INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SPECIAL ISSUE FOR
NATIONAL LEVEL CONFERENCE
"RENEWABLE ENERGY
RESOURCES & IT'S APPLICATION"

ENERGY EFFICIENT IN CONGESTION CONTROL FOR VEHICULAR AD HOC NETWORK

MR. ANAND A. BIHADE, MR. SAGAR S. JANE

Assistant professor, COETA, Akola.

Accepted Date: 12/03/2016; Published Date: 02/04/2016

Abstract: VANETs are the vehicular networks used to connect the vehicles together to share their information with each other in the cluster. They are self-distributed and organized. They can are useful in avoiding accidents and traffic congestion. Providing safety and comfort applications such as information about road block, fuel station, and traffic are main purposes of the VANET. VANET's are highly dynamic and energy consumption in nature, Due to this nature of VANET it is more challenging to achieve the accurate data of vehicle Security and energy consumption are important issues in VANET. Data confidentiality can be achieved by AES algorithm in VANET's. But AES requires more energy for the process of communication between nodes. In this paper we proposed a method sending of important data from one node to another consumption less energy.

Keywords: Vehicular Ad Hoc Network, Road side unit, network traffic analysis.

Corresponding Author: MR. ANAND A.BIHADE

Co Author: MR. SAGAR S. JANE

Access Online On:

www.ijpret.com

How to Cite This Article:

Anand A. Bihade, IJPRET, 2016; Volume 4 (8): 128-134

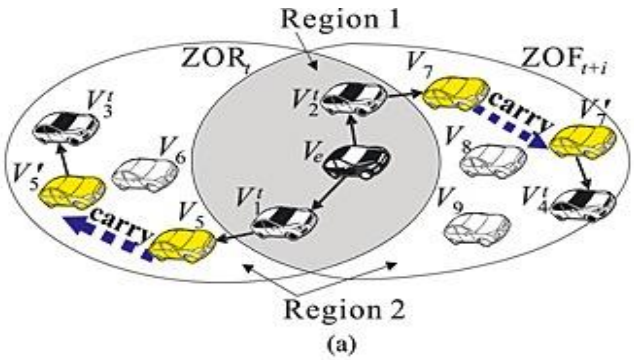
PAPER-QR CODE

INTRODUCTION

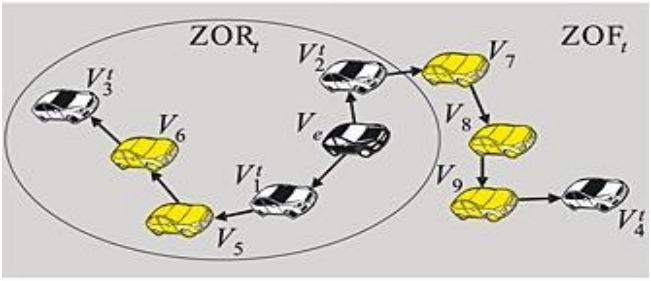
Vehicular ad hoc network (VANET) is consisting of the nodes which are the moving cars is a subclass of the MANET's (Mobile ad hoc network). The VANET infrastructure is varying according to the range of the network. Any node which comes within the range can be a part of the temporary network created by vehicle nodes coming together When the car moves out of the range, they leave the network. It may consist of the large no. Of the nodes (vehicles) which require some authority to govern it. The Road Side Management Unit used to connect the vehicles which are moving on the road when the vehicles use the radio signal to communicate with one another there may be energy consumption . VANET system spread the emergency and traffic information among the vehicles in a timely manner. It is the ad hoc communication in which no wires are required, all the nodes can move freely. VANET networks are ad hoc network in which mobile nodes uses the wireless communication to communicate one another. Vehicular network is also known as the intelligent transportation system in which the two types of the communication may be occurring: 1) vehicle to vehicle communication (V2V) and 2) vehicle to road side communication (V2R) in which the roadside unit broadcast the messages to all other vehicles it is also known as the single hop broadcast. Due to more number of message coming on a certain node which may create flooding of message which may result in lost of message.

Relevance Zone

When certain nodes are gathered together on a road they create a network of sending and receiving data and Relevance zone is created by using dynamic routing protocol can get the congestion information about the traffic and can identify shortest path to get out of the traffic zone. The goal of the VANET system is to build a vehicular communication system to provide the data more quickly for the benefit for the passenger ease, comfort, and safety. The VANET applications are divided into safety and non-safety applications. Safety applications are concern with the human life where as the non-safety applications pleasant with the passengers. [1][3] Examples include travelling map, outdoor car parking etc. For the future road traffic management system the VANET network becomes the necessary component. The reason behind to develop this network is to improve the security, efficiency, safety of the vehicles. One of the advantages of VANET system is that the cost of maintenance and implementation is very low. The Relevance Zone provide complete information of the node entered in the zone the information such as vehicle number conjection in the network root of traveling etc.



(a)

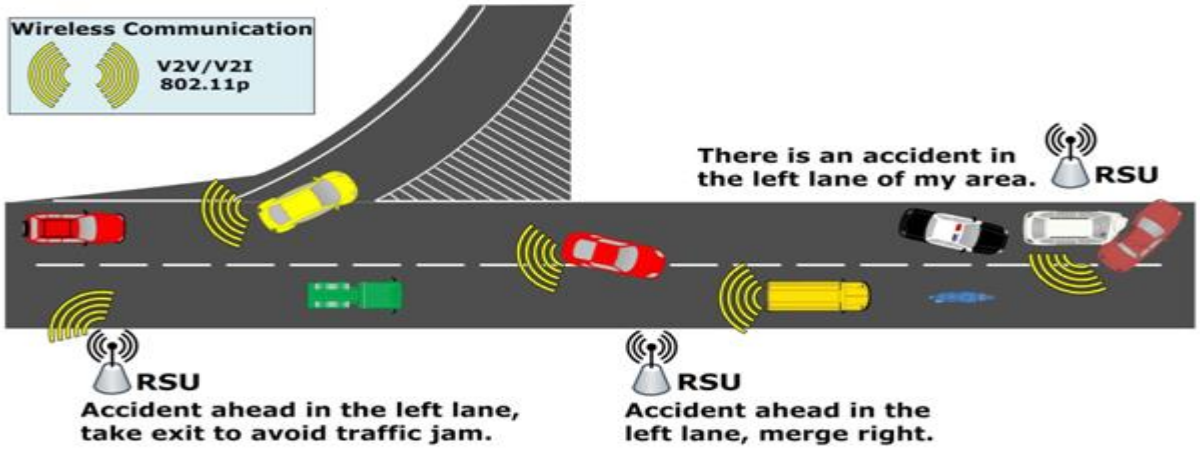


(b)

Relevance Zone

Vehicle which are entered in the network can communicate with each other broadcast of message from one to another is done through sending of data in form of packet.

Dispatch Unit



The routers used for communication called RSU (Road Side Unit), work as a router between vehicles on the highway and connected to other devices. This unit keep track of all the vehicle entered in the network it is also called as central information center Each vehicle has an (On

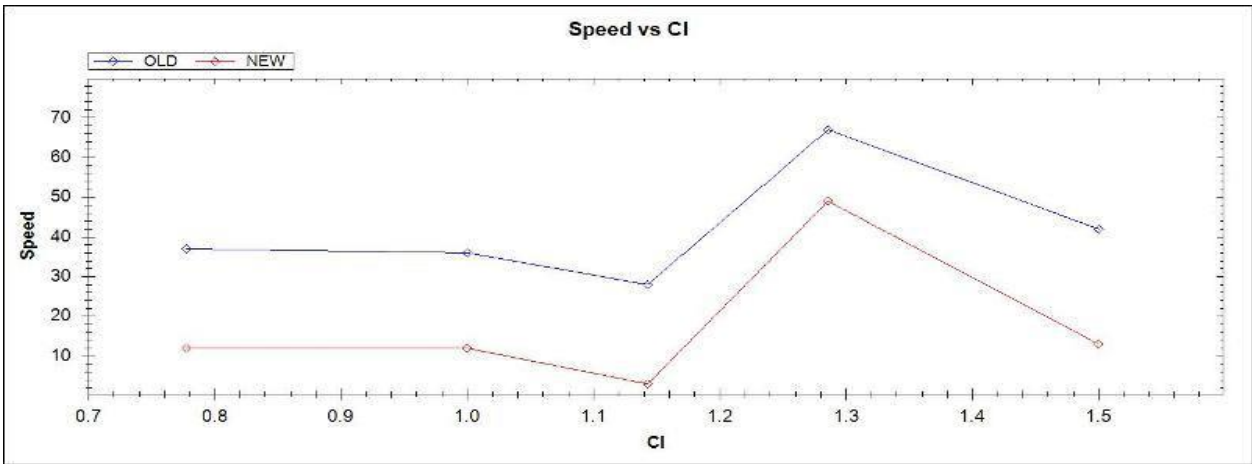
Board Unit), RSU is connected to the vehicle with this unit via DSRC radios. There is an another device called TPD (Temper Proof Device), which holds all the secret information about a vehicle like trip details, route, drivers identity, keys, the speed of vehicle….etc.

HYBRID CONGESTED APPROACH

In this work we considered using adynamic variant of the classical Dijkstra algorithm[for finding the shortest path between a departurepoint to a given destination. In genral one could have used simply classic Dijkstra by replacing the distance matrix with a congestion index matrix and thealgorithm still works since the objective is to find a path with the least distance. However, two reasons led us to modify this classical algorithm to accommodate road traffic requirements. First, unlike

distances which are static parameters for Dijkstra while, a vehicle is driving towards its destination, the least congested itinerary may change dynamically, which requires vehicles to regularly recalculate their itinerary. Second, a least congested itinerary may not be necessary the best one in terms of traveled distance and cost. Therefore, we designed a factor-based formula which encompasses both the metric distance d and the congestion index. By using Dijkstra graph search algorithm the vehicle is been trase by GPS location the information is been hand over to the universal center where all the information

of the vehicle is store .This universal center maintains all the information of all the zone of the relivance.If at any point any congestion is occurring which further aleart the vehicle coming from behind .Which by using the algorithm finds the less congested path. Which depends on the value of Congestion Index(CI)



FLOODING OF BEACON MESSAGES

When number of node increases in the congested network every node send's information to each other and to the Road side unit at some point certain node receives more number of message at the same time which may result in message flooding may also cause loss of valuable information .

Packet Delivery Ratio: It is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. It is calculated by subtracting lost packets from total number of packets and divided by number of packets transmitted. In graph of packet delivery ratio, time (seconds) is taken as X-axis and PDR is taken as Y-axis. Figure 3 shows the PDR of a simulation when data is shared between the several nodes together during the given simulation length.

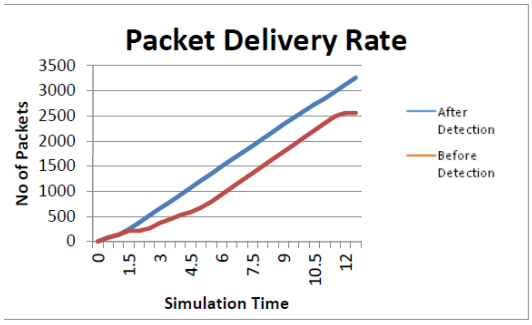


Figure 3: Packet Delivery Rate

Data Loss: The data loss or packet loss is the parameter indicates the data lost during the communication between the two given points within the given simulation. The data loss is increased heavily during the attack hours, which must be prevented by using the security scheme. Our security scheme against the denial of service and distributed denial of service attacks has been evaluated using the data loss parameters also. The total data loss has been nearly 9000 packets in the whole simulation, where hundreds of Mb/s of data has been transferred. The 9000 packets consist only 360,000 bytes of data, when a packet length is generally 40 bytes. The total data consists of only 360 Kb/s, which is nearly 0.01 % of the total data being transferred between the two points.

Network Load: The network load is the parameter which tells the volume of data being processed on a single node during the given time interval. The higher load increases the probability of data loss and higher delay, which comprises the weaker performance of the network. The given network load has been recorded at nearly 3.5 at maximum, which shows the significant reduction in the load during the attack hours using the proposed security model.

Energy Consumption: It is calculated energy is consumed during the packet receive and packet transmit event, during the idle or sleep state and active state of the sensors. The energy is calculated after each interval of 0.5s in the given simulation scenario. Energy consumption is plotted across Y-axis and the simulation time on the X-axis. The energy consumption is the important parameter in the case of wireless sensor nodes. The lifetime of sensor nodes entirely depends upon the battery life which is directly proportional of the volume of data and amount of local processes on the node. The heavy data volumes are the major factor behind the energy consumption of the sensor nodes. The sensor node's energy consumption can be reduced by mitigating the heavy traffic volume by filtering the overflowing attack data from the ingress ports of the network nodes. The energy consumption reduction directly affects the network lifetime and elongates the network lifetime in the direct manner.

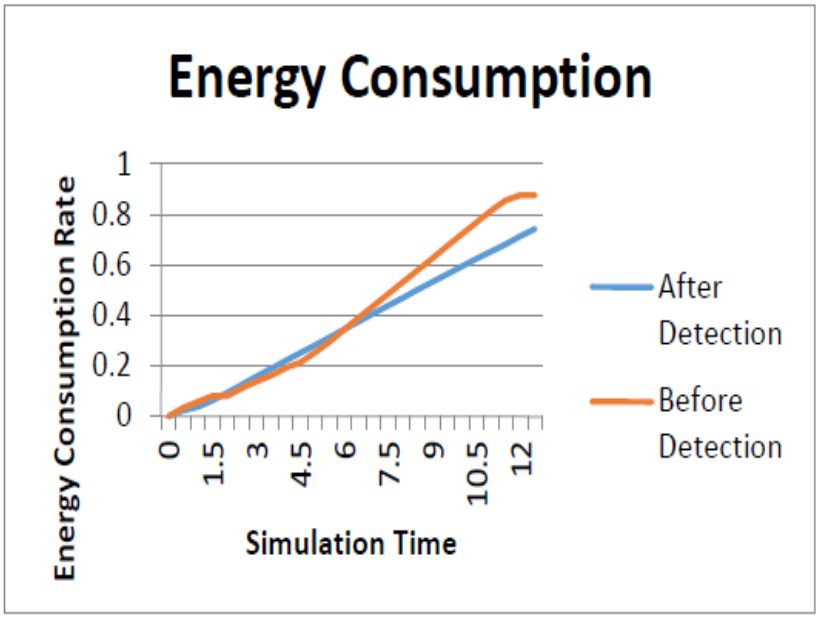


Figure 6: Energy Consumption

CONCLUSION

The proposed model has been made capable of detecting the conjection on the path created due to the vehicular collisions. The proposed model has been enabled with the ability to connect the nodes in the node-to-node and node-to-RSU in order to maximize the vehicular network reach. The proposed model performance has been evaluated on the basis of multiple parameters to judge the network performance. The performance parameters of transmission

delay, network load, packet loss, energy consumption, etc has been evaluated for the performance of the proposed model in the wireless sensor networks.

REFERENCES

1 Javed, Muhammad A., and Jamil Y. Khan. "A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." Australasian Telecommunication Networks and Applications Conference(ATNAC), IEEE, pp. 1-6, 2011.

2 Hung, Chia-Chen, Hope Chan, and EH-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks." Wireless Communications and Networking Conference, IEEE, pp. 2200-2205, 2008.

3 Dias, João A., João N. Isento, Vasco NGJ Soares, FaridFarahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." GLOBECOM Workshops (GC Wkshps),IEEE, pp. 51-55, 2011.

4 Moser, Steffen, Simon Eckert, and Frank Slomka. "An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." Future Generation Communication Technology (FGCT), IEEE, pp. 36-41, 2012.

5 Sumra, Irshad Ahmed, HalabiHasbullah, J. A. Manan, MohsanIftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." 11th International Conference on ITS Telecommunications (ITST), IEEE, pp. 708-714, 2011.

6 Detection and Dissipation ofRoad Traffic Congestion Using Vehicular Communication[1] Abderrahmane Lakas Moumena Cheqfah 2009 IEEE.

7 Distributed or Centralized Traffic Advisory Systems—The Application's Take John S. Otto and Fabi´an E. Bustamante Vehicular Systems By Miguel Sepulcre, Jens Mittag, Paolo Santi, Member IEEE, Hannes Hartenstein, Member IEEE, and Javier Gozalvez, Senior Member IEEE.