VANET Data Transmission Delivery

Syed Muzamil Nazir
Department of Computer Science & Engineering
School of Engineering & Technology, Sharda University Knowledge Park-III, Greater Noida, INDIA

Dr. Ravi Rastogi
Department of Computer Science & Engineering
School of Engineering & Technology, Sharda University Knowledge Park-III, Greater Noida, INDIA

Abstract— VANET is defined as Vehicular Ad hoc Network in which cars acts as a wireless moving router which helps to pass routes between various sources to destination in a different network. Since in vehicular network it is to be noted that the cars moving with higher speed has to send data in a reliable way of transmission so it's necessary to held the network in a strong security which means during the content delivery of traffic between the cars its essential that we need to track record of the end to end delay, packet through put and packet delivery fraction. These three parameters will be concluded through APLM model by which performance between two nodes will be examined. TESLA (Timed Efficient Stream Loss-tolerant Authentication) is another broadcast authentication protocol which can help to secure the broadcast communication by source authentication. TESLA is based on loose time synchronization between the sender side and the receiver side. Since MAC uses symmetric cryptographic function while as TESLA also uses symmetric functions for authentication. The basic concept of TESLA is that a MAC is being attached to the sender with a key k and only sender is aware about the key. After that receiver keeps the packet from the sender without being able to authenticate it. And after sometime the sender exposes k and receiver is able to authenticate the packet. A MAC per packet is sufficient for the broadcast authentication unless there is clock synchronization between the sender and the receiver. TESLA is used in various applications like in wireless sensor networks, and ad hoc routing protocols for the authentication. So in brief TESLA requires loosely time synchronization with the sender and it also needs an efficient mechanism to authenticate the keys at the receiver side for broadcast authentication.

Index Terms—VANET, MANET, AODV, SECURITY, APLM

I. INTRODUCTION

VANET may be defined as a vehicular ad hoc network in which cars acts as a node which transmits data from source to destination in a different network. Data or information is related to the current status of the moving vehicles. Since VANET is wide area network so it's necessary to held network in a strong security so that the data transmission will be accurate. In order to create communication between vehicles it's required that nodes should maintain distance of 300 meters for the reliable data transmission. Every car has got OBU (on board unit) which helps to collect all the process information received by the other sensors of the vehicle. So in other terms every vehicle in the VANET environment is known to be called as OBUs which are in a mobile position. There are also road side units (RSUs) which are stationary units found on the roads within every 1 km in order to connect back bone networks. The main aim of the RSUs is to connect vehicles to the other vehicles which are situated on the other network or area. Every vehicle has got its own unique identity (ID) which gives us identity of the vehicle in a vehicular environment. VANET is considered as a subset of MANET (mobile ad hoc network). The difference between the two is that in VANET the cars are fast moving with higher speed than MANET. In VANET there is multi hop communication between the various nodes that means the communication occurs between the various nodes in a network. Vehicles are restricted by the road layouts, huge number of vehicles and traffic rules. The vehicles in a vehicular network are also affected by the external conditions like weather, cities, and highways. VANET is been described as a vehicular ad hoc network because there is no central entity which maintains the communication between the cars so it is also known as infrastructure less network. In VANET it is essential to track down the path and mobility pattern to the reason of security purposes. Every VANET device has a large number of storage capacities which holds the information and it also includes the processing units which helps the data to transmit from one vehicle to the other vehicle in a network. There is also an internal battery fitted inside the car which helps the long range of communication in the VANET. Every VANET possess some topology which changes dynamically due to the speed of the vehicles. Each VANET vehicle tries to move in clusters in order to form a group of network for the easiness of the VANET network. In a VANET network it is necessary to have up to date information of each vehicle and other networks which are inside the VANET network. The information related to the vehicle could be the current position, protocol exchange information. Global positioning system (GPS) plays an vital role for giving

and sharing the current position of the vehicle This may lead to the fast communication and reliable way of data exchanging in the shared VANET topology

A.INTER VEHICLE COMMUNICATION

Inter vehicular communication deals with the communication between the vehicles where the propagation of message occurs between the two vehicles in to VANET network. Thus in the inter vehicular communication the information and data exchange only occurs between the vehicles it is also known as peer to peer communication. Inter vehicular communication is a type of the multi hop and multicast communication in which the messages is being sent to the other vehicles in the VANET environment.

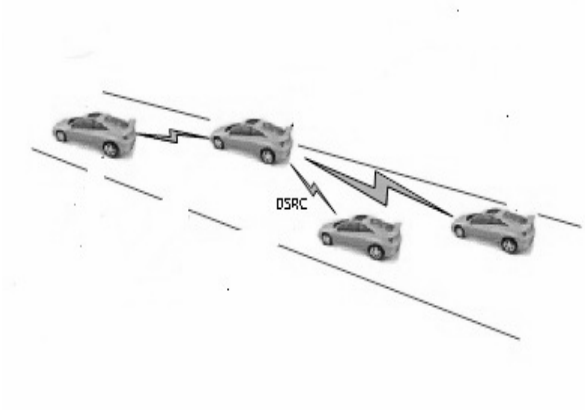

Fig. 1. InterVehicle Communication.

B.VEHICLE TO ROAD SIDE COMMUNICATION

Vehicle to road side communication is considered to be single hop communication and roadside units sends broadcast messages to all the vehicles which are in the vicinity. Road side units are placed within kilometres or less than that in order to provide and remain connected with the vehicle and to other roadside units. The main feature of road side units is that they send higher bandwidth broadcast messages to the vehicles for the future communication. The main aim of road side units is that they send messages with some speed to the vehicles and if vehicle is trying to move fast then a warn message will appear to that vehicle and speed is to be controlled by the driver. The message that the driver receives is in form of visuals and accordingly controls the speed of the car

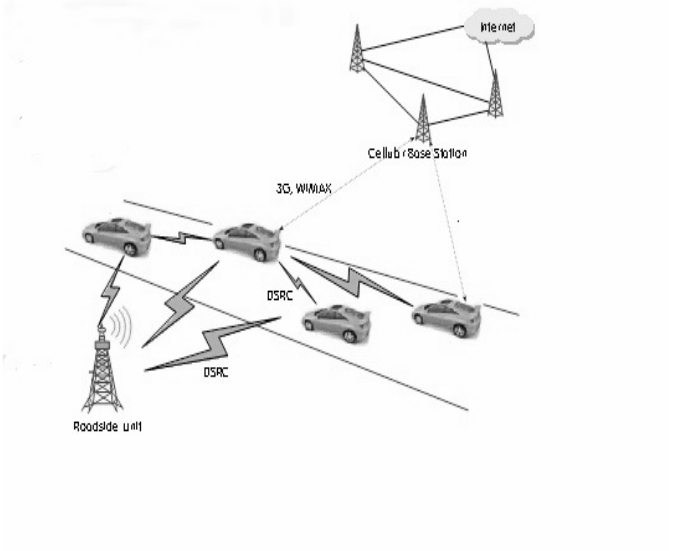

Fig.2. Vehicle to Road Side Communication.

C.ROUTING BASED COMMUNICATION

Routing based communication deals with the type of communication which is in the form of multi hop unicast. In this form of communication the routes is being propagated between vehicles to vehicles or vehicle to road side units.

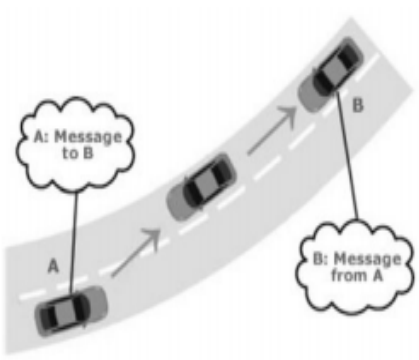

Fig.3. Routing Based Communication.

II. ROUTING AND SECURITY CHALLANGES IN VANET

Routing is very important as far as there are many networks that are connected with each other. Routing helps to carry traffic from one source of network to another network. So in order to do routing we need some wireless routing protocols for the propagation of the traffic from one node in a network to the another node in the different network. in VANET there are different clusters which forms the wide area network so it's essential to do routing in order to carry traffic from one cluster of network to the another cluster of the network. Since in VANET network, the topology change occurs very frequently due to the high mobility of the vehicles in the network so it's essential to hold a network in a strong security. These vehicles are communicated in such a way that they can provide real time information of each vehicle to the road side units. There are such protocols which can govern security challenges as well when implemented within the vehicles in a VANET network.

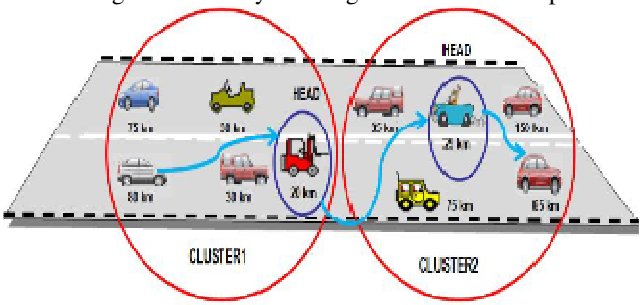

Fig.4. VANET Architecture with Clusters

Mainly there are two types of protocols that are used in the VANET network or wireless environment proactive and reactive protocols. Both protocols are based on the algorithms in order to maintain the routes from one network to another network. In proactive routing protocol it maintains a routing table thus it's also called as table driven routing protocol. Every node which has proactive routing protocol should maintain up to date information of the other nodes in order to pass routes. Since the traffic in VANET environment is very dense so it's quite difficult for every node to maintain up to date information in a table. DSDV, WRP are proactive routing protocols. On the other hand the reactive routing protocol initiates a route discovery in order to send packets to the destination. In this protocol like AODV, DSR maintains route discovery to the unknown path in which query packets are being flooded for the next path search.

VANET network is actually a wide area network which generally supports large number of mobile spectrum that is being operated in the vehicles. These spectrum are kind of application for drivers safety point of view. In VANET packets are being sent form one node to another node in open access though vehicular ad hoc network is open network as information is being transmitted openly. So it's for sure that there are malicious attackers within the network or outside the network which can easily sniff the informative data and can make big changes to that data. Now security becomes an essential criterion for the VANET environment to secure it from getting

disturbed by the malicious attackers. The attacker can make changes to data in many different ways as the attacker can get access to the source node and can keep that data as it is which is known as passive attack another attack is that where attacker sniffs the data and sends wrong information to the receiver. In security issues we need to first identify the attacker and the malicious attacked that has occurred in the network. Although there are cryptographic schemes where public or private key is being shared for the authentication purposes even IPSec is also security standard.

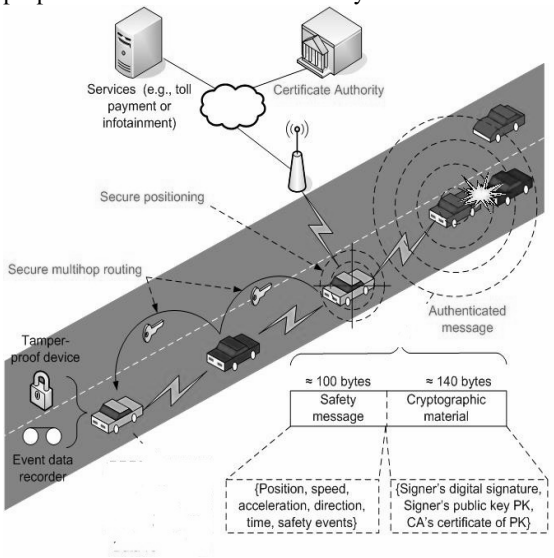

Fig.5. Cryptographic Key Exchange Scheme

III. RELATED WORK AND APLM MODEL

Since VANET is a wide area network and it's necessary that every portion of the network should remain under security. Every vehicle in network sends packets from one end of network to another end of the network. There are various threats to the data transmission in confidentiality, integrity and authentication due to open environment of VANET network. So it's required that we need to focus on the total number packet content that a receiver has received from the sender. There are such attacks in a network such as they can even become the part of the network as they can change their identity. Thus for a network it's required that we can conclude the number of packets that is being propagated across the network. In VANET network if one vehicle is being compromised then there are greater chances that other vehicles can get disturbed. Each vehicle in the vehicular environment has got their unique identity (ID) so on that basis attacker can posses that id and can pretend as the legitimate system in the network. Even there can be the attacks to the ids of the vehicle which can loss the authentication. In this case an attacker can transmit lot of messages with different ids and can make change in the road track. So it's necessary to provide security with regards to the data transmission and make data reliable. So my aim of the project is that to find out packet delivery ratio, end to end delay and through put. So by implementing APLM model we can easily conclude the above three parameters of the data content that is being send from source node to the destination node.

A. NETWORK TOPOLOGY

In order to create mobile network topology we need to install network simulator NS-2 which will help us to create number of mobile node. Each mobile node has got their own speed in dynamic VANET topology and they will behave as a wireless router. Every node in a mobile state will send traffic to other nodes through wireless medium. The communication between node to node is in a form of multi hop uni cast. There are two type channels that have been used in my project which is two ray ground and nakagami propagation model. Both these propagation models are used to deliver traffic. Two ray ground propagation model are used to built basic network topology. The main feature of using this model is that it gives us actual accurate prediction of the signal received at longer distances. Another nakagami propagation model gives us the free channel space for the mobile node used in the network. It also helps to give closer representation of the radio channels. Every node must be fitted with the omni antenna which has got property of sending signals in all the directions.

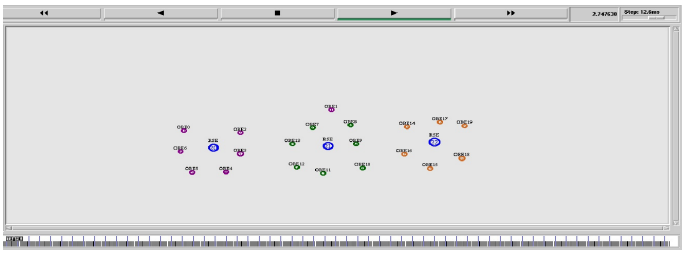

Fig.6. Node to Node communication

In my project I am using NS-2 simulator which helps to create many mobile nodes which has got different parameters. Every node has got their own coordinates in x axis, y axis and z axis. NS-2 uses c++ language in Tool Command Language (TCL) as a script. Every node moving with some speed always tries to communicate with other nodes by using wireless routing protocol. The protocol that I am using is ad hoc on demand distance routing protocol (AODV) . The feature of using this protocol is that its self starting in multi hop communication and tries to main routes but not on regular intervals. Each node used in NS-2 has got certain parameters like MAC Layer 802.11, Interface Queue (IQ), Link Layer (LL) and PHY layer which is used for the wireless channel medium.

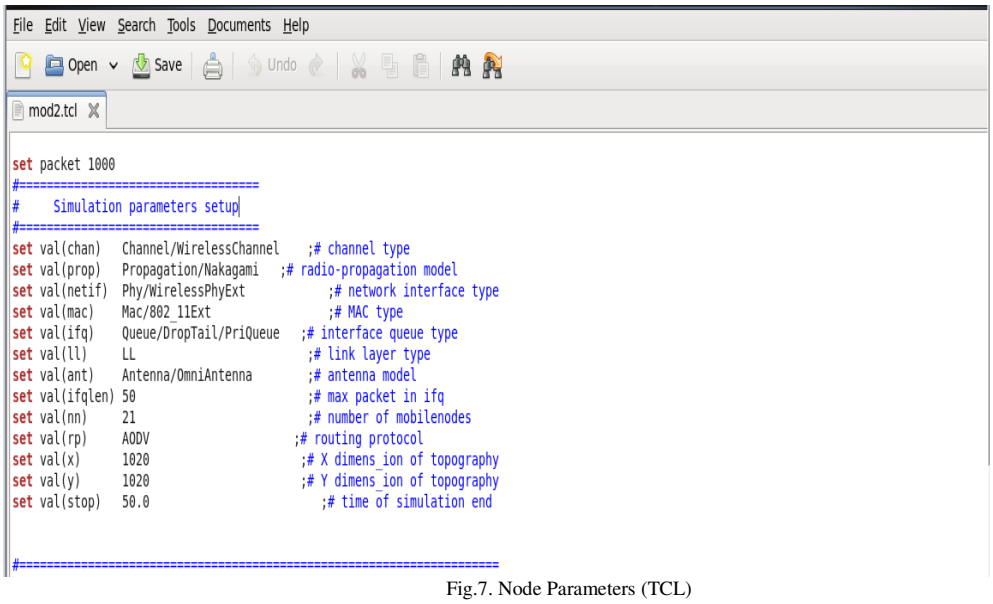

Fig.7. Node Parameters (TCL)

B. APLM MODEL.

APLM model is defined as Asymmetric Profit Loss Markov Model in which we can check the number of packet that have been received and the number of packets that have been lost in the network during communication. APLM model is used in a way that we use awk script to denote the overall results of the received packets. There are mainly there types of graph which can be obtained after implementing of APLM model packet delivery fraction, end to end delay and through put. All three helps us to verify the net data transmission of the packets in the vehicular environment. Since in VANET the vehicles are moving with higher speed and their positions keeps on changing due to track change, so at the first instance of data transmission the packet delivery ratio/fraction is very high which can be concluded by using APLM model. In APLM model On Board Units (OBUs) acts as a data hosts and Road Side Units (RSUs) acts as a data retrievers.

The three parameters in APLM can be showing in diagram which we have concluded in NS-2 simulator

$$\sum \text{No of packet receive} / \sum \text{No of packet send}$$

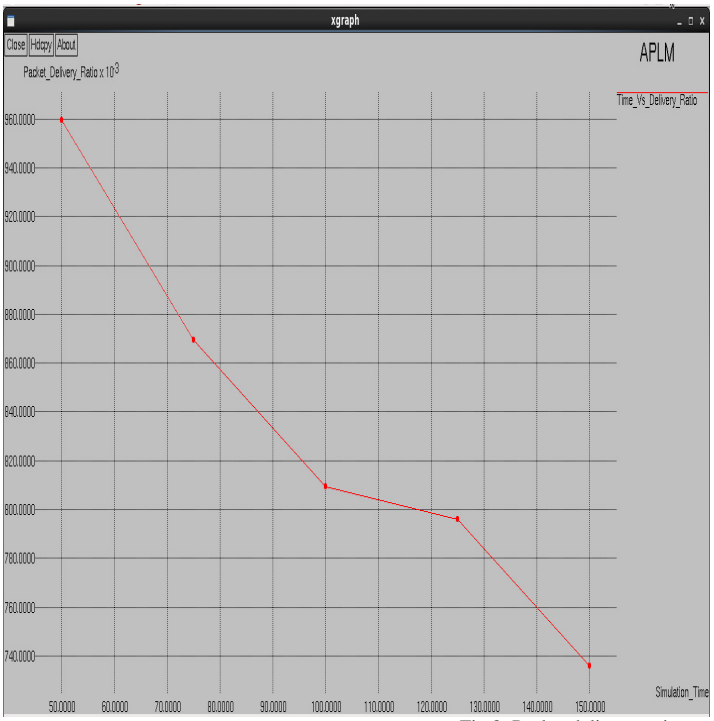

Fig.8. Packet delivery ratio

The above figure shows the packet delivery ratio which can be mathematically determined by the total number of packets received by total number of sent packet. So mainly packet delivery ratio can be defined as if the value is greater then the performance of the protocol is better.

End to end delay can be defined as the time taken by the packet to reach source to destination. It also defines us the delay that are caused by the route discovery process in order to find the path mainly which AODV protocol has that disadvantage and due to queue in the data transmission. So here the packets which are being delivered to the destination are only being taken into consideration. Value which has lower number in end to end delay means greater performance of the protocol

$$\sum (\text{arrive time} - \text{send time}) / \sum \text{No of connections}$$

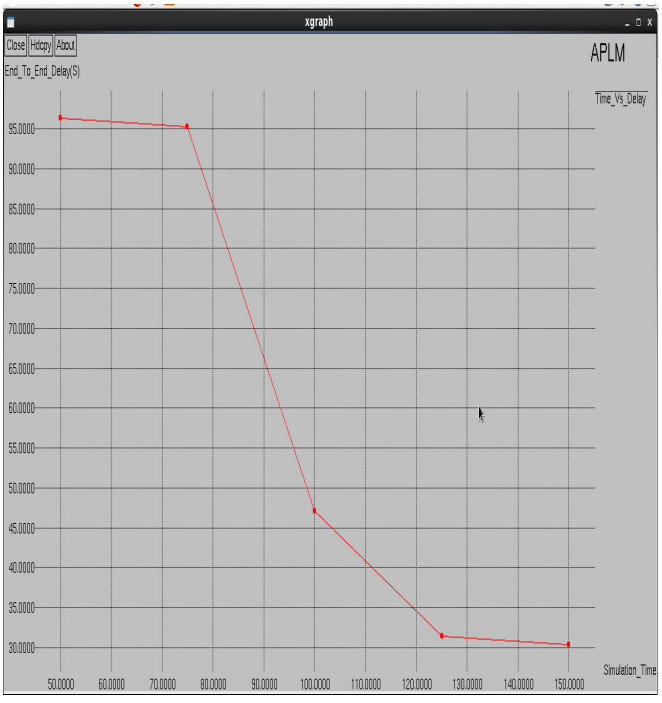

Fig.9. End To End delay

Throughput can be defined as the average delay between the source node and the destination node. Since it's very often in VANET topology that the nodes move within a transmission range and so network performance is directly dependent upon the number of hops with average delay in a network.

(Received Size/(Stop Time-Start Time))*(8/1000))

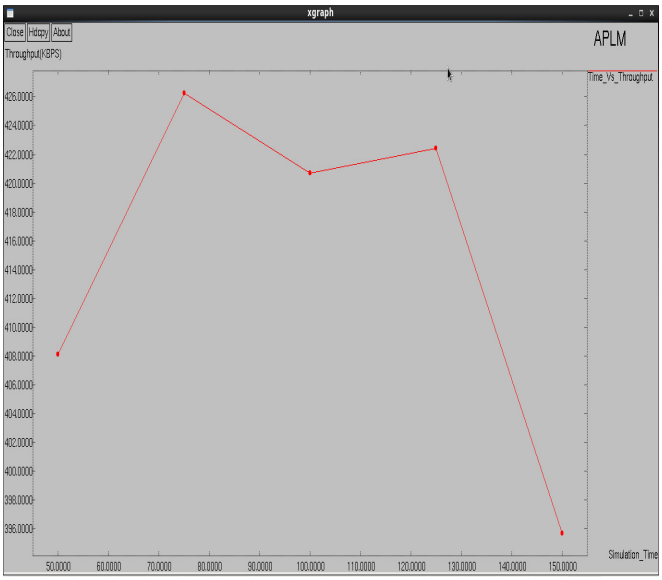

Fig.10. Throughput

These are the results that we have obtained from above three parameters

Packet delivery Ratio:0.7389

Average End-to-End Delay = 40.013 ms

Throughput [kbps] : 488.97

C. TESLA PROTOCOL

TESLA (Timed Efficient Stream Loss-tolerant Authentication) is another broadcast authentication protocol which can help to secure the broadcast communication by source authentication. TESLA is based on loose time synchronization between the sender side and the receiver side. Since MAC uses symmetric cryptographic function while as TESLA also uses symmetric functions for authentication. The basic concept of TESLA is that a MAC is being attached to the sender with a key k and only sender is aware about the key. Receiver keeps the packet from the sender without being able to authenticate it. And after sometime the sender exposes k and receiver is able to authenticate the packet. A MAC per packet is sufficient for the broadcast authentication unless there is clock synchronization between the sender and the receiver. TESLA is used in various applications like in wireless sensor networks, and ad hoc routing protocols for the authentication. So in brief TESLA requires loosely time synchronization with the sender and it also needs an efficient mechanism to authenticate the keys at the receiver side for broadcast authentication. TESLA uses digital signature for the authentication purposes. The requirement for TESLA protocol is that both the sender and receiver should be loosely time synchronized. TESLA is used in VANET networks in order to decrease overheads which are related with the user authentication. TESLA uses digital signature to authenticate the user node through a mechanism known as Elliptic Curve Digital Signature Algorithm (ECDSA). This algorithm is highly used for encryption and decryption of the messages that a sender is sending to the receiver. ECDSA is a mathematical representation which is a IEEE standard and ISO standard.

The main advantage of using ECDSA is to provide secure and faster delivering of data once authenticating the nodes in the network. Using asymmetric ECDSA pair of keys in VANET topology helps to user authentication. Asymmetric ECDSA key pair uses both private key and public key for the authentication purposes.

Asymmetric ECDSA key pair is used in VANET systems to provide User Authentication. ECDSA can also be used to generate and verify signatures.
There are mainly two steps that a user should follow for authentication at the beginning the public key of the sender is being validated. The validation of the public key is important in order to prevent attacks from the user using invalid public keys. This helps to prevent transmission errors. The second step includes the authentication of the user node by confirming and validating his or her private key. It's done because to ensure that malicious attacker is using the fake identity of the legitimate user to propagate wrong information. So at last when public key is being validated then the sender node is asked for sign the message with his private key. So this mechanism provides good authenticity and high level of reliability

V. CONCLUSION

In this paper we have proposed data transmission on VANET topology and user authentication The implementation of APLM model describes us the number of packet received by using awk script and TESLA gives us user authentication for the nodes in the VANET network Though it is necessary to conclude the number of packets that have been lost during sharing the information. It is to be noted that at the first instance the received packet is more than lost packet but with the effect of time there is more number of loss and thus decrease the through put of the network.

ACKNOWLEDGMENT

I would take the opportunity to thank Dr. Ishan Ranjan, HOD, Sharda University for encouraging me to start my work with zest and zeal.

I express my deepest sense of gratitude and respect to my supervisor Dr. Ravi Rastogi, Professor, Department of Computer Science and Engineering, Sharda University for his exemplary guidance, encouragement and support in my research work. His constant help and motivation helped me overcome all my obstacles confidently.

REFERENCES

[1] M. Nasir, A.S.M. Hossain, S. Hossain, M. Hasan, B. Ali: Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network, International Journal of Scientific & Technology Research, Vol. 2, No 4, 2013, pp. 156-61.

[2] K. Azogu, T. Ferreira, H. Liu:. A Security Metric for VANET Content delivery, IEEE Globecom, 2012, pp. 991-96.

[3] Y. Gadkari and B. Sambre: VANET: Routing Protocols, Security Issues and Simulation Tools, Journal of Computer Engineering, 2012, pp. 28-38.

[4] S. Nain and S. Tayal: A comparative study of the Security Protocols in VANET, Proceedings of the International Conference on Emerging Trends in Engineering and Management, 2012, pp. 279-81.

[5] T. Kaur and A. K. Verma: Simulation and Analysis of AODV routing protocol in VANETs, International Journal of Soft Computing and Engineering, 2012, pp. 293-301.

[6] K. Bür and M. Kihl: Selective Broadcast Algorithms for Safety Applications in Vehicular Ad Hoc Networks, IEEE VTS Workshop on Wireless Vehicular Communications, 2010, pp. 1-15.

[7] J. Haas, Y. Hu and P. Laberteaux: Real-World VANET Security Protocol Performance, IEEE Globecom, 2009, pp. 1-7.

[8] Zhang and S. Wolff: Routing Protocols For VANET in Rural Area, IEEE Automotive Networking, 2008, pp. 126-131.

[9] M. Raya and J. Hubaux: Securing vehicular ad hoc networks, Journal of Computer Security, Vol. 15, 2007, pp. 39-68.

[10] Tonguz, Wisitpngphan, Bai, Mudalige and Sadekar: Broadcasting in VANET, IEEE, 2007, pp. 7-12.