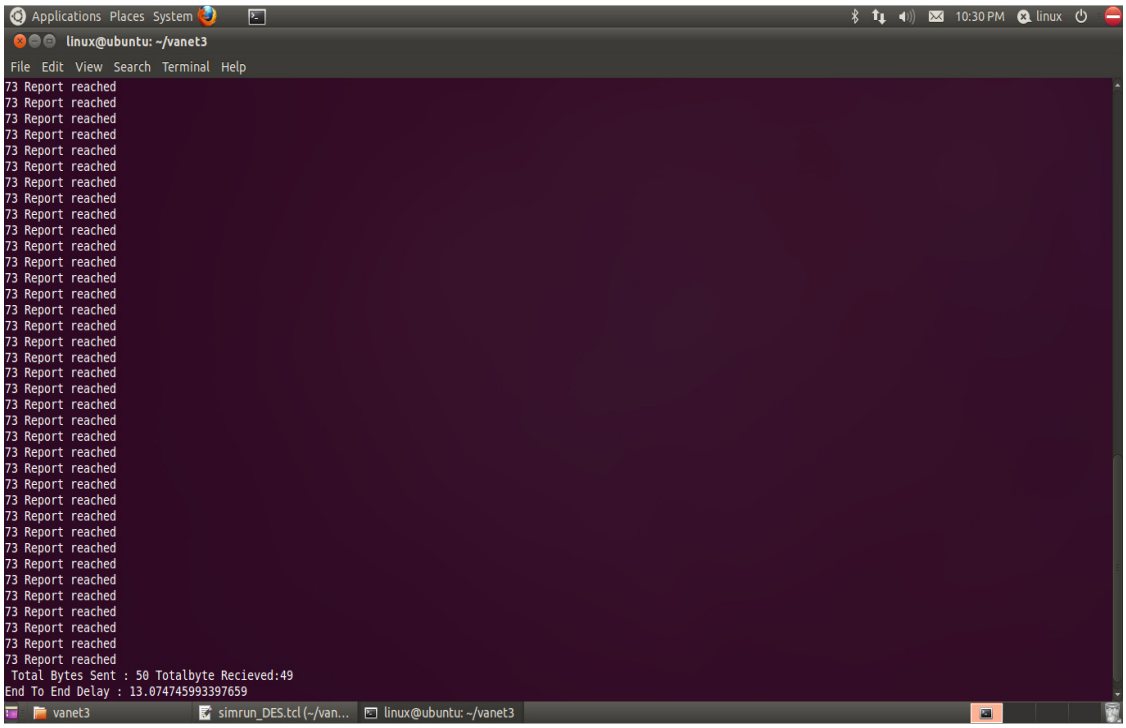

Figure 3: Run simrun.tcl for 50 packets

Title:-NAM Window with all the nodes before starting. Create road mapping using 65 nodes. Randomly use 72-75 nodes are applicants. Applicants are the vehicles to purchase the data from application server via RSU's.Application server1 located at position (400,610) sends data to Authority located at position (450,630).

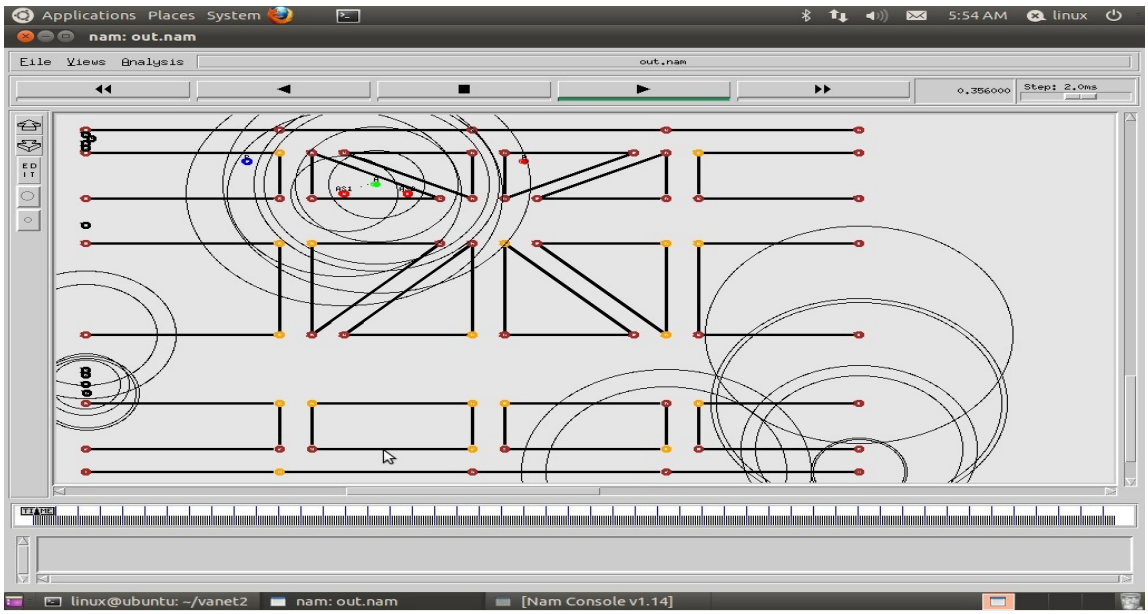

Figure 4: Application Server1 sends data to authority

Title:-Authority located at (450,630) sends data to RSU (67) located at (250,680).

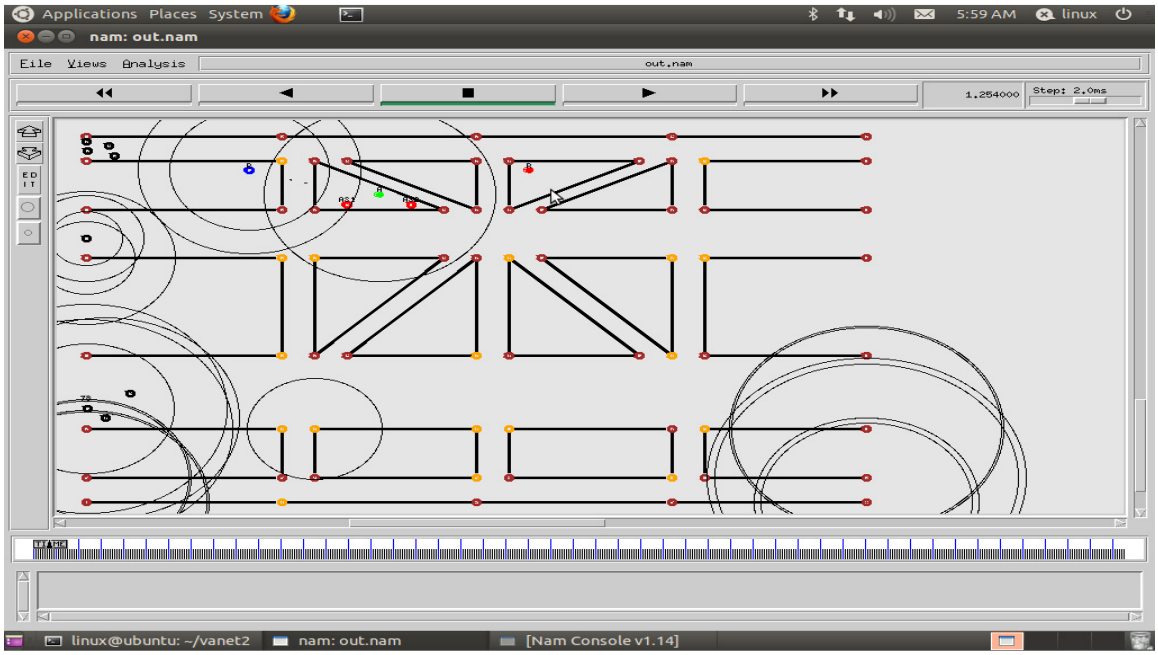

Figure 5: Authority sends data to RSU

Title:- RSU (67) located at (250,680) sends data to applicant vehicle (73) without providing security.

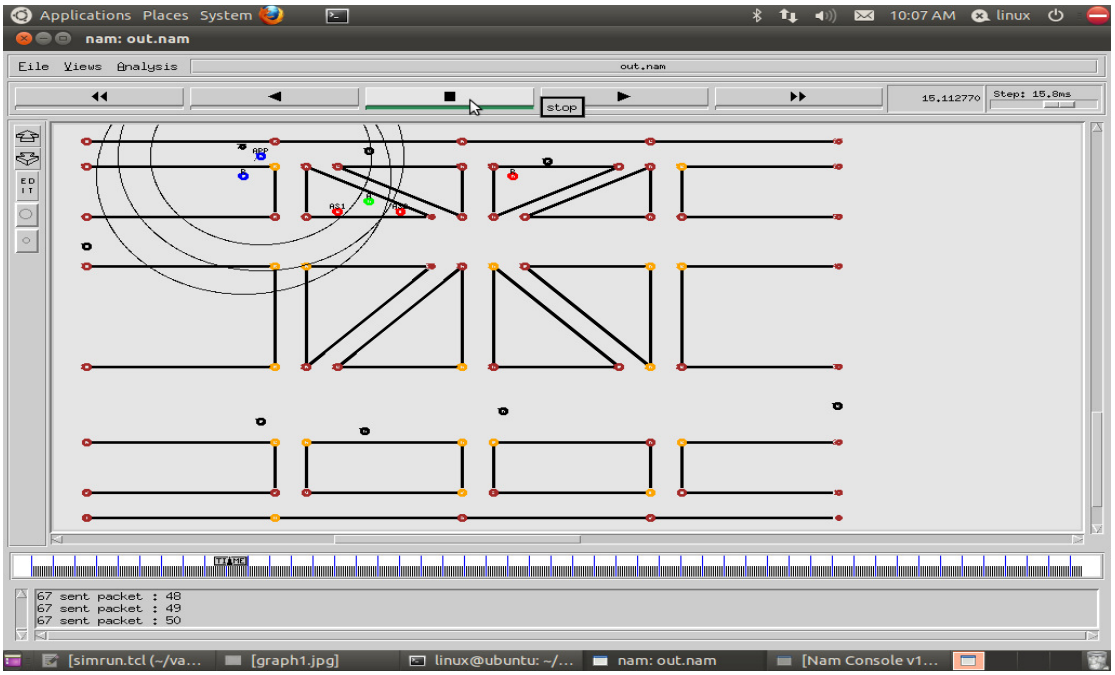

Figure 6: RSU sends data to applicant vehicle

Title:-Run simrun_DES.tcl for 50 packets, With providing security (AODV_DES) total number of sent packets will be 50 and number of received packets will be 49 and with delay was 14.047. Consider 75 as Applicant vehicle receives data from application server via RSU's after receiving data, the data will be decrypted and also cross verifies the signature, if signature is matched than message is accepted else message will be rejected are shown in the figure 7 to figure 9.

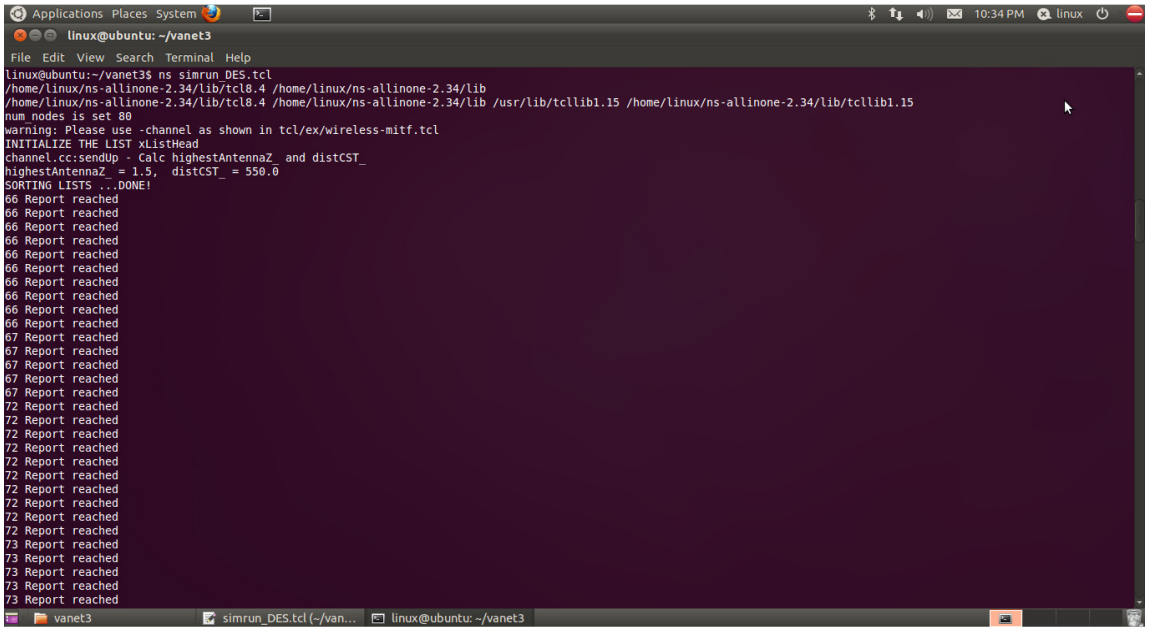

Figure 7: Run simrun_DES.tcl for 50 packets

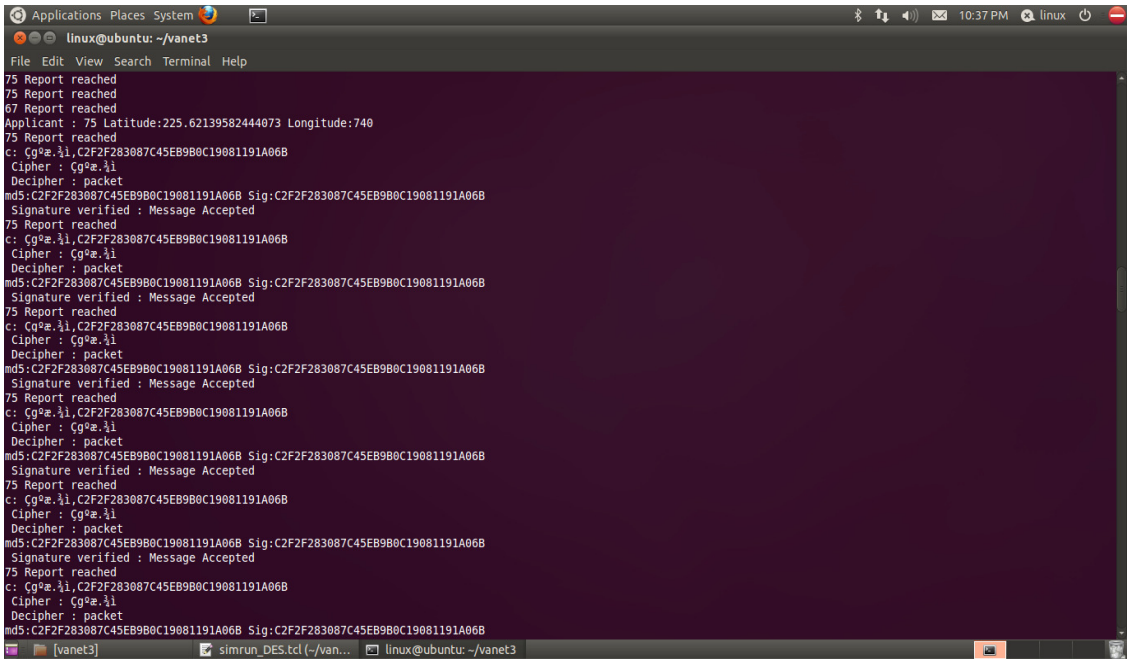

Figure 8: Run simrun_DES.tcl for 50 packets

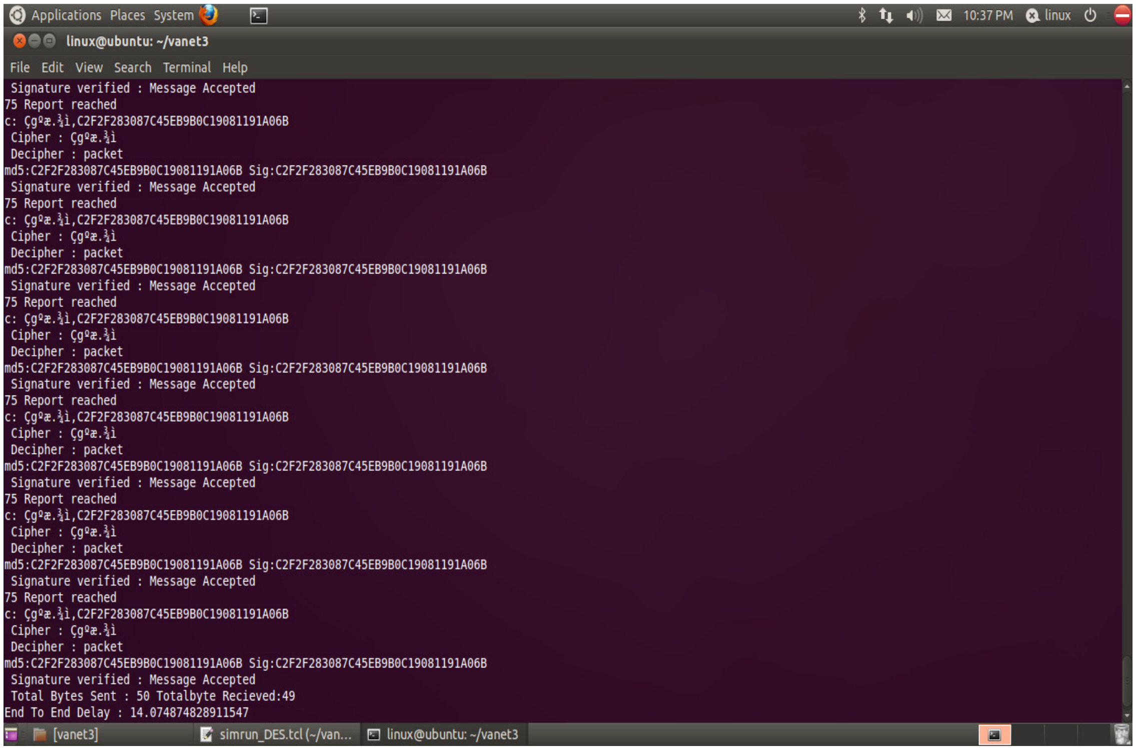

Figure 9: Run simrun_DES.tcl for 50 packets

Title:- RSU (67) located at (250,680) sends the packets to applicant vehicle (75) with providing security.

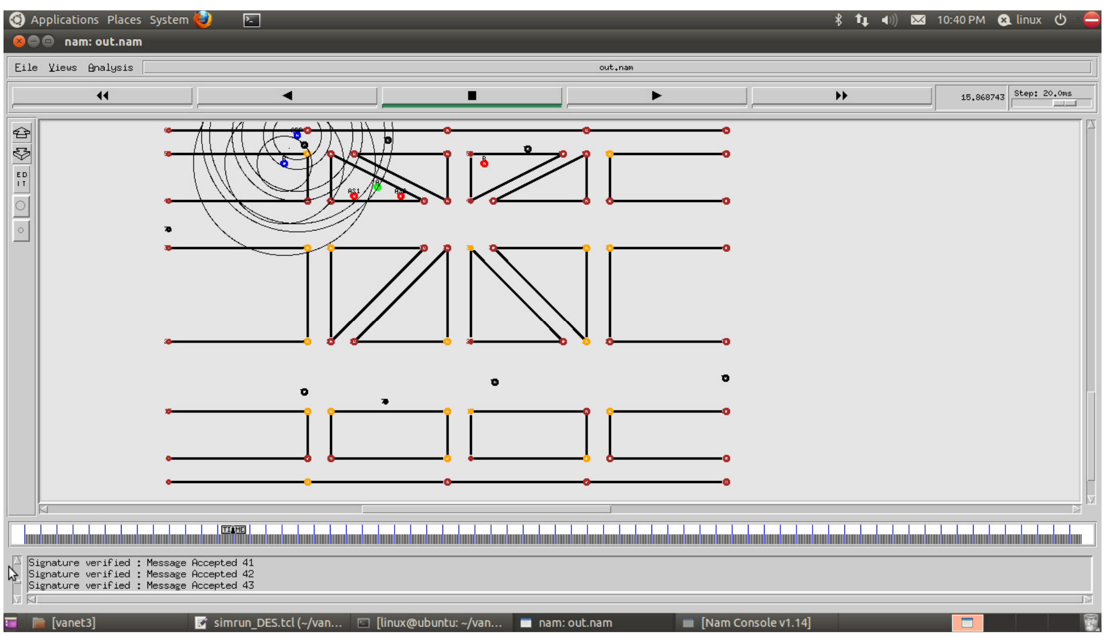

Figure 10: RSU sends packets to applicant vehicle

In Figure 11 consider three samples, sample1: Describes total number of sent packets is 50 and received 49 and dropped is 1. And sample2: Describes total number of sent packets is 55 and received 54 and dropped is 1.And sample3: Describes total number of sent packets is 60 and received 59 and dropped is 1.By observing the below chart we conclude that; the complete data with 1 dropped packet is received.

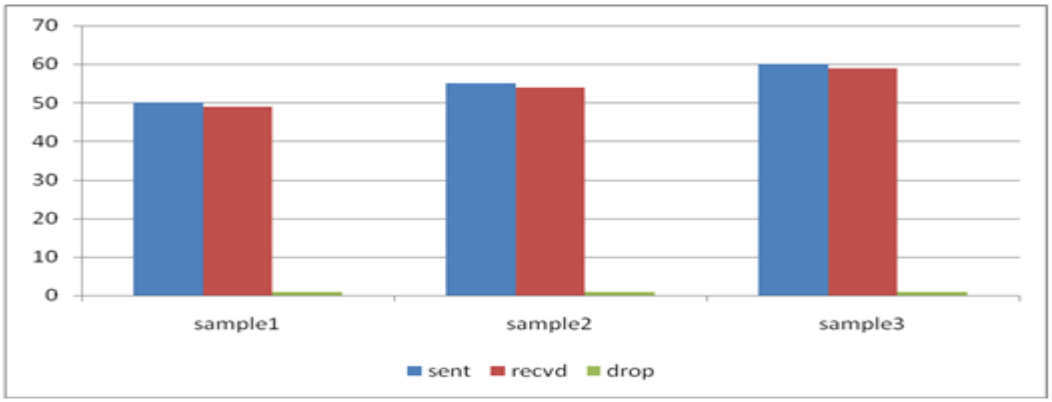

Figure 11: The comparison of delay of packets

5. CONCLUSION

Based on the above experiments & results conducted, we infer that; the transmission with DES & MD5 algorithm is secured & efficient. With such coordinated sharing can avoid medium access control (MAC) layer collisions and the hidden terminal effect can be avoided in the multi-hop transmission and also provides security protocol for voluntary services VANETs, which can ensure security and improve the efficiency of developed framework.

In future we want to share the messages using different techniques while with security as main concern & in real time transmission.

REFERENCES

[1] S. Ahmed and S. S. Kanhere, "VANETCODE: Network coding to enhance cooperative downloading in vehicular ad hoc networks," in Proc. IWCMC, 2006.

[2] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, 2007.

[3] K. Sampigethava, M. Li, L. Huang, and R. Poovendran, "AMOEBA:Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, 2007.

[4] Y. Hao, J. Tang, Y. Cheng, and C. Zhou, "Secure data downloading with privacy preservation in vehicular ad hoc networks," in Proc. IEEE ICC, May 2010.

[5] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A digital fountain approach to reliable distribution of bulk data," in Proc. ACM SIGCOMM,1998, pp. 56–678.

[6] F. Ye, S. Roy, and H. Wang, "Efficient data dissemination in vehicular ad hoc networks," IEEE J. Sel. Areas Commun., vol. 30, no. 4, pp. 769–779, May 2012.

[7] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu. "Secure incentives for commercial ad dissemination in vehicular networks," in Proc. ACM MobiHoc, 2007.