Secure Communication and Privacy Protection Using VANET

Janani. A[1], Anbin Soji. E[2],Dheepak. G[3]
[1]Assistant Professor, Dept Of ECE, Dr. M G R Educational And Research Institute, Chennai
[2]Assistant Professor, Dept. Of ECE, Narasu's Sarathy Insitute Of Technology, Salem, India
[3]Associate Professor, Dept. Of ECE, Narasu's Sarathy Insitute Of Technology, Salem, India
Corresponding Author: Janani. A

Abstract: All drivers have an awareness of finding route to the particular destination within a short period. In present scenario, thiscanbeachieved by using Global positioning system (GPS). It determines the current location and alsohelps in finding the route between the source and the destination. At present the drivers comes to know about the traffic and alsoweather conditions in the form of FM radio data system whichtransmits the information collectedfrom Traffic Message Channel. In recentdays, Vehicular ad hoc Network (VANET) isbecoming more popular in many places. VANET is an important element of Intelligent Transportation Source (ITS). VANET is a network whichallows the vehicles to broadcast the safety messages to nearbyvehicles. For using VANET in vehicles, On-Board unit shouldbeplaced in the vehicle and Road Side Unit (RSU) along the highways. The main source of communication between RSU and OBU isdedicated short range communication (DSRC) protocol. This communication isdone over the wirelesschannel. In thispaper, we propose the real time conditions gathered by the VANET to instruct the drivers to reach the destination in particular time. To prevent hacking and tracing, the source isgiven by the confidentialcredential to provideprivacy of the drivers whichisunlinkableeven by the trustedauthority. Herewe use AODV protocol to improve the efficiency of vehicle to vehicle communication.

Keywords: Intelligent Transportation System, Privacy preservation, Real- time conditions

Date of Submission: 20-07-2018 Date of acceptance: 04-08-2018

I. INTRODUCTION

The rapid advancement of wireless communications and information technologies are revolutionizing many aspects of the day to day lifestyle. A brief introduction on the networks that are commonly available is presented here. Generally communication network are classified into wired and wireless networks. The wireless networks are in turn classified into infrastructure and infrastructure less networks. The networks in which the nodes are connected to a common base station are said to be infrastructure network while the network in which the nodes can transmit within the link coverage are called infrastructure less network. Wireless Ad-hoc network is a computer network in which the communication links are wireless. Here the nodes organize themselves into a network, route among themselves, and do the address assignments etc.., it is a infrastructure less network. The network is Ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. The Ad-hoc networks are classified into 1) Mobile Ad-hoc networks (MANET), 2) Vehicular Ad-Hoc networks (VANET), 3) Underwater Sensor networks (USN). In this paper we have considered a basic VANET architecture and enhance it to support a intelligent transportation system. An application area which is expected to benefit greatly from this advancement in communication networks is vehicle safety and navigation. Travelling in this high speed era has become a difficult task that must be done every day in this busy life. To achieve this task people tend to opt the most efficient way that reduces the travelling time. In country like India where there is a heavy density population, traffic is the major consequence that is faced by each one of us. So there is a need of network that can allow the people to reach the destination at a reduced travelling time and increased security. In recent scenario we use GPS to find route for a specific destination and to discover the roadways even for an undiscovered destination. In high peek traffic scenarios FM radio is useful to know about the real time conditions of the roads in case of accidents and heavy density vehicles. If there is an emergency situation such as an ambulance or a fire engine is on the road with heavy traffic, it takes a lot of time to reach the destinations which may end in vain. For such scenarios, we need an efficient system that can guide the vehicle directly by providing the real time conditions prevailing on the road.

In our proposed system VANETs, onboard units (OBUs) frequently broadcast routine traffic-related messages with information about position, current time, direction, speed, acceleration/deceleration, traffic events, etc. By frequently broadcasting and receiving traffic-related messages, drivers can get a better awareness of their driving environment. They can take early action to respond to an abnormal situation to avoid any possible damage or to follow a better route by circumventing a traffic bottleneck.

1.1. Intelligent Transportation System

The term intelligent transportation system (ITS) refers to the efforts to add information and communications technology to transport infrastructure and vehicles, in order to improve safety and reduce vehicle wear, transportation times, and fuel consumption. It is used for many applications such as traffic and transit management, traffic signal systems, Global positioning systems, Weather information systems, Commercial vehicle electronic clearance, Real-Time Traveler Information like navigation information, bus-stop information, air- line information etc.., It is considered because of the increase in population, congestions in road and due to the decrease in land and funds for new roads. It can be simply quoted as ITS = Telecommunication + Infomatics.

1.2. VANET architecture

VANET is a network that is introduced to guide people in an efficient travelling path way. It is considered as one of the most important technologies in ITS (intelligent traffic system). It is a type of MANET, which a next- generation is networking technology that provides communication between vehicles or between a vehicle and an RSU (Road Side Unit) using wireless communication. It is a promising network scenario for facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. By being equipped with communication devices, vehicles can communicate with each other as well as with the roadside units (RSUs) located at critical points of the road, such as intersections or construction sites. VANETs are usually divided into V2V (Vehicle-to-Vehicle) communication or V2I (Vehicle-to-Infrastructure) communication. V2V communication can be established by the vehicle forming its own network and can provide information without assistance from the infrastructure.

It is generally used to provide safety services including emergency information as well as anti-collision messages and alerts. The nodes inside a VANET network communicate using a Dedicated Short Range Communications (DSRC). According to the Dedicated Short-Range Communication (DSRC) protocol, a vehicle sends each message within a time interval of 100–300 ms. Generating a signature every 100 ms is not an issue for any current signature technique. However, in a high-density traffic scenario, e.g., if 50–200 vehicles are within the communication range, the receiver needs to verify around 500–2000 messages/s, which will lead to a high computation burden to the receivers.

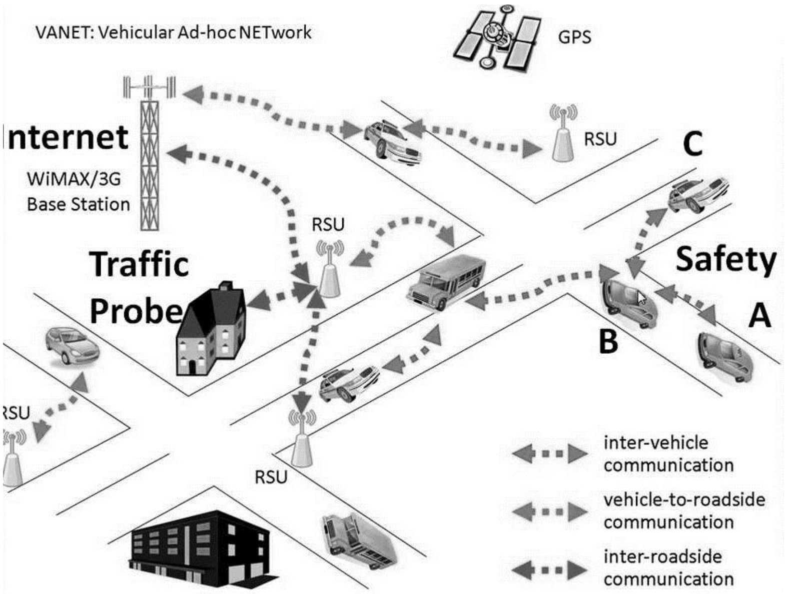
VANET: Vehicular Ad-hoc NETwork
GPS
nternet
WiMAX/3G
Base Station
RSU
RSU
C
Traffic
Probe
Safety
A
B
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig: 1.2.1 Vehicular Ad-hoc network

There are many challenges that need to be addressed since when creating vehicular ad hoc networks the topology of the network changes rapidly. Vehicles in a VANET have a high degree of mobility.

1.3. VANET communication:

VANET communication is classified into 3 types 1) V2V- vehicle to vehicle communication, 2) Vehicle to Infrastructure communication, 3) Vehicle to Roadside communication. These communications can be mixed to form a hybrid communication model such as V2V+V2I and V2V + V2R. The vehicle to vehicle communication is most suited for short range vehicular networks. It is a fast and reliable communication which doesn't need any road side infrastructure. Here it is the receiver's responsibility to decide the relevance of emergency messages and decide on appropriate actions. Location based broadcast and multicast are the proper communication methods for collision avoidance in V2V Communication. Without any roadside infrastructure, multihop forwarding must be enabled to propagate the messages or signals. Hence, V2V communication is not very useful in case of sparsely connected or low density vehicular networks.

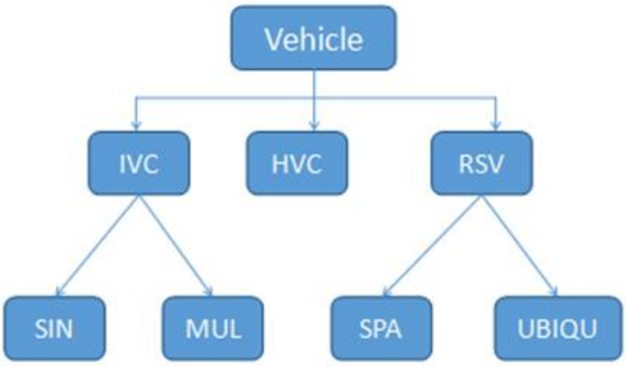

Fig 1.3.1: VANET communication

To overcome this problem, a hybrid model where a V2I and V2R infrastructure is introduced. Vehicle to Infrastructure provides solution to longer-range vehicular networks. It makes use of preexisting network infrastructure such as wireless access points (Road-Side Units, RSUs). The communication between vehicles and RSUs are supported by Vehicle-to-Infrastructure (V2I) protocol and Vehicle-to-Roadside (V2R) protocol. Here the Roadside infrastructure involves additional installation costs.

1.4. VANET protocols

The main goal for routing protocol is to provide optimal paths between network nodes via minimum overhead. Many routing protocols have been developed for VANETs environment, which can be classified in many ways, according to different aspects; such as: protocols characteristics, techniques used, routing information, quality of services, network structures, routing algorithms, and so on. VANET protocols [1] can be classified in different ways. Based on the routing characteristics it is classified as shown in fig 1.4.1.

Proactive protocols allow a network node to use the routing table to store routes information for all other nodes. This scheme may cause more overhead especially in the high mobility network.

In VANET, FSR (Fisheye State Routing) [2] which is a proactive type of routing protocol is used. It is an efficient link state routing that maintains a topology map at each node and propagates link state updates with only immediate neighbours and not to the entire network. The imprecision in routing gets corrected as packets approach progressively closer to the destination due to the reduction in broadcast overhead.Reactive routing protocols [1] (also called on-demand) reduce the network overhead; by maintaining routes only when needed. Reactive routing protocols are applicable to the large size of the mobile ad hoc networks which are highly mobility and frequent topology changes.In DSR (Dynamic Source Routing), [2] the IDs of the intermediate nodes that it has traversed are copied in the query packet. It is used for low mobility network.

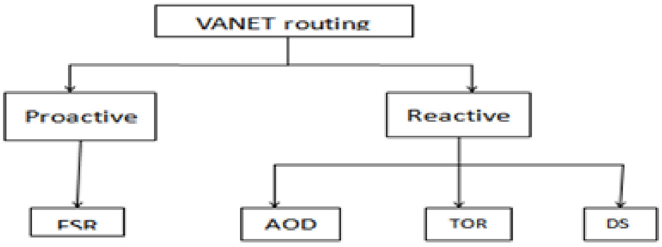

Fig 1.4.1 VANET Routing Protocols.

Temporally Ordered Routing Algorithm (TORA) belongs to a family of link reversal routing algorithms where the height of the tree rooted at the source is used to build a directed acyclic graph (DAG) toward the destination which directs the flow of packets and ensures their reachability to all the nodes. It is difficult to maintain this routing protocol especially in dynamic VANETs. Hence we use AODV (Ad-Hoc on Demand Distance Vector) routing protocol for an easy and efficient communication.

II. SURVEY

The route finding process is generally done by using GPS, a well known system that is being implemented in automobiles nowadays. It is a space-based radio navigation system GPS and was originally developed as a military force enhancement system. Later on it is extended for the civil community. There are two segments in GPS system. 1) Space segment and 2) Control segment. The space segment normally consists of 24 satellites that monitor the earth surface. It works in any weather conditions, anywhere in the world, 24 hours a day. The real-time idea by using VANET is not completely new. But we have taken it as an idea for our work [3]. There are many differences between theirs and ours. First, they have used verification scheme that verifies many messages, while ours involves the pseudo identities. Second, they have used Bloom filter for the implementation which can search data quickly and stores large amount of data in a small space. In our scheme, we have proposed Ad-hoc On-demand Distance Vector protocol (AODV) that is of reactive type of protocol and also it is a multicast network. Thus, this project cannot be applied if the vehicle is out of the RSU. This problem is solved in our project by placing OBU in the vehicle can also communicate with the vehicle far from RSU. Besides, the application of pre-defined map database is used for reaching the destination [4]. Their scheme is based on the packet forwarding protocol called STAP, while ours is based on the credential authentication. Then, they cannot have vehicle to vehicle communication, while ours include the communication with the RSU and also vehicle to vehicle communication. This idea of using the credential had been used for many applications. [5] Used this credential authentication for the secure and privacy communication. Samara et al [5] given the detailed explanation about the securities and the challenges in the VANET. The solution for [5] is given by Sampigethaya [6] called AMOEBA based on the vehicle group navigation. Different security systems have been proposed by [7], [8] and [9] used in the VANET. [7] The batch verification scheme known as IBV was used for RSU for verifying the large number of the signatures using the pairing operation. In [8], an RSU and inter vehicle communication was proposed. This is based on the signature verification.

A group communication between the known vehicles can verify the signature without the help of RSU was proposed in [10]. A common group secret key is developed for secure communication among the group members. Recently in 2011, related works was developed in [11]. In [11], the scheme was developed for protecting driver's privacy called Identity-Based Encryption (IBE). Another paper [12] with recent research and comparison between VANET and MANET showed how feasible is VANET when compared to the MANET. The main difference between them is that in VANET the nodes are moving on predefined maps.

III. PROPOSED SYSTEM

This section presents Secure Communication and Privacy-Protection using VANET. The problem in existing involves many. First, finding the route to the destination is not efficient. This problem involves the delay in reaching the destination.

In existing has only the predefined map database and it doesn't have any idea about real-time conditions. So, it takes much time to reach destination. The vehicle to vehicle communication is limited to only short range with the help of DSRC protocol. This can communicate only with the vehicle near to it within the RSU range. Beyond the RSU unit range it is not possible for it to communicate. In our paper we use, AODV protocol which can communicate with the vehicle which is not within the range of RSU. The communication between the Driver and the destination is also made secure.

In our proposed system we are intimating the drivers about the real time conditions prevailing on the road such as traffic, road conditions, and accident prone region etc.., which will be helpful for the drivers on board to reduce the travelling time and also reduce the congestion it has the advantage of finding a better route and also the information source can be properly authenticated. Here we propose a privacy preservation scheme that provides a number of security features. Besides satisfying all security and privacy requirements, our solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time.

3.1. Privacy preservation

The system consists of a trusted authority (TA), which sets up parameters and privacy credentials to the vehicles and the information secured from the road side units. TA acts like a central server or hub node of the network. When the vehicle starts the journey it sends a request to the nearby road side units that are directly connected to a trusted authority to initiate a communication link. On receiving the request the trusted authority creates a pseudo identity to the vehicle which will make the communication of the vehicle with the network as anonymous that increases the privacy of the individual navigation. Once the identity is created the communication of the specified vehicle with the road side units or with other vehicle cannot be known by any other nodes. The vehicle sends a request to the road side unit about the destination and asks for the better route to reach it. The RSU forwards the query message to the destination RSU through the intermediate RSUs. Once the query reaches the destination the RSU at destination will reply back in the reverse path. This process continues till the vehicle reaches the destination.

3.2. Real time conditions

The real time conditionsare monitored by the RSUs. Road conditions may vary abruptly. If a road which is initially in a good condition is blocked abruptly then the vehicle is informed by a road blocking information. The RSU near the blocked road that is connected to the destination creates the ROAD-BLOCKED message and sends it via the reverse path to the vehicle.Once the vehicle receives the ROAD-BLOCKED message it initiate a new navigation query message to seek for an alternate route. This process continues till the vehicle reaches the destination.

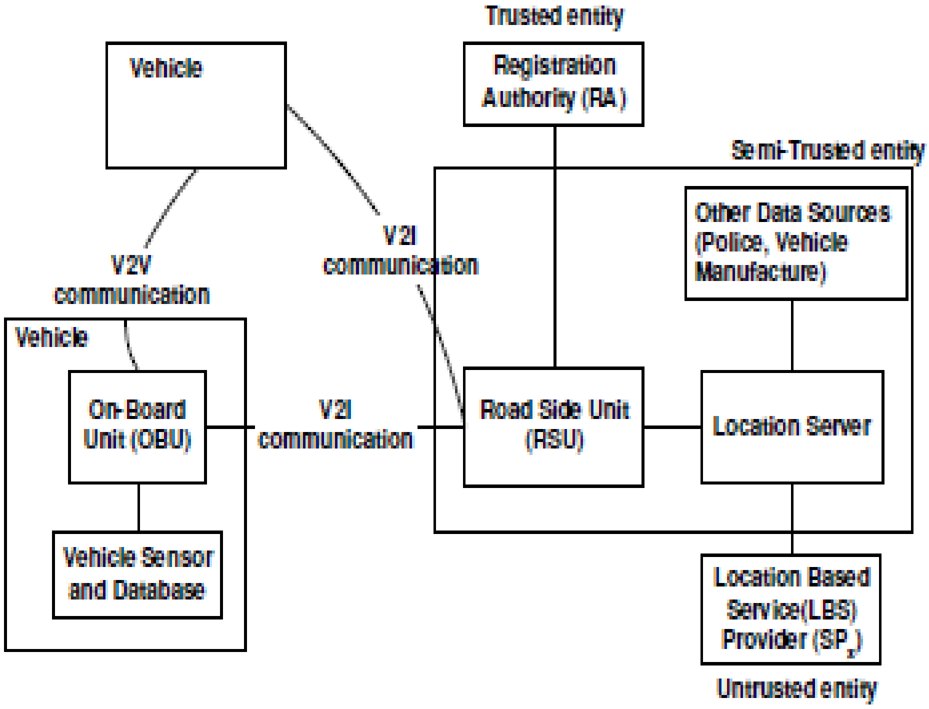

Fig 3.2.1. Network of Privacy scheme

3.4. Communication

Here we use AODV (Ad-Hoc on Demand Distance Vector) routing protocol for an easy and efficient communication in the network. AODV is a reactive type of routing protocol. In a DV every node knows its neighbors and the costs to reach them. AODV is an ‘on demand routing protocol’ with small delay. That means the routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. For unicast routing three control messages are used: RREQ (Route Request), RREP (Route Reply), RERR (Route Error).

If a node receives a RREQ which it does not have seen before it sets up a reverse route to the sender. If it does not know a route to the destination it rebroadcasts the updated RREQ especially incrementing the hop count. If it knows a route to the destination it creates a RREP. In mobile network link breakage is very common. If a node realizes that other nodes are not any longer reachable it broadcasts a RERR containing a list of the unreachable nodes with their IP addresses and sequence number and some flags. A node who receives a RERR iterates over the list of unreachable destinations checking if a next hop in its routing table contains one of these nodes. If yes it updates its routing table. If the receiving node still maintains routes to unreachable nodes it broadcasts its own RERR containing this information [13].

One of the great advantages of AODV is its integrated multicast routing. In a multicast routing table the IP address and the sequence number of the group are stored. Also the leaders IP address and the hop count to him are stored as well as the next hop in the multicasting tree and the lifetime of it. To join a multicast group a node has to send an RREQ to the group address with the join flag set. Any node in the multicast tree which receives the RREQ can answer with a RREP.

IV. SIMULATION

In this section, we evaluate our privacy preservation scheme in terms of processing delay and the reduction in travelling time using a network simulation program. Through simulation, we show that the processing delay caused by our cryptographic functions is minimal, while the savings in traveling time after using our scheme is significant. Here we have created a VANET network with RSUs and OBUs. We have assumed a traffic prone area and have monitored the action of a VANET based vehicle moving in that area. We have observed the packet delivery ratio of the VANET communication between the vehicles and the travelling time reduction when this privacy preservation scheme is used.

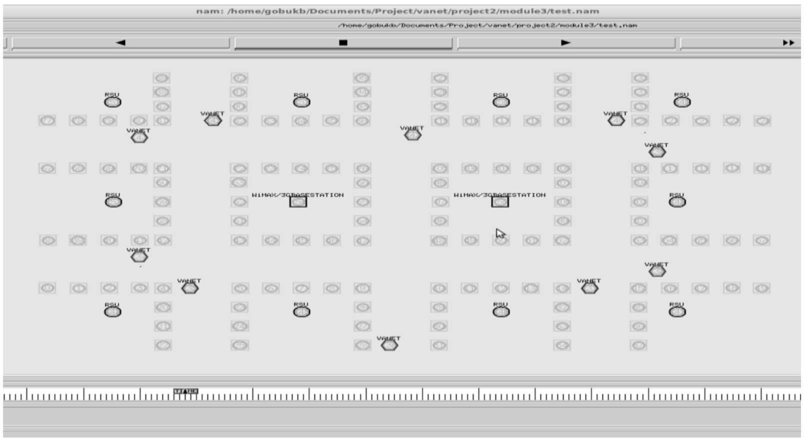
nam: /home/gobukb/Documents/Project/vanet/project2/module3/test.nam
/home/gobukb/Documents/Project/vanet/project2/module3/test.nam
RSU
VANET
WIMAX/3G BASESTATION

Fig: 4.1. Vehicular network

Fig.4.1 shows the vehicular network that is created for simulation purpose. The system consists of hexagon shaped nodes that represents the vehicles on the road. In Fig 4.2.a traffic scenario is shown,

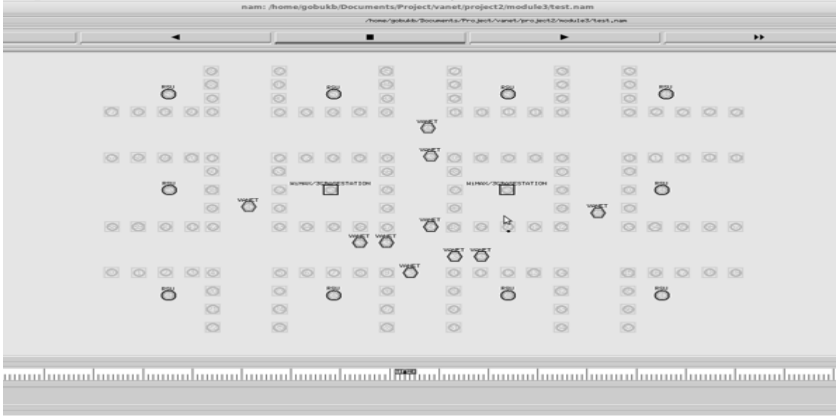
nam: /home/gobukb/Documents/Project/vanet/project2/module3/test.nam
/home/gobukb/Documents/Project/vanet/project2/module3/test.nam
RSU
VANET
WIMAX/3G BASESTATION

Fig: 4.2. Traffic diversion

while this situation occurs the other nodes in VANET will divert to alternate route by starting a new query with the Trusted Entity while the nodes in traffic communicate with each other and with the help of RSU and trusted unit, they reach their respective destinations.

V. RESULTS

Thus it has been shown that by using privacy preservation scheme we can find a better route that reduces the travelling time which also increases the communication speed between the vehicles. Through this system the privacy of a vehicle is maintained since it uses unknown credentials. Fig.4.3 shows the reduction in delay time of VANET communication when using AODV protocol. Fig.4.4. depicts the packet delivery ratio of the VANET communication and Fig.4.5.shows the improved throughput of the system on using privacy preservation scheme.

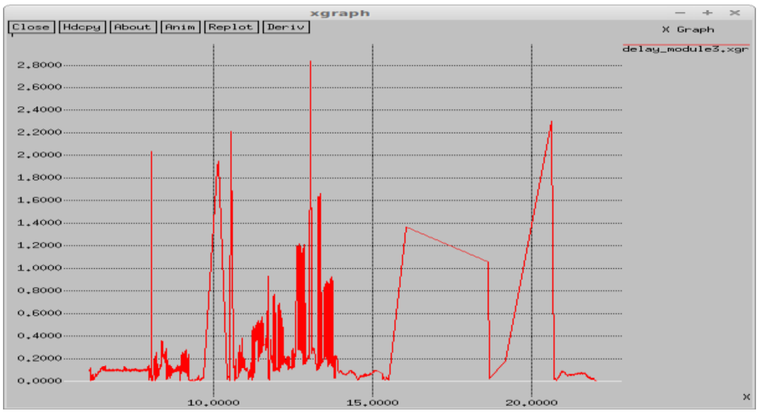

Fig: 4.3 Delay time in system

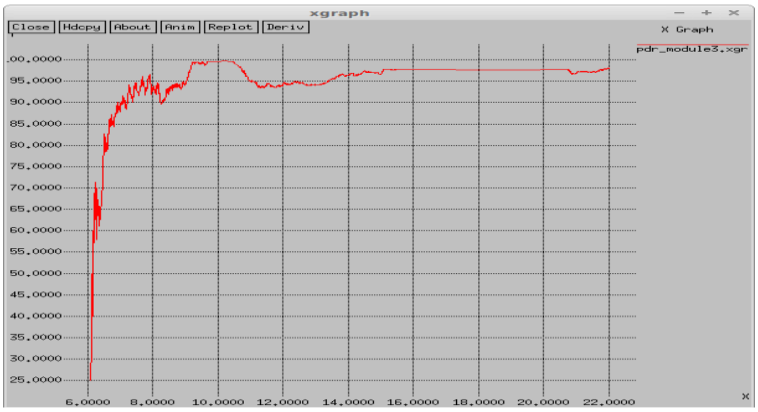

Fig: 4.4. Packet delivery ratio in V2V+V2I communication

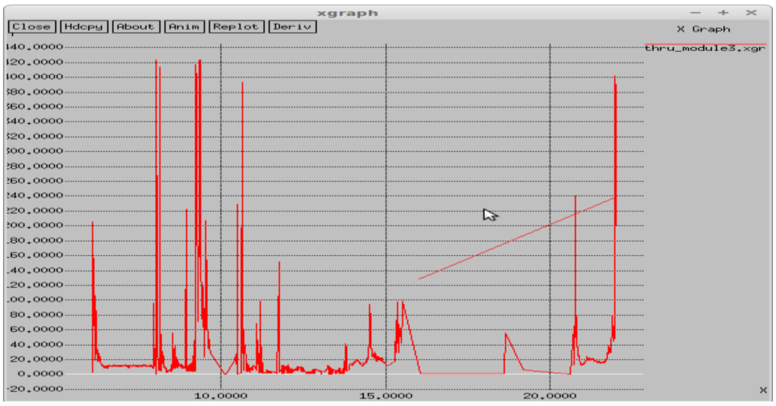

Fig: 4.5.Throughput of the system

Note that our Privacy Preservation scheme can apply to the situation where the route searching process is done by a central server (Trusted authority), which collects and verifies speed data and road conditions from RSUs. The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. However, such a centralized approach is not scalable, especially for large cities. In future, systems that overcome this problem can be designed.

REFERENCES

[1]. MarwaAltayeb and ImadMahgoub, 'A Survey of Vehicular Ad hoc Networks Routing Protocols', International Journal of Innovation and Applied Studies, ISSN 2028-9324 Vol. 3 No. 3, pp. 829-846, July 2013.

[2]. PrabhakarRanjan , Kamal Kant Ahirwar, 'Comparative Study of VANET and MANET Routing Protocols',Proc. of the International Conference on Advanced Computing and Communication Technologies (ACCT 2011) , ISBN: 978-981-08-7932-7.

[3]. 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 Vol.8, No.2 (2014), pp.9-24 http://dx.doi.org/10.14257/ijsia.2014.8.2.02

[4]. X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in VANETs," Proc. IEEE INFOCOM '11, pp. 2147-2155, Apr. 2011

[5]. E. Aimeur, H. Hage, and F.S.M. Onana, "Anonymous Credentials for Privacy-Preserving E-learning," Proc. IEEE MCETECH Conf. e-Technologies (MCETECH '08), pp. 70-80, July 2008.

[6]. K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[7]. C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.

[8]. C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSU- Aided Message Authentication Scheme in Vehicular Communica- tion Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451-1457, May 2008.

[9]. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, May 2008.

[10]. T. Chim, S. Yiu, L.C. Hui, and V.O. Li, "SPECS: Secure and Privacy Enhancing Communications for VANET," Elsevier Ad Hoc Net- works, vol. 9, no. 2, pp. 189-203, Mar. 2010.

[11]. R. Hwang, Y. Hsiao, and Y. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659, Dec. 2011.

[12]. B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf. Wireless Comm. Sensor Networks (WCSN '09), pp. 131-136, Dec. 2008.

[13]. Mario Cagalj LCA, EPFL Prof. Jean-Pierre, Hubaux LCA, EPFL, 'Performance Evaluation of AODV Routing Protocol: Real-Life Measurements'

Janani. A1" Secure Communication and Privacy Protection Using VANET." IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 8, 2018, pp. 25-32.