Safety Traffic System using VeMAC Protocol in VANET

Shubham T. Beldar, Sunita B. More, Kajal K. Patil, Pournima V. Mali

***Abstract*---Nowadays, there are large numbers of accidents take place on the road because lack of technology. Then road safety is become more important to prevent large numbers of increasing accidents. For this purpose the vehicular Ad hoc network (VANET) provide promising approach for improving road safety and other applications to the driver of vehicles. VANETs technology can make driving safe by enabling the variety of advanced road safety applications, It broadcast the safety messages to vehicle and road side unit`s. The multichannel TDMA MAC protocol designed specifically for vehicular Ad hoc networks. The VeMAC decreases the probability of transmission collision caused by node mobility by assigning time slots to vehicles moving in opposite directions. As compare to Ad hoc MAC, the time slots assigned to the node on control channel much faster in VeMAC. Thus, VeMAC has improved rate of throughput in message transfer between vehicles. The IEEE 802.11p is improved amendment to IEEE 802.11 standard is used to add wireless access in vehicular environments for vehicular communication system. Here, sometimes the message passing between the vehicle and road side units create the collision while exchanging messages. Also delay between sender and receiver. So, here TDMA concept and VeMAC protocol is useful for implementation.**

I. INTRODUCTION

A network forms by the collection of nodes dynamically without any existing infrastructure is called as VANET. Which is the network among moving vehicles. The IEEE 802.11p is an improved ammendment to IEEE 802.11 standard is used to add wireless access in vehicular environments for vehicular communication system. Here, sometimes the message passing between the vehicle and roadside units create a collision while exchanging the messages. Also delay between sender and receiver. So here TDMA concept VeMAC protocol is useful[1].

II. BACKGROUND

Vehicular Ad-hoc Networks (VANET) are a technology that provides communication between vehicles or between a vehicle and Infrastructures or road side units i.e. RSU using wireless communication. A vehicle accident is likely to cause a serious tragedy. Therefore, the Vehicular Ad-hoc Networks system provides an essential information exchange protocol for communication between vehicles and or vehicles and infrastructures. However, a previous key exchange scheme based on the recommended general network for a rapid communication environment which is not suitable for vehicles. In this system, the first communication from the Infrastructures passes only group keys and it updates the key value in the communication with the vehicle using Bloom filters to verify the proposed method. In this system in Vehicular Ad-hoc Networks (VANET), dispersed operations are carried out in the Infrastructures or road side units i.e RSU. By reducing to a minimum the number of keys exchanged, more safe group communication can be realized. In this system, a message batch verification scheme that can verify multiple messages and cession authentication systematically even for multiple communications with many vehicles[1].

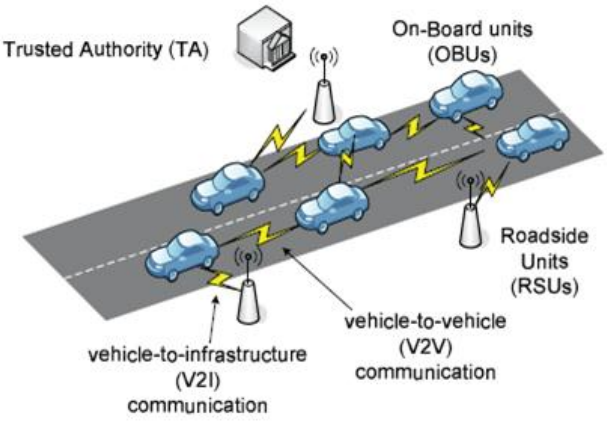

Fig. Overview of VANET

Vehicular ad-hoc networks (VANET) have attracted considerable attentions recently as a promising technology for reorganizing the transportation systems and providing broadband communication services to vehicles. VANET consist of entities including On-Board Units (OBUs) and infrastructures. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure, which respectively allow OBUs to communicate with each other and with the infrastructures. Since, vehicles communicate through wireless channels, a variety of attacks such as for inserting wrong information, modifying and repeating the disseminated messages can be easily launched[2].

A security attack on VANET can have severe harmful consequences to legitimate users. Accordingly, ensuring secure vehicular communications is must before any VANET application can be put practically. A well-recognized solution to secure VANET is to deploy Public Key Infrastructure (PKI), and to use Certificate Repeal Lists (CRLs) for managing the revoked certificates. In PKI, each node in the network carries an authentic certificate, and each message should be signed before its communication. A CRL, usually issued by a Trusted Authority (TA), is a list

containing all the revoked certificates. In a PKI system, the authentication of any message is performed by first checking if the sender certificate is included in the current CRL, i.e. checking its repeal status. Then, verifying the sender certificate, and finally verifying the sender signature on the received message. The first part of the authentication, which checks the invalid status of the sender in a CRL, may suffer longer delay depending on the CRL size and the employed mechanism for searching the CRL. To preserve the privacy of the drivers, i.e. to keeping the leakage of the real identities and location information of the drivers from any external Infrastructures or road side units i.e. RSU Infrastructures or road side units i.e. RSU snooper each OBU should be preloaded with a set of undefined digital certificates, where the OBU has to periodically change its undefined certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size the scale of VANET is very large.

According to the United States Bureau of Transit Statistics (USBTS), there are approximately 250 million OBUs in the United States in 2005. Since the number of the OBUs are large and each OBU has a set of certificates, the CRL size will increase dramatically if only a small part of the OBUs are revoked. To have recommendation of how large the CRL size can be, consider the case where only 100 OBUs are override, and each of this has 24,000 certificates. According to appointing the mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard does not state that either a non-optimized search algorithm[2].

III. MOTIVATION

Every year in the United States, about six million trace accidents occur due to automobile crashes. In 2003 alone, these accidents accounted for 220 billion in damaged property, 2,790,000 nonfatal injuries, and 42,573 deaths. While different factors contribute to vehicle crashes, such as its mechanical problems and bad weather, driver behavior is considered to be the leading cause of nearly more than 90 percent of all accidents. The inability of drivers to react in time to emergency situations often creates a potential for chain collisions, in which an series of collisions occur because of the beginning collision between two vehicles involving the vehicles that moving in the same direction. In emergency situations, a driver typically relies on the tail brake light of the vehicle immediately ahead to decide braking action. Under typical road situations, this is not the best strategy for collision avoidances. Driver reaction time typically ranges from 0.75 to 1.5 s. At a speed of 70 mph, this means that between 75 and 150 ft is traveled before any reaction occurs. In dense traffic, the effects of cumulative reaction times, as one vehicle after another reacts to the vehicle ahead braking, can further aggravate the situation. As a result, a single emergency event can often lead to a string of secondary crashes, creating a multi-vehicle chain accidents. Chain collisions can be avoided by reducing the delay between the time of analytic event and the time at which the vehicles behind are informed about it. One way to provide more time to drivers to react in critical situations is to develop Intelligent Transportation System applications using emerging wireless communication technology. The benefit of such communication will be to enable the important information to be propagated among vehicles much quicker than a traditional chain of drivers reacting to the brake lights of vehicles immediately ahead. The protocol to be implemented as a part of the project helps such quick propagation and works positively to avoid the aforementioned chain collisions among vehicles.

IV. EXISTING SYSTEM

Previous research works about warning messages have concentrated on three issues: medium access control, message dissemination protocols and collision prevention mechanisms. Authors considered a counter-based method to assign additional delays on top of the MAC back off, and used it as a rebroadcast suppression mechanism that reduced packet collisions. They also combined a position-based method with the counter based method to make a better choice of the next hop forwarder. Some Authors also proposed a efficient IEEE 802.11 based Urban Multi-hop Broadcast protocol (UMB) which was designed to address the broadcast attack, hidden node and to sure problems of multi-hop broadcast in urban areas. They showed that this protocol had a very high success rate and efficient channel utilization. Some Authors also tried to achieve low-latency in delivering emergency warnings in various road situations. They designed an effective protocol, comprising crowd control policies, service separation mechanisms and methods for emergency warning dissemination[3].

V. PROPOSED SYSTEM

In our system, each vehicle occasionally broadcasts information about itself. When a vehicle receives a broadcast message, it stores and immediately forwards it by re-broadcasting the message. Warning messages should be broadcast to all adjacent nodes up to a certain number of hops, and so a flooding-based routing protocol fits our requirements adequately. We pretend that the warning packets sent by damaged nodes can be received by all the vehicles in the nearby area, and so this protocol offers the best reliability in terms of coverage[4].

The purpose is to provide the minimum set of statements required to ensure compatibility between wireless devices that communicate in potentially rapid changing communication environments, as well as in situations where agreement must be completed in time frames much shorter than the minimum allowed with ad hoc networks. The proposed warning advertisement system is composed by the damaged nodes that send warning messages periodically (T-warning) to inform about their situation to the rest of the vehicles. These messages have the highest priority (AC3). Unimpaired vehicles make the propagation of these warning packets and periodically send other messages with information such as their position, their speed, etc. These periodic messages have less priority (AC1) than warning messages and are not broadcast by distinct vehicles. With respect to warning messages, each vehicle is only allowed to transmit them once for each sequence number, being that

older messages are dropped.

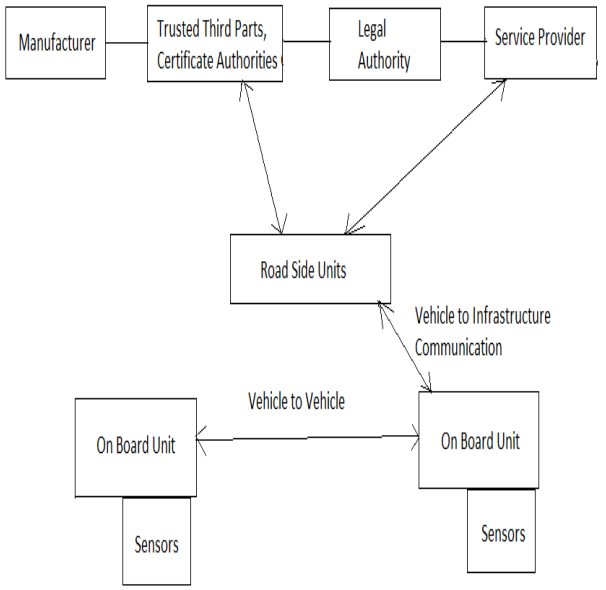

Fig. Architecture of VANET

Architecture of VANET consist of different components such as- 1.Manufacturer, 2.Trusted Third Parts & Certificate Authority, 3.Legal Authority, 4.Service Provider, 5.RSU, 6.On Board Unit, 7.Sensors. Which can be described as follows:

1. Manufacturer: Manufacturer notifies each vehicle in the VANET model one by one.
2. Trusted Third Parts & Certificate Authority- TTP are also available in VANET model. They can provide different services like certification and qualification.
3. Legal Authority: There are mainly two task are available in legal authority- vehicle registration and offence reporting. Every vehicle when manufactured get register first to issue authority license plate. It also provides traffic reports and fines.
4. Service Provider: Service provider provides facility that can be access through VANET.
5. RSU: Road Side Units
6. OBU- (On Board Unit): OBU authorize V2V and V2I communication.
7. Sensor: Sensor measures its own condition and its surrounding background.

A. IEEE 802.11p

The IEEE 802.11p standard is the main solution presently suggest for wireless access in VANETs [8]. The standard is based on the legacy IEEE 802.11 standard (WiFi), which was developed mainly for unicast transmissions, such as between a user device and a WiFi access point. accordingly, to support the broadcast-based safety applications in VANETs, IEEE 802.11p has considerable limitations. The main reason for the poor performance of IEEE 802.11p in supporting safety applications is the high probability of "collision" of the broadcast safety messages. That is, if two nodes are near to each other they simultaneously broadcasting their safety messages, the messages will "collide" at each surrounding node that is located within the communication range of the two transmitting nodes. Consequently, these surrounding nodes cannot successfully receive any of the two colliding messages. For unicast communications, as specified in IEEE 802.11p standard, the possibility of a dispatch collision is reduced by using a two-way handshaking mechanism before the actual transmission of data. That is, if a source node needs to transmit a packet1 to a destination node, it first transmits a short control packet, known as request-to-send (RTS), and waits until the destination node replies by another control packet, known as clear-to-send (CTS). Subsequent the RTS/CTS exchange, all the neighboring nodes defer accessing the wireless channel (in order to avoid any transmission collision) until the source and destination nodes complete the exchange of the actual data, that is, the source transmits a data packet and the destination replies by an acknowledgment (ACK) packet. Unlike the unicast case, according to IEEE 802.11p, no RTS/ CTS exchange should be used for broadcast packets, and no ACK should be transmitted by any recipient of the packet. Consequently, this lack of RTS/CTS interchange results in a high possibility of a transmission collision, which reduces the rate of successful packet delivery of the IEEE 802.11p broadcast service, especially with the absence of ACK packets[4].

B. VeMAC Protocol

VeMAC provides well organized one-hop and multi-hop broadcast service on the control channel by using implicit acknowledgment and eliminating the hidden terminal problem. VeMAC reduces transmission collision due to node movability on the control channel by allocating disjoint sets of time slots to vehicles among opposite directions and to road side units[5].

There are two types of units under consideration:

1) OBU(On-board unit consisting radio interference to connect to the other OBU's and RSU's and wired or wireless interference to connect to other application unit).

2) RSU(Road Side Units).

3) VeMAC is used because it decreases the transmission collision of messages. By assigning the time slots to vehicles more another for opposite direction as compare to Ad hoc. So, VeMAC protocol is beneficial for faster forwarding the messages from sender to receiver without any collision and delay between the messages. VeMAC is completely contention free protocol. This protocol support single-hop and multi-hop broadcast services uncontrolled channel which provides smaller rate of access collision. In VeMAC these collision are reduce by assigning separate sets of time slots to cars moving is opposite direction and to roadside units. So, here the implementation of TDMA's VeMAC protocol is essential because TDMA allows several user to share the same frequency channel by dividing the messages in faster speed one after the another each using its own time slot. This allows the another vehicle and roadside units to share same frequency channel. so, here by implementing VeMAC protocol the vehicles and roadside units have proper time to send secure or safety messages without collision and provide the delay[6].

VI. RESULT AND ANALISYS

Figure shows the simulation of the VeMAC Protocol. In figure, the node 6 at which event has occurred sends safety message to his neighboring nodes and other nodes forwards that message to other adjacent nodes.

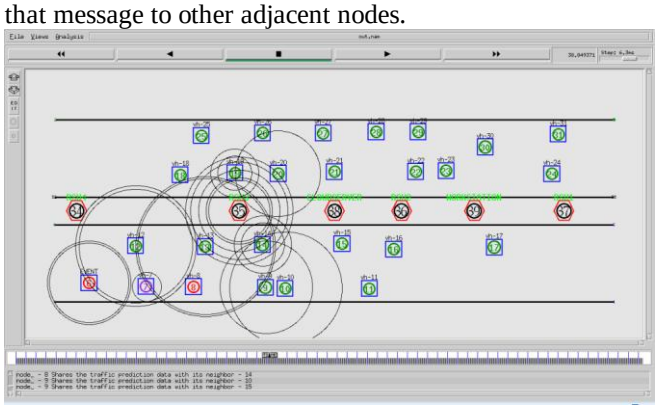

Fig. simulation of VeMAC Protocol in ns2

Following graph shows the throughput ratio that is the total number of message transmitted by vehicles using the VeMAC protocol. The message transmitting rate of the VeMAC protocol is more while the broadcasting messages because it uses the acknowledgement packet. So, VeMAC allows a node to deliver safety messages to all the nearby nodes in its communication range[6].

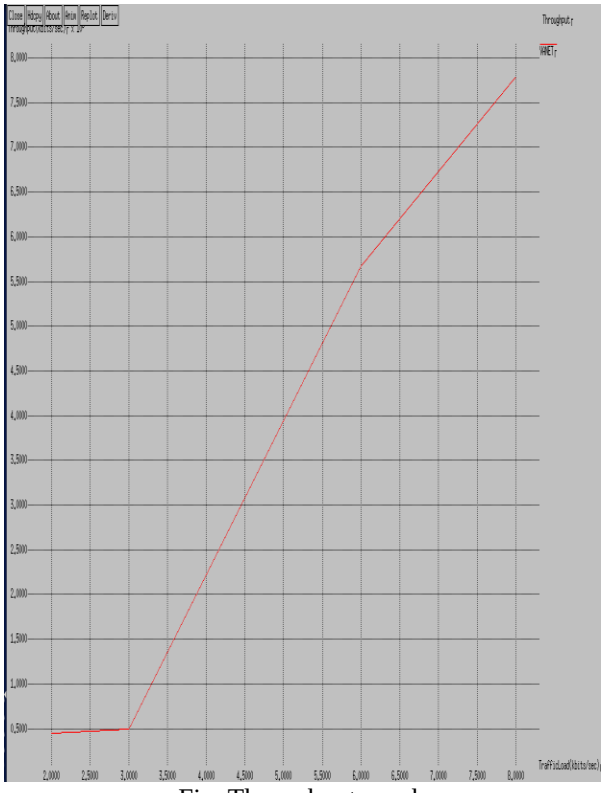

Fig. Throughput graph

VII. CONCLUSION AND FUTURE WORK

The propagation delay is lower when density of node increases. Besides, the percentage of blind nodes highly depends on the factor. When the area increases, the system requires more time to notify the remaining vehicles and the percentage of blind nodes highly depends on the factor, also. When the area is very small, the percentage of blind nodes is also very small. When there is a large area, the number of blind nodes also increases. Nevertheless, the total number of packets received per node decreases. The size of the packets sent does not affect the warning advertisement systems behavior. When we vary the priority of the packets sent by the undamaged nodes, the propagation delay of the system changes. The results demonstrated that to obtain the lowest probable propagation delay in our system, the best result is to give less priority to the background traffic, while the warning messages must have the highest priority.

The role of mobility of vehicles in the performance of any dissemination technique is very important. The future work will have to be concentrated on adapting the protocol in different mobility scenarios. Also, increasing the priority of the warning messages can even more increase the efficiency of the protocol, which is left as a part of future work.

REFERENCES

[1] Hassan Aboubakr Omar, Ning Lu, and Weihua Zhuang \Wireless Access Technologies for Vehicular Network Safety Applications" IEEE 2016

[2] Mohamed Hadded, Paul Muhlethaler, Anis Laouiti, Rachid Zagrouba, Leila Azouz Saidane "TDMA based MAC Protocols for Vehicular Ad Hoc Networks A Survey, Qualitative Analysis and Open Research Issues" IEEE 2015.

[3]LZhang,Z.Liu,R.Zou,J.Guo,andY.Liu,"Ascalablecsmaand self organizing tdma mac for ieee 802.11 in vanets, Wireless Personal Communications", vol. 74, no. 4, pp. 11971212, Feb. 2014.

[4] I. Khou, A. Laouiti, and B. Wahbi, "Tar channel access mechanism A study of a highway ramp car merge case, in International Conference on New Technologies, Mobility and Security (NTMS)", Dubai, UAE, Mar. 2014.

[5] K. Ota et al.," MMCD Cooperative Downloading for Highway VANETs, IEEE Trans. Emerging Topics Comp".

[6] H. A. Omar et al.," Performance Evaluation of VeMAC Supporting Safety Applications in Vehicular Networks, IEEE Trans". Emerging Topics Comp., vol. 1, no. 1, June 2013.

Shubham T. Beldar received his B.E. degrees from North Maharashtra University in 2017, Jalgaon, State Maharashtra, India.

Sunita B. More received his B.E. degrees from North Maharashtra University in 2017, Jalgaon, State Maharashtra, India.

Kajal K. Patil received his B.E. degrees from North Maharashtra University in 2017, Jalgaon, State Maharashtra, India.

Pournima V. Mali received his B.E. degrees from North Maharashtra University in 2017, Jalgaon, State Maharashtra, India.

Shubham T. Beldar received his B.E. degrees from North Maharashtra University in 2017, Jalgaon, State Maharashtra, India.