IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network Level Performance Enhancement in VANET using wireless Nano sensor

Ganesh Auchar,Uppin Swapnil ,Wagh Prakash

Department of Computer Engineering

TSSM's Padmabhooshan Vasantdada Patil Institute of Technology,

Bavdhan, Pune, India. http://pvpittssm.edu.in

Abstract

Urban areas around the world are populating their streets with Vehicular Ad Hoc Network (VANET) in order to feed incipient smart city IT systems with metropolitan data. In the future smart cities, VANET technology will have a massive presence in the streets, and the operation of municipal services will be based to a great extent on data gathered with this technology. However, from an information security point of view, VANET can have failures and can be the target of many different types of attacks. The ability to route the packet to the next node is the foremost requirements of such vehicular networks. One of the main issues to be addressed in VANET is congestion. When a sudden burst of traffic is detected, the nodes need to forward it towards the destination. The node that is forwarding may also have some packets to be delivered from it. The outgoing packets and transitory packets lead to buffer overflows at a node which in turn lead to packet drops and finally degrades the overall network performance. Congestion control schemes are essential in such situations to increase network performance and ensure a fair use of the resources. This work proposes a congestion control scheme distributed across the transport, network and MAC layers that can detect and avoid congestion in the network. It provides priority based traffic scheduling with a dual queue scheduler which favors transitory packets. When congestion is detected based on the buffer occupancy, source sending rate is updated by the sink periodically with the help of dual queues and route the packets through less congested paths.

1.Introduction

1.1 Background

Vehicular Ad Hoc Networks (VANETs) are special types of networks having high mobility rate of the nodes. Its ultimate goal is to provide various services to the users to make their journey an unforgettable experience. These networks support various services such as access of internet, Intelligent Transport Systems (ITS), online video streaming applications to the users. Users access these services by sitting in the vehicles with the help of internet connectivity. But as the numbers of users increases rapidly, it becomes a challenging task to detect the activities of those in VANETs. The problem becomes more complex due to large variation of mobility and density of the nodes. Nodes pass the information about a particular area to other nodes while moving and exchange the valuable information such as speed of the nodes, position of the nodes, direction of motion of the nodes, data exchange or any other relevant information. This information is exchanged among the vehicles periodic all so that neighboring vehicles can take precautionary measures in case of some emergency on the road.

Security always remains a challenging task in VANETs due to the high mobility of the nodes. While nodes share the information with other nodes, there are chances of leakage of information sent by one node to other. In such a case, we say that nodes are compromised, i.e., the nodes that access the information of the other nodes in an unauthorized manner to breach the confidentiality, integrity and availability are called as intrusions in the network. In view of the above, efficient mechanisms are required for detection of all malicious activities by various nodes in the network. Once nodes are identified which may act as intrusions then several precautionary measures (such as the use of asymmetric key cryptographic solutions can be taken to mitigate the affect of those in VANETs.

As discussed above, most of the existing solutions in literature have used asymmetric key mechanisms for secure communication among the vehicles. The authentication mechanisms provided in these proposals have considered various phases for authentication such as key generation, maintenance and update which generates considerable delay and overhead. Such generated delays degrade the performance of the applications such as video streaming, alert generation in case of emergency or mission critical applications. Hence a novel intelligent mechanism is required which not only detects intrusion in the network but also provides the way to overcome the same. The mechanism should detect the intrusion without causing much overhead in VANETs.

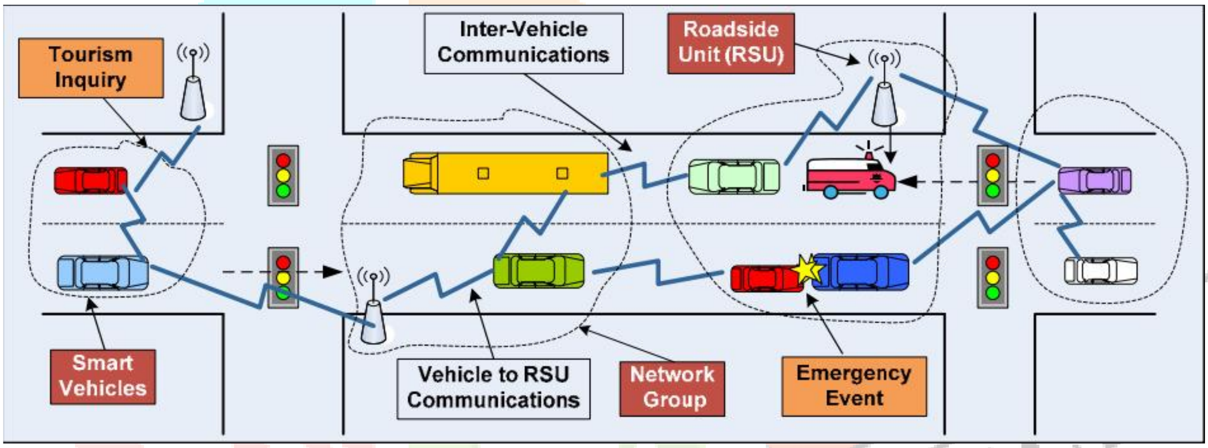


Figure 1. A basic structure of VANETs

1.2 Characteristics of VANET:

The feature of VANET mostly resembles the operation technology of MANET in the sense that the process of self-organization, self-management, low bandwidth and shared radio transmission criteria remain same. But the key hindrance in operation of VANET comes from the high speed and uncertain mobility of the mobile nodes (vehicles) along the paths. Moreover, VANETs have unique attractive features over VANETs as follows:

- Higher transmission power and storage: The network nodes (vehicles) in VANETs are usually equipped with higher power and storage than those in MANETs.
- Higher computational capability: Operating vehicles can afford higher computing, communication and sensing capabilities than MANETs.
- Predictable Mobility: Unlike MANETs, the movement of the network nodes in a VANET can be predicted because they move on a road network. If the current velocity and road trajectory information are known, then the future position of the vehicle can be predicted.

1.3 Working procedure of VANET

VANET security is an important issue. Periodically exchanged safety packets might have prominent consequences on VANET applications such as preventing collisions of vehicles. In Sybil attack, a single attacker node plays the role of multiple nodes of VANET by impersonating their identities (IDs) or claiming fake IDs. In this way, a Sybil attacker creates an illusion of existence of multiple nodes in the network. Legitimate nodes are deceived in believing that they have many neighboring nodes around. In Sybil attack, an attacker can take over the control of whole VANET system and inject false information in the network, forcing other vehicles and vehicular authorities to take incorrect decisions. Attacker can impact the data consistency of the system. It comprises of a gathering of self-ruling nodes that are spatially differentiated and are integrated with sensors that helpfully monitor physical and natural conditions. Such systems find expanding utilization in assorted territories like over-taking, speed control and so forth. A local VANET may comprise of tens or hundreds of nodes scattered in an area. When an event is detected, there is a sudden outburst of data .The data generated by the nodes increases and the offered load exceeds available capacity and the network becomes congested. Congestion in the network can be transitory (link level congestion) or persistent(node level congestion). Transitory congestion is mainly due to over flow of a link, as a result of the burst of packets arriving at the switch or router buffer. It occurs as a result of link variations. Persistent or sustained congestion happens when the long term arrival rate at a link exceeds its capacity. This happens when data sending rate from the source increases and the buffer over flows whereas, transient congestion solely introduces a delay in data transmission, and persistent congestion leads to data loss. Congestion ends up in packet dropping, delays, exaggerated throughput, and wastage of communication resources, power, and eventually decreases the life span of the network. Congestion control involves several strategies for monitoring and regulating the quantity of data entering the network to keep traffic levels at a suitable level.

In VANET, congestion control has an affluent history of algorithm development and theoretical study. Varied schemes for congestion control have been projected and enforced over the years. The existing works differ in the algorithms they use for adjusting the sending rate from source and techniques to deal with transient congestion like dropping packets or using back pressure mechanism that mitigates the rate of links feeding the congested buffer. They are classified based on whether to follow a traditional stratified approach or cross layer approach.

In Recent years, research is done rapidly and effectively in area of mobile computing. After long research in ad-hoc networking and mobile computing Mobility of node is still challenge in front of researchers. A mobile ad hoc network consists of two things one is mobile hosts or node and another one is wireless links. Due to mobility of devices or host, the topology of the network always changes and that change is not uniform. Change of node's position is random and wireless links break down and reestablish frequently. Collectively we can say that, an adhoc network operates in the absence of fixed infrastructure forcing the node to organize the exchange of information. A prominent type of mobile ad hoc networks is direct wireless communication between vehicles in road traffic. In this network, the vehicles are equipped with a computer controlled radio modem allowing them to contact other equipped vehicles in their vicinity. This type of network is named Vehicular Ad hoc Network (VANET).We believe that the best applications of inter-vehicle communication are to provide improved comfort and additional safety in driving. Most of safety applications require dissemination of information among participating vehicles, so broadcasting is one of fundamental services in these networks, which because of high importance of exchanged messages especially in safety applications require high reliability in delivering messages.

[1] According to [2] more than 30% of all accidents happen at intersections so broadcasting in intersection requires high reliability. But at intersections, communication range of a vehicle in one road may cover some vehicles in another road and so, broadcasting of vehicles in one road can affect broadcasting of vehicles in other roads that according to current broadcast mechanisms this communication range overlap results in cancelling broadcast in some directions. In this paper we demonstrate this problem and present a broadcast

method that overcomes it. In the proposed method by classifying vehicles based on their location to the last forwarder of message, we distinct between vehicles in different roads constitutes intersection and omit effect of broadcasting of vehicles in different roads on each other.

VANET as comfort communication can be made by two means: Periodic Safety Message (in this paper we refer them as Beacon) and Event Driven Message (refereed as Emergency Message here), both messages share only one control channel. The Beacon messages are messages about status of sender vehicle. Status information includes position, speed, heading towards.etc about sender. Beacons provide resent or latest information of the sender vehicle to the all present vehicles in the network which will help them to know the position of the current network and anticipate the movement of vehicles. Beacons are sent antagonistically to neighbouring vehicles 10 messages each second. Emergency Messages are messages sent by a vehicle who defect a potential dangerous situation on the road, this information should be disseminated to alarm or worn other vehicles about a feasible danger that could affect the incoming vehicles. VANET is a high mobile or volatile network where the nodes are keep changing their position and they are moving in speeds, which means that this vehicles may be get influence, even if these vehicles are very far from the danger, they will reach near to danger very soon, in this case fraction of seconds will be very important to avoid the danger [6, and 7].

In VANET Emergency messages are delivered in broadcasting way. Purpose behind this is all the vehicle within the communication range of the sender should receive the message. Message is hardly reaches a 1000m (which is the DSRC communication range) which is coverage area of sender and it is not enough as due to attenuation and fading effects. Critical information should receive by vehicles which are out of senders range. By using this information they can avoid the danger. In short distances the prospect of message reception i.e. percentage of message reception can reach 99% and as we move forward it decreases up to 20% at half of the communication range (Moreno, 2004). Therefore, there is requirement of a technique to increase the emergency message reception with high reliability and availability. Duo to the high mobility of vehicles, the distribution of nodes within the network changes swiftly, and unexpectedly that wireless links initialize and break down customarily and randomly. Therefore, broadcasting of messages in VANETs plays a pivotal rule in almost every application and requires novel solutions that are different from any other form of Ad-Hoc networks. Broadcasting of messages in VANETs is still an open research challenge and needs some efforts to reach an optimum solution .

2. Problem Statement

System proposes a congestion control scheme distributed across the transport, network and MAC layers that can detect and avoid congestion in the network. It provides priority based traffic scheduling with a dual queue scheduler which favors transitory packets. When congestion is detected based on the buffer occupancy, source sending rate is updated by the sink periodically with the help of dual queues and route the packets through less congested paths.

3. Project Objective

- To design and implement a system using network simulation in vehicular ad hoc network.
- To implement proposed scheduling protocol according to message type of vehicles.
- To eliminate network congestion during the vehicle movement in transport network.

- To impalement a defense mechanism for different type of network attacks like jamming attack, spoofing attack etc.
- To evaluate the proposed system performance analysis with existing approaches

4. Performance Parameter

4.1 Network lifetime:-

Network lifetime has become the key characteristic for evaluating sensor networks in an application specific way. Especially the availability of nodes, the sensor coverage, and the connectivity have been included in discussions on network lifetime. Even quality of service measures can be reduced to lifetime considerations. network lifetime as a measure for energy consumption occupies the exceptional position that it forms an upper bound for the utility of the sensor network. The lifetime of a sensor node depends basically on two factors: how much energy it consumes over time, and how much energy is available for its use.

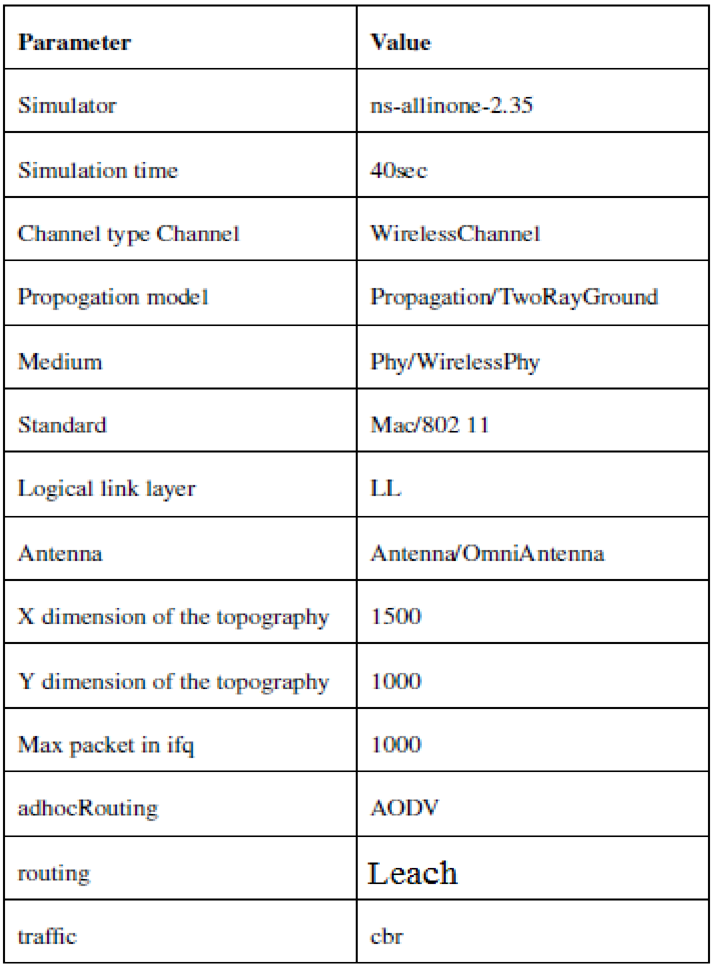
4.2 Energy consumption:-

Energy consumption and energy modeling are important issues in designing and implementing of Wireless Sensor Networks (VANETs), which help the designers to optimize the energy consumption in VANET nodes. Good knowledge of the sources of energy consumption in VANETs is the first step to reduce energy consumption.

4.3 Simulation Environment

In our simulation, each node is set with a single omni-directional antenna, and two-ray ground reflection radio propagation model are applied. Default value used for each parameter in NS-2. The carrier sensing ranges and transmission range dependent on different factors such as the environment, the transmission power and the antenna. While evaluating simulation energy consumption due to radio's energy consumption is focused. Table 1 gives the list of the parameters used while evaluation of simulation. To evaluate the performance of both proposed and existing grid topology scenarios is used. The performance of the scheme deliberates in terms of the packet delivery ratio and end-to-end delay that depends on the energy available in a network. On horizontal scale numbers of nodes are in use and on vertical scale transform according to performance metrics.

List of the parameters used while evaluation of simulation



Parameter	Value
Simulator	ns-allinone-2.35
Simulation time	40sec
Channel type Channel	WirelessChannel
Propogation model	Propagation/TwoRayGround
Medium	Phy/WirelessPhy
Standard	Mac/802 11
Logical link layer	LL
Antenna	Antenna/OmniAntenna
X dimension of the topography	1500
Y dimension of the topography	1000
Max packet in ifq	1000
adhocRouting	AODV
routing	Leach
traffic	cbr

5. PROJECT DESIGN

System Architecture

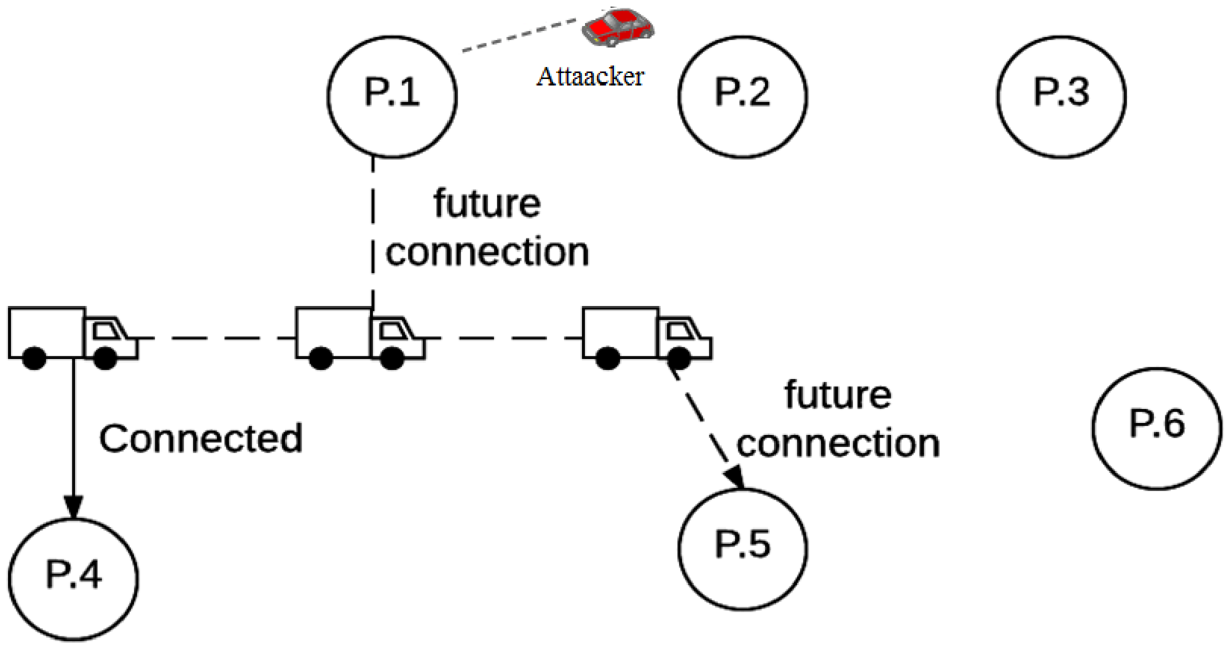


Figure 2. Proposed System Architecture

6. List of Modules and Functionality

6.1: Network Initialization

The proposed work first initialized the network with 89 nodes which contains some relay nodes, some vehicles and some are RSU's. Each vehicle moving on whole topography network during the execution. The vehicle send some packet as request to RSU for release the vehicle from this region.

6.2. Process of assigning priorities

Each vehicle generates the request packets queue by vehicle called as incoming packets which is first received by router. This queue consist the some generated packets, low priority transitory packet, high priority transitory packets. After RSU classify those packets based on this function there are two types of data namely locally generated data and transit data. The data generated from any source node is called locally generated data.

6.3: Persistent Congestion Control

The system also focuses to eliminate the congestion during the multiple packet transmission using multi queue scheduler. Using scheduling approach it will set the vehicle scheduling according to message type like emergency, normal, low priority etc.

6.4: Delivery ratio and performance

Finally after running the simulation we have to measure the delivery ratio as well performance ratio of system. with the help of confusion matrix of system evaluate the performance analysis like packet drop ratio, error rate, accuracy etc.

7.DESIGN IMPLEMENTATION

7.1 Class Diagram

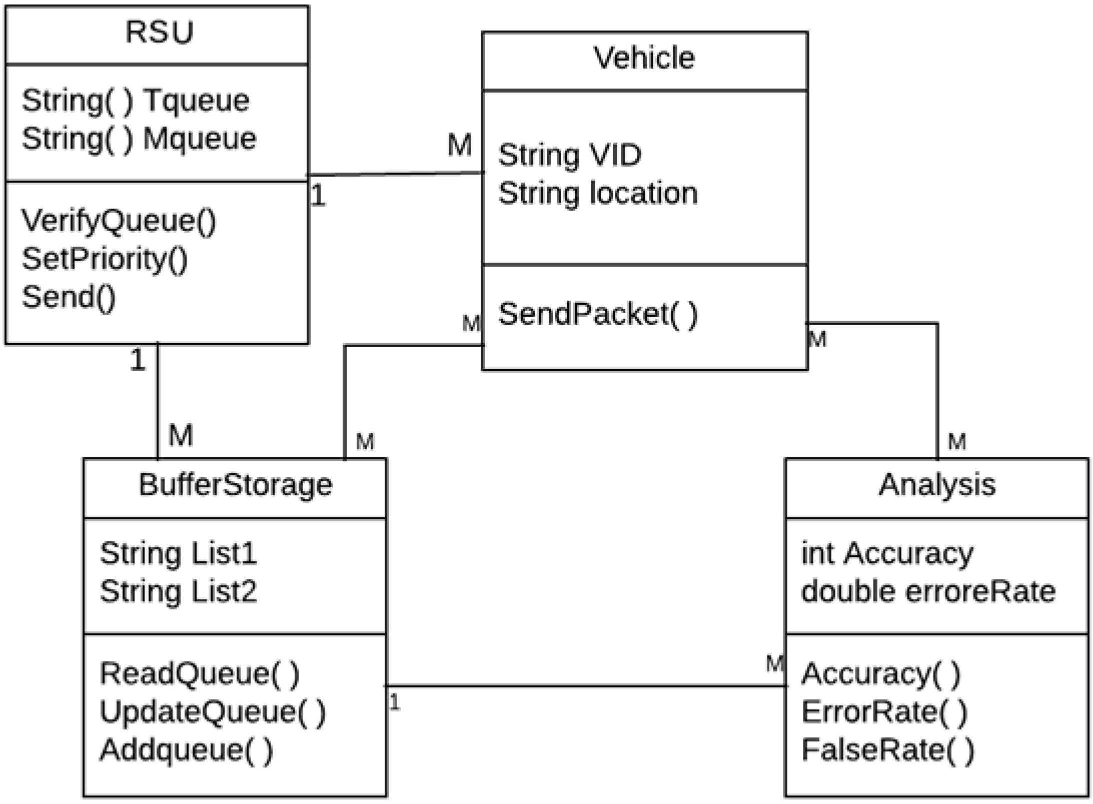


Figure 3: Class Diagram

7.2 Activity Diagram

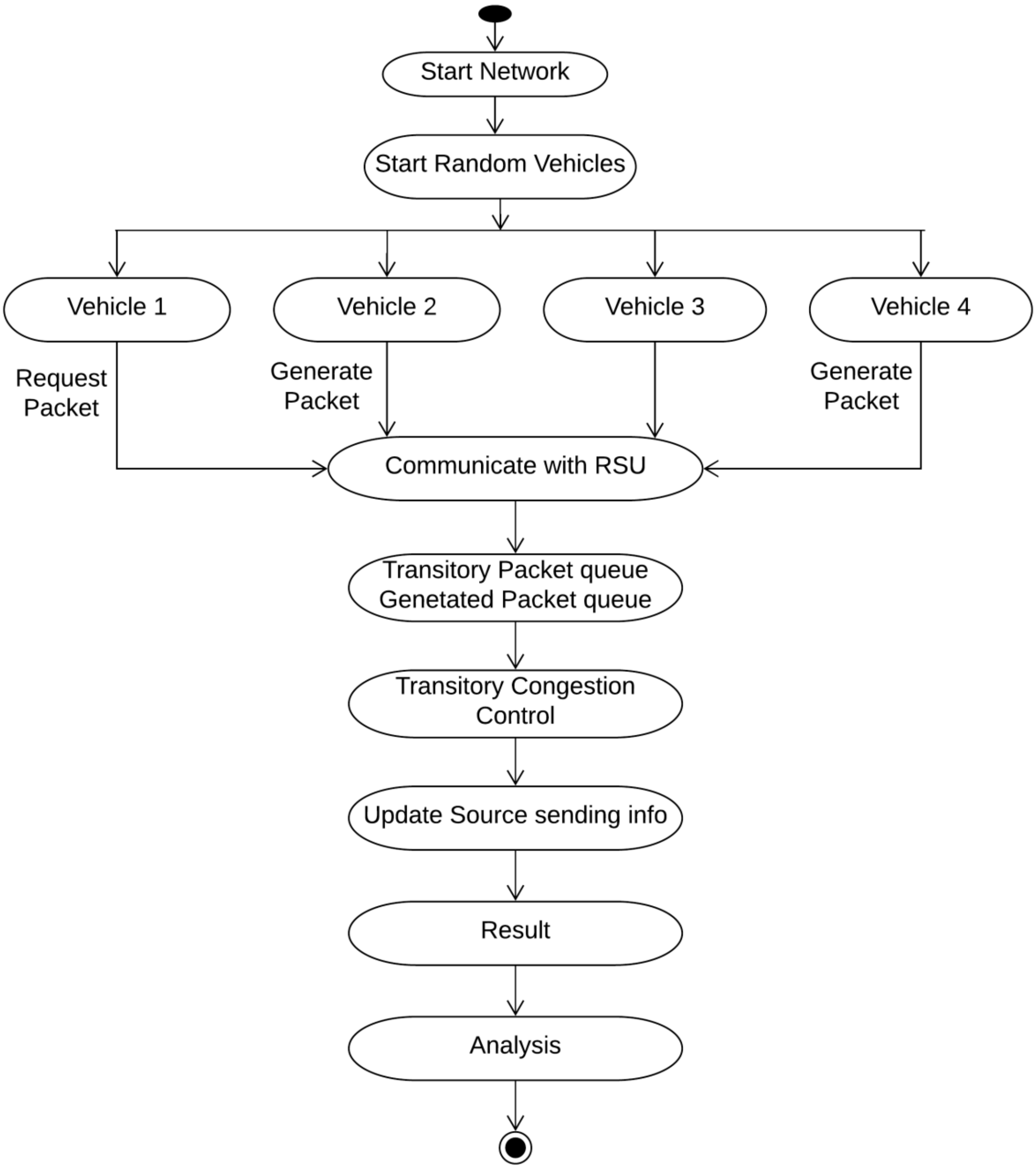


Figure 4. Activity Diagram

7.3 Use Case Diagram

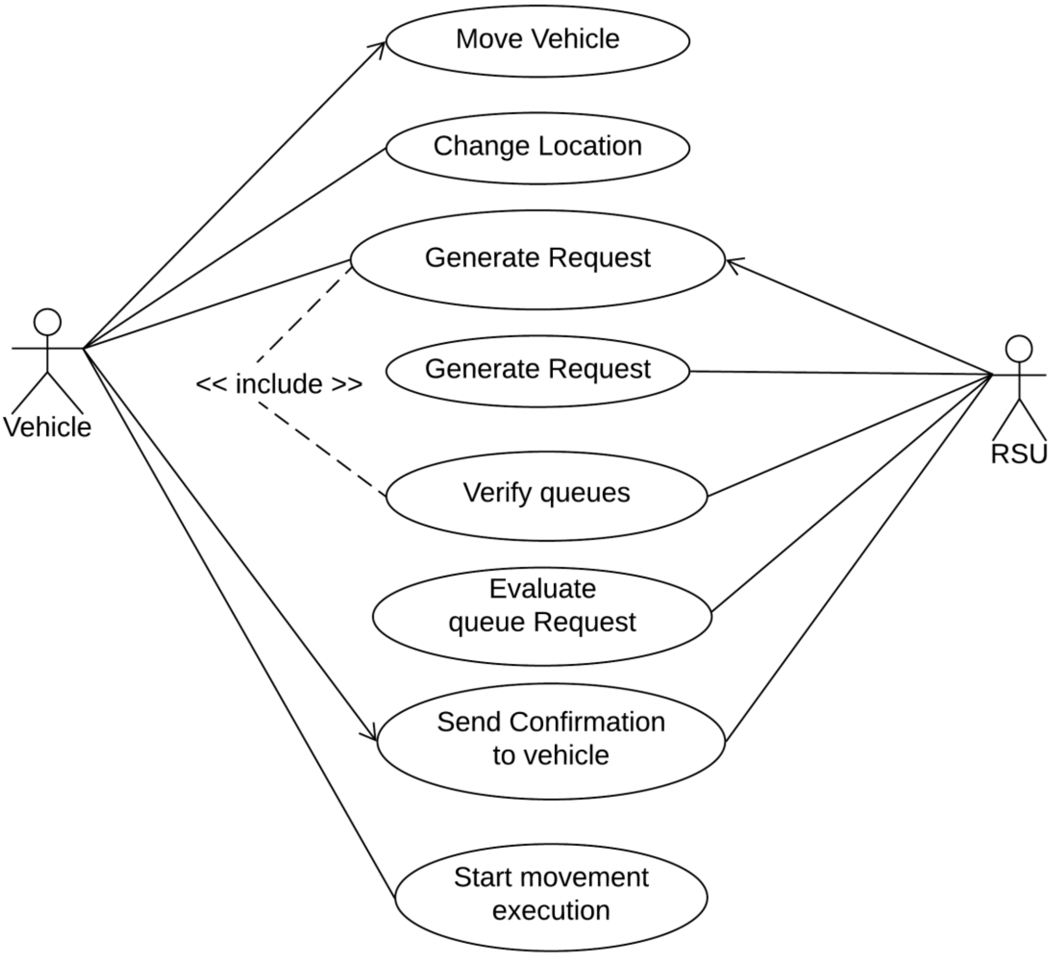


Figure 5. Use Case Diagram

7.4 DFD Context Level

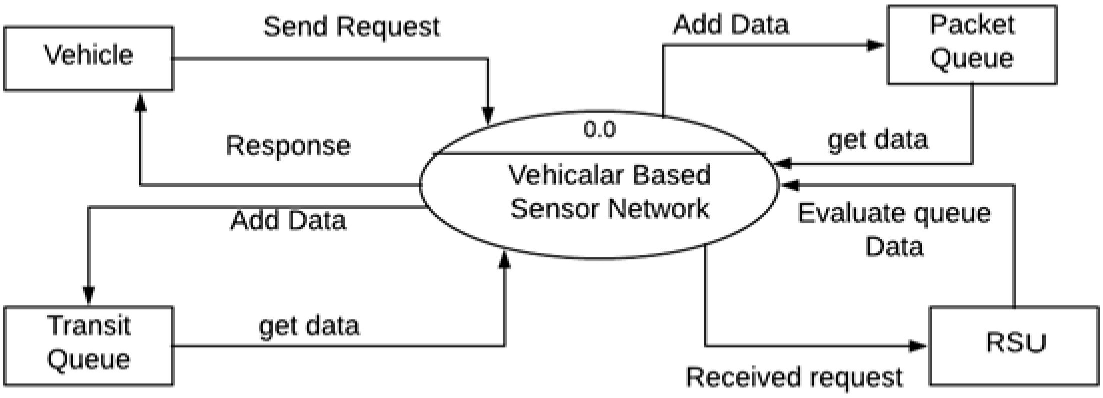


Figure 6. DFD Context Level

8. Performance Accuracy

Energy consumption is most important concepts in VANET. The lifetime of the sensor network is based on energy consumption of the sensor node. Total energy consumption of the node defined as the difference between initial energy and final energy of the node. The energy consumption of EAACK, EEAR and Proposed system increases with increase in number of nodes as shown in Table 6.3.5 . However, increasing treads in EEAR proposed is much higher than EAACK as shown in Fig 6.4.5 The smallest amount value of energy consumption states superior performance of the protocol.

.

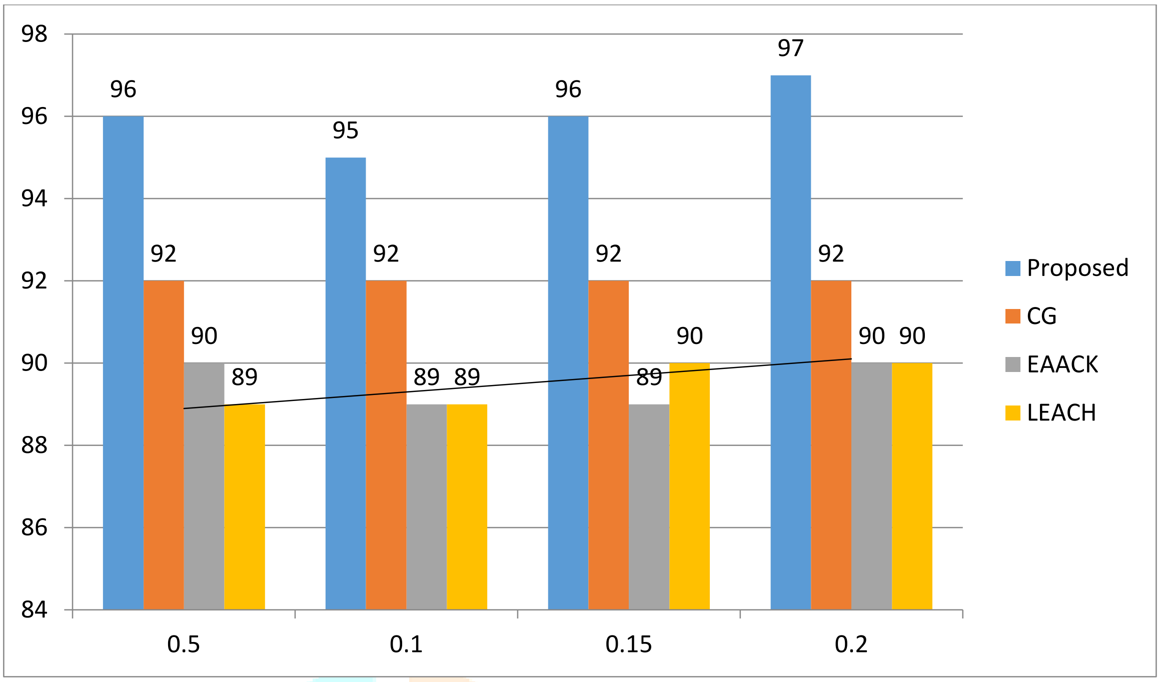


Figure 7

In order to evaluate the performance of system performed. The network architecture considered is the following:

- The proposed system provides the accuracy around 96% it highest than other detection algorithm.
- System used KDDCUP 99 dataset for data classification as well as attack detection like raining as well as testing.
- The pattern matching based machine learning algorithm has used for categorized the various attacks.

9. RESULTS AND DISCUSSIONS

9.1 Advantages

- System can easily identify the emergency scenario using different message type.
- Provide easy communication to remote vehicles which is not in RSU’s range.
- It also provide runtime packet transmission rate according to current scenario.

9.2 Disadvantages

- Congestion in handover.
- Nearest vehicle can’t send own message to RSU, even in case vehicle having emergency.
- Packet overhead generation during the communication when both queues already full.

10.CONCLUSIONS

A cross-layered congestion control algorithm for VANET is proposed. It enables joint optimization of different layers and is more advantageous compared to the traditional layered approach. Concentration is majorly on congestion control. Here congestion can be detected using the buffer occupancy in dual queue. During congestion more priority is given to the transit packet than generated packet. One of the common situations where this approach would make a difference is in the vehicular overtaking scenarios.

When a speeding vehicular node is overtaking another node, the vehicles further ahead also need to be made aware of the overtaking. One of the common situations where this approach would make a difference is in the vehicular overtaking scenarios. When a speeding vehicular node is overtaking another node, the vehicles further ahead also need to be made aware of the overtaking. Such communication would prevent accidents from taking place because, the speed of the vehicle can be overwhelming and time taken for the generated packets to reach the appropriate nodes may be large. Another compelling scenario is when vehicles are forced to enable sudden brakes. In such a case informing the vehicles following behind the given vehicle will help these vehicles to not engage in series of heart overhead collisions. Hence, the VANET can be enhanced by prioritizing transitory packets over the generated packets. Such communication would prevent accidents from taking place because, the speed of the vehicle can be overwhelming and time taken for the generated packets to reach the appropriate nodes may be large. Another compelling scenario is when vehicles are forced to enable sudden brakes. In such a case informing the vehicles following behind the given vehicle will help these vehicles to not engage in series of rear to head collisions. The propose work has done with NS2 environment with given packet scheduling approaches, provides the accepted results. To defense some unknown type of network, active and passive attack detection is the future work for this system.

Future Work

To apply the various packet scheduling schemes and reduce the packet drop ratio, in VANET using different security algorithms.

Acknowledgment

I would like to express my gratitude towards Prof. N.S. Bagal for guiding me throughout the project. The mentioned project was done under the supervision of Prof. Dr. B.K. Sarkar.

I express my kind gratitude towards staff of our institution Padmabhooshan Vasantdada Patil Institute of Technology and I feel thankful to the all college staff, I thank all participants for their positive support and guidance.

11. REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.

[3] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[4] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,” IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/ Passenger_vehicles_in_the_United_States, 2012.

[8] J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc. Sixth ACM Int’l Workshop VehiculAr InterNETworking, pp. 89-98, 2009.

[8] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, “The Broadcast Storm problem in a Mobile Ad Hoc Network,” 5th annual international conference on Mobile computing and networking (MobiCom), 1999.

[9] Briesemeister, Linda, Lorenz Sch¨afers and G¨unter Hommel: “Disseminating Messages among Highly Mobile Hosts based on Inter Vehicle Communication” .In Proceedings of the IEEE Intelligent Vehicles Symposium 2000, pages522–527, Piscataway, NJ, USA, October 2000

[10] M.Zorzi and R.R.Rao: “Geographic Random Forwarding (GeRaF) for adhoc and sensor networks: multihop performance”, IEEE Transaction on Mobile Computing, Vol. 2, no. 4, Oct-Dec.2003