www.ioirp.com

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 3, Issue – 3. May 2018

EMERGENCY ALERT USING IOV

Karthikmohan[1], Sow Kishore[2], Siddharth[3], Dhinesh[4]
[1,2,3,4] B.E. Computer Science and Engineering,
Dr.Mahalingam College of Engineering and Technology,
Pollachi, Tamil Nadu, India

Dr.A.Noble Mary Juliet[5]
[5]Associate Professor, Department of Computer Science and Engineering,
Dr.Mahalingam College of Engineering and Technology,
Pollachi, Tamil Nadu, India

***Abstract*—** Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network for data exchange to the domain of vehicles. Internet of Things (IOT) has provided a promising platform to build powerful vehicular networking systems by leveraging the growing ubiquity of wireless, mobile, and sensor devices. The communication between vehicles and their internal and external environments can be provided by various wireless connectivity. The entire vehicles are moving in the road using the VANET at that time they communicate with the Road Side Unit (RSU). The VANET information is checked by RSU and that is transferred to other RSU's. When an accident is occurred, that VANET arise an emergency message, the RSU which is near to accident place will receive the signal from the accident node. That RSU will change as authorized RSU. Authorized RSU will transfer the message between the other VANETs and RSU devices, then that message transferred to microcontroller by RSU, when a signal is received then the lane is closed.

***Key terms*: Vehicular ad hoc networks, Road Side Unit, Internet of Things, Mobile ad hoc networks, Public Key infrastructure**.

I. INTRODUCTION

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. The next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Vehicular Ad-hoc Networks (VANETs) can be considered as a subset of Mobile Ad hoc Networks (MANETs) with unique characteristics. A typical VANET consists of vehicles and access points along the road. Vehicles move on the roads sharing information between themselves and with the Internet through the access points. VANETs are used for short range high-speed communication among nearby vehicles, and between vehicles and roadside infrastructure units. VANET is a special class of MANET to provide communication among nearby vehicles and between vehicles and nearby roadside units. It is based upon short range wireless communication between vehicles. It is assumed that in these networks, each vehicle is equipped with embedded computers and computing devices and GPS (Global Positioning Systems) receivers.

GPS receiver provides all the information of a vehicle like speed, direction of movement of vehicle, time, location etc. Each vehicle stores the information about itself and other vehicles in a local database. The internet of things used for the purpose of hardware to close the lane, to prevent other more accidents. Microcontroller is used to receive a signal from VANET, when a signal is received then the lane is closed.

II. RELATED WORK

Zhu Qiankun et al proposed a Mobile Ad Hoc Networks Algorithm Improved AODV Protocol [20]. Ad Hoc network is a group of mobile devices with a wireless transceiver nodes, the communication between wired base stations do not rely on traditional, but by wireless mobile nodes with their neighbors to exchange information, support for dynamic reconfigurable Multi-hop ad hoc networks.

In the case of no central infrastructure, the number of mobile users by the formation of self-organizing multi-hop wireless mobile network, the system is fully distributed, without using constraints, each node not only receives and to send information terminals, but also can act as a router for communication between other nodes, nodes via multi-hop wireless link to communicate.

Ad Hoc AODV protocol is the most commonly used mobile ad hoc networks of a classic on-demand routing protocol (on-demand routing protocol), also known as reactive routing protocol, the node does not save the timely and accurate routing information, the purpose when the source node needs to send packets, the source node in the network initiated the process of route lookup.

Find the route before starting to send packets, the topology and the routing table on demand content is created, its advantage is not periodically broadcast routing information only when needed, before opening the routing process, issue the control signal to establish and maintain paths, which could reduce the cost of establishing and maintaining the path, saving a certain amount of network resources, the drawback is to send data packets, if no go destination routing, the packets need to wait for the time required to establish the route, while the agreement in the path of choice to select only the shortest path routing, without considering the load path on the node size. The result is to increase the routing of blindness, resulting in some of the routing congestion and delays may occur and even data loss and other issues.

Kundala Sandeep et al [6] proposed that Internet of Things (IOT) has provided a promising platform to build powerful vehicular networking systems by leveraging the growing ubiquity of wireless, mobile, and sensor devices. The communication between vehicles and their internal and external environments can be provided by various wireless connectivity's. Such a vehicular networking solution is expected to be the next frontier for automotive revolution and the key to evolution for the next generation intelligent vehicular systems (IVSs).

The challenges and review the state-of-the-art wireless solutions to connect vehicle to sensor, to vehicle, to Internet, and to road infrastructure. The users anticipate new technologies to be embedded in their vehicles for better performance. With rapid growth and development in information and communication technology, connecting automobiles with wireless solution is expected to be the next frontier for automobile revolution.

Vehicular networking will make way for various applications for smart transportation, eco-friendly transportation, road safety (collision detection and avoidance, cooperative driving) and in-vehicle internet access.

Noble et al [1] proposed that, many applications are built on broadcast communications, so efficient routing methods are critical for their success. The Distribution-Adaptive Distance with Channel Quality (DADCQ) protocol to address this need and show that it performs well compared to several existing multihop broadcast proposals. The high cost aggravates the inherent resource constraint problem in MANETs particularly in multimedia wireless applications. An Anonymous Location-based Efficient Routing protocol (ALERT). It is also called Reliable Application Level Broadcasting (RALB) protocol. RALB dynamically dividers the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no traceable anonymous route. RALB is for the protection to sources, destinations, and routes. RALB has policies to successfully counter intersection and timing attacks. The theoretically analyze RALB for anonymity and efficiency. RALB achieves similar routing effectiveness to the GPSR geographical routing protocol. The DADCQ protocol utilizes the distance method to select advancing nodes. The performance of this method be contingent heavily on the value of the result threshold, but it is difficult to choose a value that results in good performance crossways all scenarios. An anonymous communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field Node density, spatial distribution pattern, and wireless channel quality all touch the optimum value. The node recognizes its neighbor as a node that inside the node's radio range. Once the source need to send a packet, it usually stores the position of the destination in the packet header which will help in promoting the packet to the destination without needs to route discovery, route maintenance, or even alertness of the network topology.

III. PROPOSED SYSTEM

A VANET typically consists of vehicles and properly distributed roadside units (RSUs). A vehicle can send/receive safety-related messages (e.g., speed, location, dangerous road conditions) to/from nearby vehicles and RSUs. These messages reduce the drivers' risk of having an accident and help them manage small emergencies.

It is essential to ensure that the safety-related messages are authenticated, non-reputable and unmodified. Otherwise, a vehicle could send fraudulent messages for its own error, other vehicles to launch attacks without being caught. Vehicle privacy is also a critical concern. In VANETs, a vehicular message usually contains information on a vehicle's speed, location, direction, etc. From those messages, a lot of private information about the driver can be inferred.

- Emergency message generation and passing
- Connecting to Microcontroller (IOT)

The scenario was created using the node placed along the side of road to make a wireless transmission. The nodes are used to created a road structure to show it as wireless network, the node is covered by square to differentiate it. Because wired connection is not possible for highways. In cities and other some developed towns the wired connections are possible, for highways are not possible. So we moved to wireless connection. The RSU's are placed along the sides of the road; the size and structure of RSU are differentiated by a hexagonal structure. At first the colour of the RSU is sky blue, when it is changed as authorised RSU, then its colour is green. Other VANET's in the road is visible as green colour node.

The entire vehicles are moving in the road using the VANET at that time they communicate with the Road Side Unit (RSU). The VANET information is checked by RSU and that is transfer to other RSU. At first the node colour is blue, it is the starting node in the road, it need to reach the destination given. When the node moves from the starting position its

colour is changed to green as other VANET's. The shortest path for that vehicle is displayed by highlighting the nodes placed along the sides of the road. It is like map indicating by blue colour segment of nodes.

When an accident is occurred, that VANET arise a emergency message, the RSU which is near to accident place will receive the signal from the accident node. That RSU will change as authorised RSU. Authorised RSU will transfer the message between the other VANETs and RSU devices, then that message transferred to microcontroller by RSU, when a signal is received then the lane is closed. Then the other way to reach the destination is mapped. Then other VANET's also able to choose their different way to reach their destination from the map. After that emergency measures can be taken to them. The accident place can be located using the RSU location. When a cleared message is received then the lane is opened it is planned as an future work.

A vehicle should be authenticated before it can issue a navigation query. On the other hand, an RSU (vehicle) is able to verify that a message is indeed sent and signed by a certain vehicle (RSU) without being modified by anyone. The real identity of a vehicle should be kept anonymous from other vehicles as well as from RSUs and a third-party should not be able to reveal a vehicle's real identity by analyzing multiple messages sent by it. Although a vehicle's real identity should be hidden from other vehicles and RSUs, TA should have the ability to obtain a vehicle's real identity so That the vehicle can be charged for using the navigation service. Also TA has the role to maintain liability via non repudiation property of messages when accidents happen on the road.

The VANET sends the emergency alert to nearest RSU, then the RSU becomes authorized RSU, it sends the signal to other VANETs and to the IOT receiver. When a signal is received then the lane is closed.

IV. ALGORITHM

Before that the message is transferred to other VANET and RSU the communication are made. When an accident is occurred the message is transferred to the nearest RSU. Then the message is validated, after the validation the RSU becomes authorized RSU. The message is sent to the first VANET node, and then it is passed to other VANETs. Then that RSU sends the message signal to the microcontroller. When a emergency message signal is arise then that corresponding lane is closed.

.

A. Proposed system block diagram

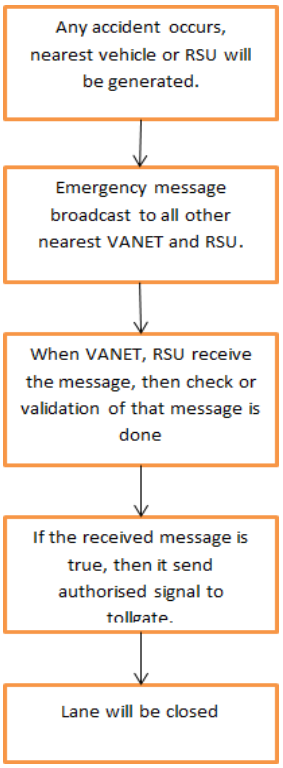

Fig.1. Proposed system block diagram

B. Forward Algorithm

When an accident is occurred, the vehicle sends the message to nearest RSU and VANET. When the message is true , the RSU send the signal to first VANET, then it will passed to other VANETs. The message will be forwarded to other VANET to change the route.

V. EXPERIMENTAL RESULT AND DISCUSSION

The proposed system adopts some security primitives in a nontrivial way to provide a number of features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity. 3) Information provided by RSUs can be properly authenticated before the route is actually being used.

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. Privacy is preserved using the idea of pseudo identity. At the same time, the

vehicle's real identity can be traced if necessary. Navigation queries and results are protected to preserve user's confidentiality and operator's profit. One's real identity and navigation query are completely delinked using the idea of anonymous credential. Information provided by RSUs can be properly authenticated in an efficient way. The nodes are created with the help of NS 2.34 version and the RSU are chosen from 3 nodes so that the requests from every vehicle are obtained.

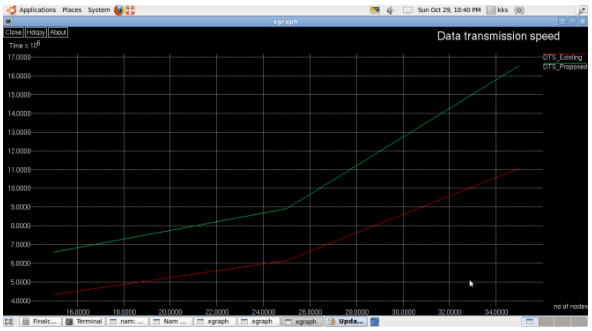

Fig.2.Data Transmission Speed

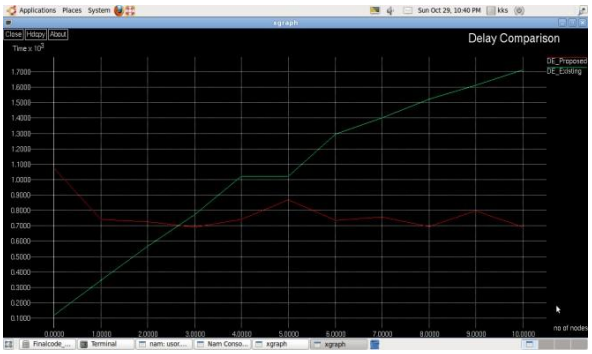

Fig.3.Dela y Compariso n

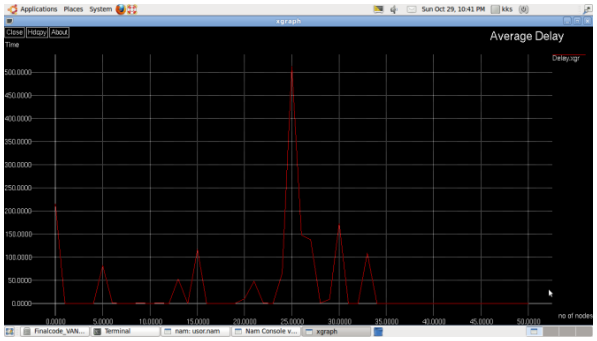

Fig.4.Average Delay

VI. CONCLUSION

A vehicular ad hoc network (VANET) uses cars as Vehicular nodes in a MANET to create a vehicular network. It is an important element of the Intelligent Transportation Systems (ITSs).In a typical VANET, each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority and maybe some other application servers are installed in the back end. A VANET can also be interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications.

In results this centralized approach is scalable, especially for large cities. Our scheme on a test bed to further verify its performance is implemented and also achieves data transfer in an efficient way to decrease packet loss and delay and increase the reliability of VANETs. RSUs at the intersections send the determined communication parameters to the vehicles stopped before the red traffic lights to reduce communication collisions and other traffic. The proposed strategy significantly improves the delay, throughput, and packet loss ratio in comparison with other control strategies using the proposed AODV protocol strategy. When an emergency message is arises, the nearest RSU becomes authorized RSUs, it send the signal to IOT receiver to close the lane. Vehicle accident location can be traced using the location of authorized RSU

REFERENCES

[1] A. Noble Mary Juliet, Dr.M.L.Valarmathi, Joan Pavithra, *"Data Redundancy with Location-Based Detection Scheme for Detecting Attacks in VANET"* , Australian Journal of Basic and Applied Sciences ISSN:1991-8178,) July 2014, Pages: 343-348.

[2] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, *"An efficient identitybased batch verification scheme for vehicular sensor networks*," inProc. IEEE INFOCOM, 2008, pp. 246–250.

[3] F. Qu, Z. Wu, F. Wang, and W. Cho, *"A security and privacy review of VANETs,"* IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2958–2996, Dec. 2015.

[4] IEEE *Trial-Use Standard for Wireless Access in Vehicular EnvironmentsSecurity Services for Applications and Management Messages*, IEEE Std.1609.2-2013. [Online]. Available: https://standards.ieee.org/findstds/ standard/1609.2-2013.html

[5] J. Li, H. Lu, and M. Guizani, *"ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs,"* IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938–948, 2015.

[6] Kundala Sandeep,Abishek "*Vehicular Networking using IOT*", International journal of advances in electronics and computer sciences ISSN:2393-2835 .

[7] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, *"Privacypreserving vehicular communication authentication with hierarchical aggregation and fast response,"* IEEE Transfer Computation., to be published, doi: 10.1109/TC.2015.2485225.

[8] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, *"A*

scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[9] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, *"APPA: Aggregate privacy-preserving authentication in vehicularad hocnetworks,"* inProc. ISC, 2011, pp. 293–308.

[10] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, *"Practical secure and privacy-preserving scheme for value-added applications in VANETs,"* Comput. Commun., vol. 71, no. 2015, pp. 50–60, Nov. 2015.

[11] [11] S. Vijayakumar , A. Noble Mary Juliet , Dr. M.L.Valarmathi, "*A reliable application level broadcasting protocol for vanet"*, IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1288 – 1294

[12] M. Raya and J. Hubaux, *"Securing vehicularad hoc networks,"* J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.

[13] M. Raya and J. Hubaux, *"The security of vehicularad hocnetworks*," in Proc. SASN, 2005, pp. 11–21.

[14] P. Golle, D. Greene, and J. Staddon*,"Detecting and correcting malicious data in VANETs,"* inProc. VANET, 2004, pp. 29–37.

[15] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, *"Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,"* IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[16] Sheng Liu, Yang Yang, Weixing Wang, " *Research of AODV Routing Protocol for Ad Hoc Networks*", 2013 AASRI Conference on Parallel and Distributed Computing and Systems, AASRI Procedia 5 (2013) 21 – 31.

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

[18] X. Wen, L. Shao, Y. Xue, and W. Fang*, "A rapid learning algorithm for vehicle classification,"* Inf. Sci., vol. 295, no. 2015, pp. 395–406, 2015.

[19] X. Zhu, S. Jiang, L. Wang, and H. Li, *"Efficient privacy-preserving authentication for vehicular ad hocnetworks,"* IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 907–919, Feb. 2014.

[20] Zhu Qiankun, Xu Tingxue, Zhou Hongqing, "*A Mobile Ad Hoc Networks Algorithm Improved AODV Protocol,* " 2011 International Conferenceon Power Electronics and Engineering Application (PEEA 2011).