IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 10, October 2020, ||Series -I|| PP 37-44

Self-assured Vehicle Communication System in Vehicular Ad Hoc Networks

Majji Raghurama krishna[1],Vasantha Murali Krishna[2]
#1. M.Tech (CSE) and Department of Computer Science Engineering,Avanthi Institute of Engineering &Technology, Visakhapatnam,
#2. Associate Professor, Department of Computer Science and Engineering,Avanthi Institute of Engineering &Technology, Visakhapatnam,
Received 30 September 2020; Accepted 13 October 2020

ABSTRACT:
Vehicular adhoc networks (VANETs) is the present innovation utilizing as a part of vehicles like cars and vans. Vehicles are considered as nodes in a MANET to make a versatile system likewise the most imperative applications for VANET is the dispersion of dynamic security messages to enhance wellbeing. In these system the Vehicle-to-vehicle (V2V) correspondences needs more secure transmission of information to the vehicles. The chart hypothesis used to devise the issue of agreeable correspondences planning and decrease the intricacy in the systems. The planning plan to allocate both vehicle-to-framework (V2I) and V2V joins for both single-bounce and double barrier interchanges. Vanets are the aftereffect of the imagined Smart Transportation Systems. It permits different vehicles to communicate with one another and structure system. Vanet is one application in which specially appointed systems are utilized at their maximum capacity. In vanets vehicles can get to store and course information to each other.
KEYWORDS: cooperative communications, vehicular networks, Vehicle-to-vehicle (V2V)communications.

I. INTRODUCTION

VANET-Vehicular networks is liable to create in the forthcoming years and subsequently turn into the most relevant type of specially appointed systems. Vehicular Ad hoc Network (VANET) comprises of the basic components of Intelligent Transportation System (ITS) in which vehicles are masterminded with a few short-range and medium-range remote correspondences. In VANET two kind's correspondence are conceivable. One is vehicle-to-vehicle (V-2-V) correspondence; the other is roadside-to-vehicle interchanges (V-2-R).By V-2-V correspondence, individuals can acquire more data and utilize the common data to enhance street wellbeing. By V-2-R correspondence, individuals can speak with RSU to get to web for downloading and upgrading documents or ask neighborhood area data. In this way, contrasted and the conventional unadulterated foundation based system, the half breed of V-2-V and V-2-R correspondences is promising since it can not just beat the drawbacks of base based system, however can likewise conquer the hindrance of non-framework based system.

As of late, VANETs-vehicular specially appointed systems have increased much consideration in the realm of autos and Research. One reason is enthusiasm for an expanding number of utilizations intended for wellbeing of travelers, for example, automobile overload recognition and agreeable driving furthermore for crisis braking, As well as in applications for the solace of travelers like diversions, talk rooms and dissemination of vehicle information (egCarTorrent). The expanded utilization of programming has influenced the car insurance costs, as well as made most hard to auto repairs. Information downloading is a handy and conspicuous application in VANETs-vehicular specially appointed systems, which can convey solace and diversion to clients. In information downloading, vehicles send administration solicitations and afterward get the information stream from the current or the following roadside units (RSU). In the downloading application, the measure of information a vehicle can download at a drive-through of a RSU is extremely constrained because of the short association time. Agreeable download is a promising plan in which vehicles download the information when gone through a RSU and after that share information when going outside the interchanges' extent of RSU. In this manner, the aggregate sum of information that can download a specific vehicle will increment. A key issue in agreeable download is the means by which vehicles offer information with others. There are some current studies on information trade in VANETs [1]. In any case, existing trade conventions are constrained to issues of medium access control (MAC) layer of the crashes, restricted pertinence to numerous information trade units, and there is no surety of receipt of complete information.

We propose an application layer convention for information trade with the supposition that every vehicle knows the positions of the own and neighboring vehicles (which can be gotten through worldwide situating framework (GPS) and related security messages transmitted frequently by neighboring vehicles [2]). In the proposed convention, vehicles utilized for coordination channel to facilitate hand-off transmissions in

VANETs for information trade in light of GPS vehicle area. With such agreeable trade, crashes and MAC layer shrouded terminal impact can be stayed away from in the information channel. Moreover, Design a sleek determination of hand-off vehicles component for the space between the two RSU can be totally misused for information trade. A noticeable element of the proposition trade convention is that it can guarantee the information's receipt for every candidate vehicle pass a RSU. Security is additionally discriminating issue. A vehicular impromptu system (VANET) utilizes autos as nodes as a part of a MANET to make a versatile system. A VANET makes each taking an interest auto into a remote switch or an imparting hub. It permits autos which are almost 100 to 300 meters of one another to associate and, make a system with a vast reach. At the point when a solitary auto drops out of the system, different autos can join in, in this manner uniting vehicles to each other so that a portable web is made. Auto to roadside correspondence is in light of a WLAN (IEEE 802.11p) stage grew especially for the vehicles. In VANETs, the vehicles for the most part move really quick which prompts short vehicle to vehicle availability time. Along these lines, introducing RSU at the vital spots in an arranged way is likewise imperative. Vehicular systems are the imagine of shrewd transportation framework (ITS) in which vehicles speak with one another by means of entomb vehicle correspondence (IVC) furthermore with roadside base station

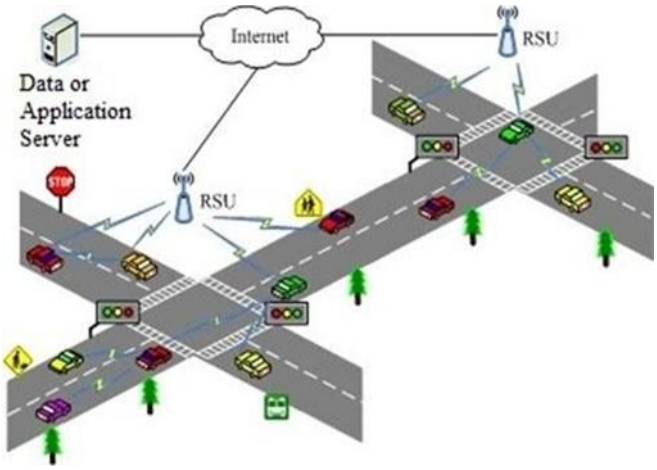

Fig.: VANET (Vehicular Network)

II. SECURITYOFVEHICULAR COMMUNICATION

Vehicular systems have many characteristics that is different from mobile systems and computer networks connected to the Internet. Vehicular applications are divided into two types. The first type includes application that is related to security and driving processes. The main purpose of this type of application is to reduce the number of traffic accident and to solve the problem of congestion on road and highway. In [5], traffic congestions are formed by many factors; some are (somehow) predictable like road construction, rush hour or bottle-necks and some are unpredictable like accidents, weather and human behavior. Drivers, unaware of congestion ahead eventually join it and increase the severity of it. The more severe the congestion is, the more time it will take to clear once the cause of it is eliminated. The second type is mainly focused on ensuring comfort for the driver and the passengers while travelling. For example, access to the information (i.e. Internet, music, films and etc.).

VANETs will combine a variety of wireless technologies like DSR (Dedicated Short Range) communications described in the draft of standard for VANETs IEEE 802.11p WAVE (Wireless for Access Vehicular Environments), with Cellular, Satellite and WiMAX technologies in new future. Such a device allows the node to receive and send messages through the network.

Roads have been always in dangerous and a lot of efforts have been undertaken to improve their safety. Vehicles, road signs have been improved throughout generations. New solutions are available to assist the driver in hazardous situations and to decrease road dangers. In a near future, vehicles will be equipped with wireless devices, so that can communicate with each other. The primary application of this technology is to let vehicles exchange about their current context. The information exchanged can be divided into two types, (1) periodic exchange of status messages among the vehicles in direct communication range and (2) safety messages triggered by a critical event and distributed in a geographical region. Typically, WSN technologies help where neither the vehicle's sensors nor the driver can detect the danger, e.g. very localized road condition, animal crossing the road out of a forest, and etc. Hence, it is either the driver or the vehicle itself could initiate appropriate reactions according to the current environmental conditions with the overall aim to increase the driver's safety.

A combined scenario of WSN and VANET architecture aims at the provisioning of two services:
1. Accident prevention, 2. Post-accident investigation.
1) Accident prevention: It retrieves environmental data collected by the roadside sensors, when a car passes on road by sensor network. Data can be processed within the WSN network, in order to higher level information. Data can contain various physical quantities, such as temperature, light and humidity, and also detect moving obstacles. This information is potentially displayed to the driver and is processed in OBU vehicles. Wireless sensor nodes can measure road conditions data more than accurately an on-board sensor. Once a vehicle has processed the sensor data, it may translate the data as a risky situation and send a safety warning message to neighboring nodes. The vehicle finds a geographical region defined by geometric shape and scattered the messages to neighbor vehicles.
2) Post-accident investigation: Sensor nodes measured continuously and environmental data are stored. These data contains the collected quantities (e.g. temperature) and event data also, such that previously detected obstacles. This information stored over a long time period may interest for a team of forensic.

III. APPLICATIONS OF VANET

The applications of vanet can be broadly classified as follows

A. Real time Traffic Information's:

The network should be able to provide real time traffic alerts and information on traffic conditions on roads ahead. This can be done by actively collecting and storing location information of various vehicles on a particular area and storing it on the RSU. When other vehicles approaching the same area requests this information, it can be directly provided from the RSU to that particular vehicle requesting it.

B. Active Prediction and Traffic Alerts:

This application can be used to promptly broadcast the traffic information priory to the vehicles before they reach the congested areas on the road.

C. Cooperative Data Sharing:

When a car on the road suddenly hard brakes, the information should be relayed and transferred to all the vehicles behind the particular vehicle and the information should be delay sensitive.

D. Commercial Applications:

The vehicular network can be used to provide business based or commercial data to the vehicles such as real time video streaming from the cloud, internet access, on demand entertainment services, etc.

E. Real Time Map Generation:

The drivers can request the real time maps of the regions which they area about to travel prior to overtaking it.

F. Real Time Data Relay:

This is especially for normal people travelling in the vehicles connected to the vanet. They will be able to transfer or relay real time data such as live video calls, data transfer and share files across vehicles of their choice while on the move.

G. Advertising:

This can be effectively used to provide live ads to the customers who are on the move. For example, when a vehicle moves across a motel, restaurant or a movie theatre, the business people can use this technology to provide ads to the vehicles about their enterprise so as to effectively attract customers.

H. Vehicle Registration & Regulation:

This system can be used to effectively register and save information on number of vehicles crossing a particular area without the requirement for the vehicle to be stopped and have to register automatically.

I. Toll Collection:

Payments in toll can be done electronically at certain collection points [4]. It is beneficial to both the traverllers and the toll operators.

IV. Attacks on VANET Network

- **Denial of Service Attack:** DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplus data.
- **Broadcast Tampering:** An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.
- **Malware:** The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.

- **Spamming:** The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralized administration.
- **Black Hole Attack:** A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages. Alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:
- **Masquerading:** Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.
- **Replay Attack:** In a replay attack the attacker re injects previously received packets back into the network, poisoning a node's location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.
- **Global Positioning System (GPS) Spoofing:** The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.
- **Tunneling:** An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.
- **Position Faking:** Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.
- **Message Tampering:** A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.
- **Message Suppression/Fabrication/Alteration:** In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.
- **Key and/or Certificate Replication:** Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle's identity across several other vehicles. The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.

V. SYSTEM ARCHITECTURE

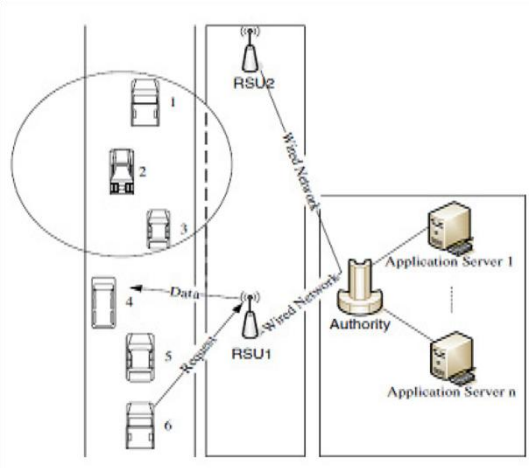

Figure: System Architecture

Applicant vehicle download the data from the application server via RSU. Initially applicant vehicle send request for data to RSU, then RSU will forward that request to authority. Authority is responsible for selection of downloading vehicle based on geographic information and also check the identity of the vehicle

whether it is valid to purchase the data or not from application server. If vehicle is valid to purchase the data then it will download the data from the server and that will send to RSU. Finally RSU sends data to the Applicant vehicle.

The application authority and application servers: These are responsible for the management and provision of service data, respectively. The authority knows all the keys and is in charge of programming service. They can be kept either by the authority or third party operators.

Road side infrastructure: Consisting of RSUs deployed at the edges of the roads that are responsible for forwarding request and response. RSUs communicate with authority via wired network. Nodes: These are ordinary vehicles on the street and highway road that can communicate with each other and RSUs through radio.

VI. PROPOSED SCHEME

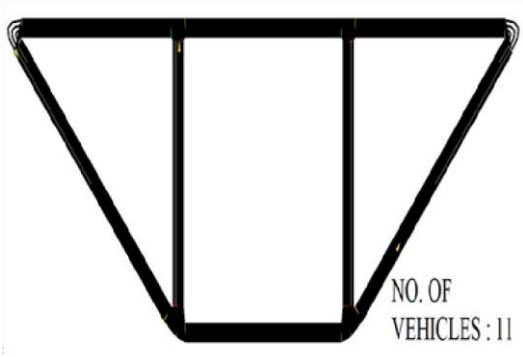

Fig.: Road Structure & Number Of vehicles

A. System Model:

Consider a one-dimensional road and choose one segment of the road, which is a straight line as,

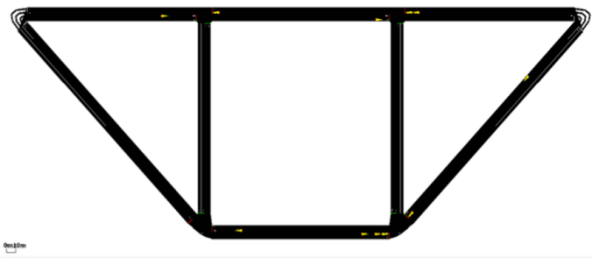

Fig.: VANET Network design

The Vehicles are distributed as poisson points over the road segment. That is, given that there are k vehicles, they are independent and uniformly distributed over a initially. We are interested in a network scenario on highways or rural areas, where the vehicle density (defined as the average number of vehicles per unit road length) is low enough to have disrupted vehicle-to vehicle and vehicle-to-RSU connectivity. With a high vehicle density, a multihop end-to-end path can be found between a vehicle and an RSU with a high probability. Also, we do not consider the case where no packet relaying is possible (i.e, data packets will be carried by their originator vehicle till it meets the RSU) since wireless communication has no significant role in the packet delivery delay in such a case. This may happen either when the vehicle density is extremely low and/or the number of RSUs covering the road is fairly large. Although an RSU can receive packets from the vehicles heading toward the RSU or moving away from it, we consider only one direction in packet transmission, as considering both directions (i) does not constitute a significant difference in the analysis, and (ii) is difficult to implement as a vehicle needs to know the location of the RSU and its own location (otherwise it may not be able to know when to switch its transmission to the RSU ahead of it).

Here, we do not consider packet relaying via vehicles moving in the opposite direction. The reason is that it makes packet transmission subject to severe physical channel impairments, which are very significant due to the high relative speed between two vehicles moving in the opposite directions. In addition, the meeting time between two vehicles moving in the opposite directions may not be enough for transmitting a significant number of packets unless the available bandwidth is very large. The vehicles can upload data from RSU when they are in range of RSU. Usually the RSU maintains non-preemptive scheduling in which one service cannot be interrupted until it gets completed. The communication takes place with the help of the wireless channel and the vehicle which wants to access data from RSU sends a request which consists of the vehicle number, identifier of the requested data and the operation that vehicle can do. The RSU then serves the request as per the scheduling

algorithm provided to it and removes the request from the queue. Each request from each vehicle has it own timeout amount after which the request will be dropped if not processed.

B. Cooperative Data Downloading:

Firstly the vehicles are identified for their types as follows,

- Requestors: These are vehicles that request the data at the first place.
- Receiving vehicles: These are vehicles that actually receive or download the data from the RSU.
- Intermediate vehicles: These are vehicles that act as a relay towards delivering the data to the requestors. These vehicles use the store and forward[20] mechanism to deliver data to the vehicles which are out of range of communication from the RSU.

C. Prioritization of Message Data:

We analyse the messages and the messages classify them in to categories based on priority, timeout, message size and the order in which the request was received. Then based on our proposed scheme we use a scheduling algorithm based on the application or as an on demand request from the following.

- Data with Small Short Deadline: In this the request which is most urgent will be processed first.
- Very Small Data First: In this the request wills the data of smallest size will be processed first.
- Priority Based on Request Order: The request that arrived early will be processed first.

D. Performance Evaluation:

We use the following performance metrics to evaluate the performance of different on-demand scheduling algorithms in our model. *1) Deadline Miss Rate:*

It measures the percentage of missed requests to the total number of requests received by the RSU. If the deadline miss rate is low, it means scheduling algorithm is better.

2) Throughput:

Throughput is the number of requests successfully processed by a RSU in unit time. Hence, many requests will be served concurrently, when the scheduler broadcasts the most popular data item and throughput increased. High throughput means better system performance.

3) Full Response Time:

The average response time of a RSU on receiving a request.

Low average response time initiates system is improvement.

E. Algorithm for Shortest Data First and Priority based on Request Order Schemes:

Our aim is to schedule the maximum number of vehicles in the scheduling. With the help of scheduling schemes we can reduce the turn-around time of a process while increasing the throughput. We are also able to maintain the congestion control which helps in controlling the delay of the request. Our proposed method has reduced the congestion and delay control of the data. The CCH channel is congested if the packet queue of the beacon message exceed the define threshold value so that is why we assign the priority to the message and these message according to their priority. Highest priority is given to immediate message and after sending the immediate message we will send the urgent message and then after the information message. By sending these messages according to their priority we can control the congestion and delay of the data.

VII. VII.CONCLUSION

The project provides a more comprehensive set of methods for VANETs. This method satisfies all security requirements for VANETs. This project provides two secure and privacy enhancing communications schemes for VANETs to handle ad hoc messages and group messages for inter-vehicle communications. In terms of effectiveness, this project gives a solution of lower message overhead. In this project, bloom filter and binary search techniques are used for RSU message verification and reduction of message overhead. This project first provides a group communication protocol to allow vehicles to form a group and communicate securely. The scheme is used to communicate vehicles in the same group without RSU. This scheme is used for vehicles to send and receive messages more securely and confidentially. All of these techniques have their pros and cons. In this paper we argue that future localization systems for VANets are likely to use some kind of Data Fusion technique in order to provide position information for vehicles that is accurate and robust enough to be applied in VANet critical applications. We then show how Data Fusion techniques can be used to compute an accurate position based on a number of relatively inaccurate position estimations. By using graph theory the scheduling problem in the dual-hop communications for vehicular networks has been identified .Due to the channel variation and mobility of VE(vehicle equipment), the dual-hop network topology is time-varying, which can be modeled as a spanning tree based on the V2I and V2V links. The extensive literature reviewed in this paper, has indicated that capable to achieve better fairness among VE and can noticeably enhance the date rate of the VE with poor channel conditions also the cooperative communications are able of improving the throughput which makes the system low complexity.

It can give safety message to the other vehicle so millions of human life can be saved. To use VANET in daily day to day life, there are different protocols are available, which can provide security to this technology. Different protocols are available to address the security issues, all protocols have their advantage and disadvantage which can handle security related problems. These protocols provide security against above mention security threats.

REFERENCES

[1]. Srivastava. D and A.Arawak, "Traffic Congestion Detection in Vehicular ad hoc Networks Using GPS," e-ISSN: 22700661, p-ISSN: 2278-8727,vol. 16, issues 2, ver. 1, pp. 6369, Mar-Apr. 2014.
[2]. S. Bahrati and Zhuang, "CAH-MAC: Cooperative ADHOC MAC for Vehicular Networks," IEEE Communication, vol. 31, no. 9, Sep. 2013.
[3]. Z. Hu and C.-K.Tam, "CC-MAC: Coordinated cooperative MAC for Wireless LANs," Computer Network., vol. 54, no. 4, pp. 618-630. 2010.
[4]. F. Ye, S. Roy, and H. Wang, "Efficient data dissemination in vehicular ad hoc networks," IEEE J. Sel., Areas Communication vol. 30, no. 4, pp. 769–779, May 2012.
[5]. P. Asthana, N. Dhruva, "Design Approach for Cooperative Security in Vehicular Communication System," p-ISSN: 2277-1581, vol. 2, issue no. 10, pp. 1049-1055, Oct. 2013.
[6]. Borgnovo, A. Capone, M. Cesena, and, "ADHOC MAC: New MAC Architecture for Ad Hoc Networks Providing Efficient and Reliable Point-to-Point and Broadcast Services," Wireless Networks, vol. 10, pp. 359-366, 2004.
[7]. Jiang and Luca, "IEEE 802.11p: Towards on International Standard for Wireless Access in Vehicular Environment," Vehicular Technology Conference, May. 2008.
[8]. "VEMAC: A TDMA-based MAC Protocol for Reliable Broadcast in VANETs," IEEE Transaction on Mobile Computing to be published.
[9]. Yong Tang and Yu Cheng, "Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks," IEEE Communication, vol. 31, no. 9, Sep. 2013.
[10]. Miao. Pan, Pan Li, Y. Fang, "Cooperative Communication Aware Link Scheduling for Cognitive Vehicular Networks," IEEE Communication., vol.30, no. 4, May. 2012.
[11]. J. Zhang, Q. Zhang, and W. Jiao, "VC-MAC: A cooperative MAC protocol in vehicular networks," IEEE Trans. Vehicle. Technol., vol. 58, no. 3, pp. 1561–1571, Mar. 2009.
[12]. Fukumoto, Juniya, "Analytic Method for Real-Time Traffic problems by Using Content Oriented Communication in VANETS. 7th International Conference on ITS. 2007, pp. 1-6.
[13]. J.Nzouonta, N. Guiling Wang C., "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information," Vehicular Technology, IEEE Transactions on vol. 58, no. 7, Sept. 2009.

Authors

Majji Raghurama krishna is currently pursuing his 2 year M.tech in Department of CSE at Avanthi Institute of Engineering & Technology,Cherukupalley(p), Near Tagarapuvalasa,Ap 535006. His area of interests are Computer Networking, cloud Computing.

Vasantha Murali Krishna is Currently working as assoc. Professor in Dept of CSE at Avanthi Institute of Engineering & Technology, Cherukupalley (P), Near Tagarapuvalasa,Ap 535006. He has more than 11 yearsofteachingexperienceinvariouscolleges. His area of interest is Machine Learning.

MajjiRaghuramakrishna, et. al. "Self-assured Vehicle Communication System in Vehicular Ad Hoc Networks."*IOSR Journal of Engineering (IOSRJEN)*, 10(10), 2020, pp. 37-44.