VANET based Communication on Vehicles for Accident Prevention

Mrs. N. Premalatha, M.E.,(*Author*)
Assistant Professor, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India

Ms. Manju Kumaresan, B.Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India

Ms. Shalini Devi Raja, B.Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India

Ms. Yamunasri Loganathan, B.Tech.,
Student, Department of Information Technology
V.S.B. Engineering College, Karur
Tamilnadu, India

***Abstract*—The condition of the road surfaces consider as a major indicator of quality of the roads. In fact, classification of a road as either safe or dangerous, more often than not taken into consideration the surface condition of the road. Typically, parameters such as potholes, bumps and slipperiness consider as the distinguishing features of quality of the road surfaces . As a result, this is an area where systems for monitoring road conditions are critical to improvement of safety in roads, decreasing accident rates and protection of vehicles from getting damaged as a result of poor surface road conditions. This project describes the Monitoring Vehicle Communication and Road Condition in Vehicular Ad-hoc Networks and accident alert system. Based on ambulance system give the alert for to vehicle.Traffic has controlled before ambulance come that particular area. This system control the traffic and accident in future system.**

Keywords—VANET, traffic, network, vehicles, transmit, accident

I. INTRODUCTION

Vehicular ad-hoc network (VANET) could be a challenging network environment that pure-sues the concept of ubiquitous computing for future. Vehicles equipped with wireless communication technologies and acting like computers are going to be on our roads soon, and this can revolutionize our concept of traveling. VANETs bring lot of possibilities for brand spanking new range of applications which can make our travel not only safer, but also fun. The continuing increase in road track accidents worldwide has motivated the event of Intelligent Transportation Systems (ITS) and other applications to boost road safety and driving comfort. A communication network, called a VANET1, during which the vehicles are equipped with wireless devices has been developed to create these applications feasible. Recently, VANETs have attracted plenty of attention within the research community and in automobile industries thanks to their promising applications. Nevertheless, VANETs have own specifies: high node mobility with constrained movements and also the mobile nodes have ample energy and computing power. In a VANET, communications can either be Vehicle to- Vehicle (V2V) or Vehicle-to-Infrastructure (V2I). The applications of VANET are often divided into the subsequent three services namely, safety services, track management and user-oriented services. Safety services have special requirements in terms of quality of service. At the identical time, user-oriented services need a broad bandwidth. MAC2 protocol will play a crucial role in satisfying these requirements. In VANETs, nodes share a typical wireless channel by using the identical radio frequencies and thus an inappropriate use of the channel may cause collisions and a waste of bandwidth. Hence, sharing the channel is that the key issue once seek to supply a prime quality of service. MAC schemes must be designed to share the medium between the nodes. However, thanks to the special characteristics of VANETs, traditional wireless MAC protocols aren't suitable to be used in VANETs which leads either to adapting these traditional MAC protocols or to designing new mechanisms. Generally, MAC protocols constitute one amongst two broad categories: contention-based and contention-free. In contention-based protocols, each node can attempt to access the channel when it's data to transmit using the carrier sensing mechanism. Several neighbouring nodes can sense a free channel, so plan to access and transmit their data at the identical time, which generates collisions at the destination nodes. Contention-free MAC protocols attempt to avoid this issue by assigning access to the channel to only 1 node in an exceedingly neighborhood at any given time. Contention-based protocols don't require any preened schedule, each node will compete for channel access when it has to transmit, with none guarantee of success. For real-time applications, random access may cause problems like packet loss, or large access delay. On the opposite hand, contention-free protocols can provide bounded-delays for real-time applications, but require the periodic exchange of control messages to keep up the schedule table and need time synchronization between all the nodes within the network.

In order to provide QoS and reduce collisions in VANET, MAC protocols must broadcast service with predictable bounded delays. Moreover, they must also handle frequent topology changes, different spatial densities of nodes and the hidden/exposed node problem. They have to support multi-hop communication and nodes (vehicles) moving in opposite directions. The relevance of these issues has been corned by the development of a specie IEEE standard to support VANETs.

The IEEE 802.11p which is the emerging standard deployed to enable vehicular communication, is a contention-based MAC protocol, using a priority-based access scheme that employs both Enhanced Distributed Channel Access (EDCA) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanisms. However, the IEEE 802.11p standard does not provide a reliable broadcast mechanism with bounded communication delay. This disadvantage is particularly challenging in VANETs which are specially designed to improve road safety. Therefore, designing an MAC protocol that satisfies the QoS requirements of VANET applications is a particularly crucial task.

Currently, a great deal of research work on contention-free MAC protocols for VANETs is being carried out. These protocols help avoid the disadvantages of the IEEE 802.11p standard by eliminating the need for a vehicle to listen to the channel before it starts its transmission and by reducing the time to access the channel when node density is high. Several contention-free MAC protocols have been proposed in the literature for inter-vehicle communications including Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), and Time Division Multiple Access (TDMA). These protocols solve the collision problem as in the IEEE 802.11p standard by assigning respectively a unique frequency band, code sequence or time slot to each vehicle in a given channel contention area3. Therefore, these protocols are suitable for VANET safety applications in terms of access delay and collision rate. FDMA-based MAC protocols require that the transmitter and the receiver be synchronized to the same channel frequency. Hence, a frequency synchronization mechanism is necessary to match the communicating vehicles to each other.

The synchronization algorithm usually requires creating a dedicated control channel frequency which will be used by the vehicles to negotiate frequencies by exchanging control messages. This makes the FDMA mechanism very complex and adds a high communication overhead. Unlike FDMA, the CDMA scheme uses the same channel frequency which is shared between different vehicles by assigning unique code sequences. At the beginning of each communication, the sender and receiver must agree on the code to use in a way that reduces the risk of collision as much as possible. A CDMA code assignment algorithm is therefore required to negotiate and allocate codes for every communication, which means that the CDMA scheme has a significant overhead and an increased transmission delay.

II. EXISTING SYSTEM

In an existing system a brand new privacy-preserving signature theme for inter-vehicle communication has been enforced victimization bloom filters. information authentication and integrity protection in automatic dependent surveillance-broadcast system has been enforced. Ad-hoc or Topology Driven Routing generally, VANETs square measure infrastructure - less networks and plenty of routing protocols devised for previous ad-hoc
network like Manet supported supported topologies could also be applied to VANETs with sure sure. Topology driven protocols square measure sub-classified into three classes like proactive, reactive and hybrid. A variety of such protocols were designed to cater the wants of VANET surroundings. In a proactive protocol, nodes continuously update their routing table with info relating to new routes among the network. This informant particle is passed around to any or all nodes by causing periodic greeting packets. This approach, however, creates substantial management overheads. This restricts the employment of restricted wireless resource like accessible information measure. Resource like accessible information measure. On the opposite hand, in reactive approaches, as an example AODV, DSR, BRP nodes can solely send the management information once there's a necessity. This reduces overheads related to establishing the link, and helps distribute the particular info quicker. This approach but still puts undue resource overheads like maintenance of used/UN used routes. These unused ways square measure created and broken, thanks to rigorous topology of VA web. Overheads created in reactive protocols square measure related to discovering the trail to send the knowledge. the trail the trail is initiated by causing sure form of message referred to as Route Request Message (RREQ).

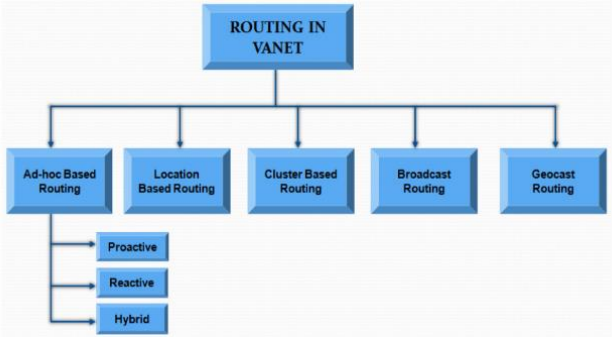

Fig: Routing types in VANET

Privacy preserving signature: As mobile devices are connected to the network all the time, through the vertical handover, they'll obtain a notion of social nodes. Such nodes can more easily be tracked down and are more vulnerable in several sorts of attacks, like impersonation, eavesdropping, man-in-the-middle, denial of-service, replay and repudiation attack[9]. Maintaining a high level of QoS in terms of delay, when huge volume of information is transferred inside a 5G network, while keeping on the identical time high security and privacy level, is critical so as to forestall malicious files from penetrating the system and propagating fast among mobile devices.Thus communications that satisfy zero latency requirements are cumbersome once combined with secure and privacy-preserving 5G networ
ks. For the method of conducting the literature review, follow the identical process conducted by our previous work in[9]. Specifically, the identification of literature for analysis during this paper was supported a keyword search, namely, "authentication and privacy-preserving scheme", "authentication and privacy-preserving protocol",

"authentication and privacy-preserving system", and "authentication and privacy-preserving framework".

III. DISADVANTAGES OF EXISTING SYSTEM

Delays because of congestion will be overcome via the addition of parallel routing protocols which bypass network access interference in an exceedingly differential algorithmic program. Network namespace maintains access node integrity during this setting by defining sequential parameters within the interface.[1] Cloud access relays maintain this architecture when massive data sharing is taken into consideration. Network congestion in data networking and queueing theory is that the reduced quality of service that happens when a network node or link is carrying more data than it can handle. A consequence of congestion is that an incremental increase in offered loads leads either only to low increase or maybe a decrease in network throughput. Flooding is that the forwarding by a router of a packet from any node to each other node attached to the router except the node from which the packet arrived. Flooding could be a thanks to distribute routing information updates quickly to each node in an exceedingly large network. it's also sometimes employed in multicast packets from one source node to several specific nodes in an exceedingly real or virtual network.

IV. PROPOSED SYSTEM

In this project road monitoring scheme implemented based on RCoM algorithm. Different types of feature implemented based on different kind of features a root authority (RA), many sub-authorities (SAs), many roadside units (RUs), a cloud server, and many vehicles. RCoM algorithm trained based on these features. And it's used to monitoring road vehicles.

This system has the following objectives:

- Introduce a set of TDMA-based MAC protocols that taken into account the unique VANET topology features without having to use expensive spectrum and complex wide-band mechanisms such FDMA or CDMA. These solutions should be able to dynamically adapt to frequency changes in VANET network topology as well as provide a reliable one-hop broadcast service that can ensure collision-free and delay-bounded transmission for safety applications.
- Present a TDMA-aware routing protocol for real time and multi-hop communications that can ensure coherent decisions between the MAC and routing layers by selecting the next relay node based on the TDMA schedule.The main goal of this work is to allow vehicles to send their event-driven safety messages over long distances.

RCoM architecture: The RCoM system consists of five types of entities that is, a root authority (RA), many sub-authorities (SAs), many roadside units (RUs), a cloud server, and many vehicles. As in VANET, RA, SAs and RUs are the trusted participants. In real-world applications, RA can be the Department of Transportation. The goal of RA is to monitor the real-time road conditions with the help of a cloud server, so that it could make timely response to emergency cases. The cloud server is maintained by some cloud service provider (CSP), which has significant computing and storage resources, and provides on-the-move access to outsourced data (i.e., road condition information) to end users. In RCoM, the cloud server is a curious entity, which is engaged by RA to maintain and process all road information collected by vehicles.

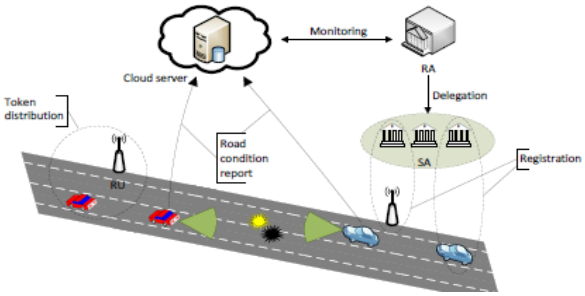

Fig: Architecture of RCoM

V. ADVANTAGES OF PROPOSED SYSTEM

In this proposed system, network delay and network congestion are reduced by using sub-authorities. In existing system, there is no sub-authorities so network delay and network congestion may occur. Public feel safety by using this system, because predict weather conditions and monitor the road conditions to prevent the accidents by intimating to the vehicle users. Through these predictable things, they can change the route and prevent the accidents. Public can feel comfort by using this system. In this proposed system, there is a mongoDB which is used to store the data and it is used to send the messages to the respective registered vehicle users.

VI. PROJECT IMPLEMENTATION

Module

1. Registration and contact module
2. VANET
3. Accident intimation
4. Weather forecast
5. MongoDB
6. Trace module

6.1.Registration and contact module

User can view the details about the all other users. It is processed by user module get all the user information's. Web system is connected with local host. The user enter the personal details for registering in the web system.

6.2 VANET

Vehicular ad-hoc networks (VANETs) includes vehicle-to-vehicle and vehicle-to infrastructure communication. In this, a novel smart phone integrated driving safety application along with a traffic signal priority control method in an attempt to clear the way for emergency vehicles is modeled. Management of Road Traffic information Retrieval In VANET Environment),a server and Road Side Units (RSUs and SA).

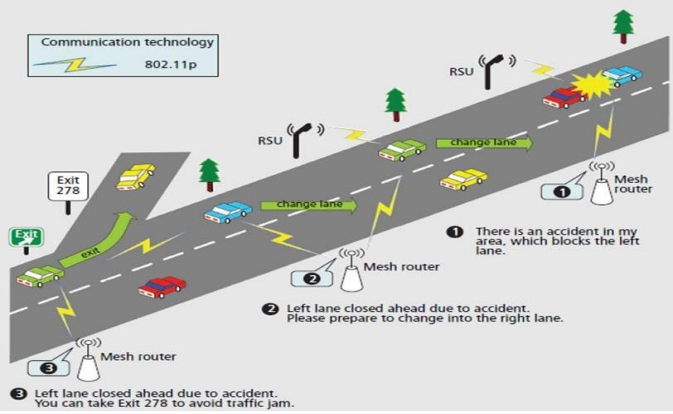

Fig: VANET diagram

6.3. Accident intimation

An accident management system that make use of VANET coupled with systems that employ cellular technology in public transport. The provides systems ensures the possibility of real time communication among vehicles, ambulances, hospitals, road side unit ,sub authorities and cloud servers.

6.4. Weather forecast

Weather forecast system that create use of VANET coupled with systems that employ cellular technology in public transport.The provides systems ensures the possibility of real time communication among vehicles, ambulances, hospitals, road side unit ,sub authorities and cloud servers. It is intimate the weather condition to the vehicles.

6.5. MongoDB

MongoDB is a document database with the scalability and flexibility that you want with the querying and indexing that you need. Here it is used to display the speed level of vehicles and presenatation chart.

6.6. Trace module

It is used to track the vehicle particular location. It is used to track the vehicle particular location.

VII. CONCLUSION

In this project, a typical system to manage accidents in order that vehicles area unit ready to avoid engorged areas inside associate degree ITS. Initially, a tendency to established associate degree accident management system that employs cellular systems of the general public transportation systems and VANETs to form economical period of time communication between vehicles potential, together with ambulances, hospitals, RSUs, and central servers. A tendency to afterwards propose a period of time algorithmic program for coming up with routes with the aim of up the use of house whereas at a similar time reducing the value of move, through vehicles' ability to avoid engorged road segments. Finally, the trail coming up with algorithmic program a tendency to propose can scale back the time taken by ambulances to be alerted and sent to a scene of accident through having the ability to avoid road segments that area unit engorged and can increase the possibility of saving the lives of accident victims. A tendency to thought of the matter of privacy-preserving cloud-based road condition observance with supply authentication (RCoM). There area unit 2 levels of authorities such the basis authority delegates sub-authorities to perform registration for vehicles and RUs. RA monitors period of time road conditions through a third party treater, that is, vehicles report the detected road conditions to the cloud server for verification and process, during this approach, solely the valid info sent from legitimate vehicles are going to be picked out for RA to form response. to safeguard the privacy against the cloud server, the road condition report ought to be uploaded in cipher text format, that brings another challenge for the cloud server to tell apart a similar road condition for a similar place from legion reports. In response to those functionalities and security and privacy necessities in RCoM, a tendency to given associate degree economical theme and compared it with connected techniques. Through in depth theoretical and experimental analyses, a tendency to demonstrate that the planned RCoM theme is sensible in application settings.

A Road Accident interference (RAP) theme for immediate EWM dissemination to the vehicles is planned so as to forestall them from road road traffic accidents. Thereby the death and injury rates will be reduced in Indian four lane highways. In RAP theme, once the RSU predicts the chance of incidence of associate degree accident or emergency state of affairs, instantly it generates EWM, forms a VBN structure and disseminates EWM to the vehicles that have high reception priority. The performance analysis of RAP schemesis finished by victimisation NS-2 machine. From the simulation results, it's detected that RAP theme with VBN structure outperforms RAP theme while not VBN structure by providing higher EWM dissemination performance in terms of (i) reducing the S-D distance, (ii) up notification by nineteen p.c and (iii) reducing end-to-end delay by fourteen.38 percent. Further, the quantity of RSUs needed is reduced because of the usage of VBN structure in VANET. But, the network process overhead of RAP theme with VBN structure is found to be higher.

VIII. FUTURE ENHANCEMENT

In future attempts can be made to reduce this overhead. It is proved from the simulation experiment that the overall performance of the RAP scheme is promising in four lane highway road than its counter parts such as two lane and six lane highway roads. The impacts of the RAP scheme will be analyzed based on fuel consumption and emissions of the traffic flow in future. The RAP scheme is designed only for linear four lane express highways. In future, the RAP scheme can be enhanced to work with real two dimensional highways.

IX. REFERENCES

[1] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[2] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 2,pp. 559–573, Feb 2010.

[3] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, Dec 2015.
[4] "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages,"IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240,March 2016.
[5] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, March 2017.
[6] L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 605–615, March 2011.
[7] Y. Liu, J. Ling, Q. Wu, and B. Qin, "Scalable privacy-enhanced traffic monitoring in vehicular ad hoc networks," Soft Computing, vol. 20, no. 8, pp. 3335–3346, Aug 2016.
[8] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud based vehicular networks with efficient resource management,"IEEE Network, vol. 27, no. 5, pp. 48–55, September 2013.
[9] J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, December 2015.
[10] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp.50–58, Apr. 2010.
[11] C. Gentry, "Fully homomorphic encryption using ideal lattices,"in Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, ser. STOC'09. New York, NY, USA: ACM, 2009, pp. 169–178.
[12] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and ` J. A. Manjon, "Contributory broadcast encryption with efficient ´encryption and short ciphertexts," IEEE Transactions on Computers, vol. 65, no. 2, pp. 466–479, Feb 2016.
[13] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 601–610, April 2017.
[14] V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," Computers & Security, vol. 60, pp. 193–205, 2016.
[15] A. Malhi and S. Batra, "Privacy-preserving authentication framework using bloom filter for secure vehicular communications,"International Journal of Information Security, vol. 15, no. 4, pp. 433– 453, Aug 2016.
[16] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," IEEE Transactions on Industrial Informatics, pp. 1–1, 2018.
[17] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," IEEE Computer, vol. 45, no. 1, pp. 39–45, Jan 2012.
[18] B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in the cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, Dec 2014.
[19] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores,"in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007,pp. 598–609.
[20] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.
[21] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology–ASIACRYPT 2009, M. Matsui, Ed. Springer Berlin Heidelberg, 2009, pp. 319–333.