International Journal of Engineering & Technology, 7 (4.39) (2018) 710-713

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Vehicular safety using Medium Access Control and Particle Swarm Optimization

Shilpa Choudhary *[1], Awanish Kaushik [2], Mudita Vats [2] , Arpana Mishra [3]

[1,2,3,4] *Department of Electronics & Communication*
[1, 2,3, 4] *G. L. Bajaj Institute of Technology & Management, Greater Noida, G.B.Nagar, Uttar Pradesh, India*
**Corresponding author E-mail:shilpadchoudhary@gmail.com*

Abstract

Vehicular ad hoc networks (VANET) are emerging as a prominent form of mobile ad hoc networks (MANETs) and as an effective technology for providing a wide range of safety applications for vehicle passengers. Nowadays, VANETs are of an increasing importance as they enable accessing a large variety of ubiquitous services. Such increase is also associated with a similar increase in vulnerabilities in these inter-vehicular services and communications, and consequently, the number of security attacks and threats. It is of paramount importance to ensure VANETs security as their deployment in the future must not compromise the safety and privacy of their users. The successful defending against such VANETs attacks prerequisite deploying efficient and reliable security solutions and services, and the research in this field is still immature and is continuously and rapidly growing. As such, this paper is devoted to provide a structured and comprehensive overview of the recent research advances on VANETS nodes crossing each other but having no collision between them using mac protocol a layer of data link layer and particle swamp optimization technique (PSO) that is a probabilistic approach to send a best probable massage to the link layer or mac protocol , and we are also using the frequency range of 5.9GHZ of dedicated short range communication (DSRC) a family of IEEE 108.11ac.

Keywords: *DSRC, MANET, PSO, VANET.*

1. Introduction

Vehicular Ad-Hoc Networks (VANETs) make it possible for vehicles to broadcast warnings about environmental hazards (e.g., ice on the pavement), traffic and road conditions (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information to other vehicles. Once it is known that there is a traffic jam, road closure or accident ahead, a driver may safely avoid the route and save time. Communication between vehicles is therefore suitable because vehicles are able to distribute warnings to other vehicles. The minimal configuration and quick deployment of VANETs also makes them suitable for emergency type situations. Messages can be sent from vehicles to summon for help if needed and to inform authorities of dangerous behavior on roads. In another paper by Papadimitratos et al. VANETs are said to assist to make roads safer, and offer convenience. Much has been written on the various scenarios where vehicles may obtain value from communication. However, one needs to be sure that the messages are valid and that the network will not be used maliciously. One could, for example, conceive of a situation where a vehicle whose permanent identity is known could be travelling with a low fuel reserve and request for help, but because the vehicles identity is known an attacker monitoring communication in the network will be aware that there is a vulnerable vehicle on a road and could follow the vehicle until it has run out of fuel and possibly attack the occupants and steal all valuable items in their possession. The vehicle occupants could then be stranded without a means of contacting the authorities.

However, if the vehicles permanent identity is hidden from all other vehicles and can only be seen by the authorities then only authorized personnel will know which vehicle has requested help and would be able to assist accordingly. This ensures that the malicious users will not know which vehicle has requested help for a fuel shortage, hence protecting the vehicle and its occupants. It is also necessary for the vehicle to be registered with some central authority so that nodes caught sending erroneous and malicious messages can be determined and held accountable. It means that nodes must identify themselves as the source of all their messages. This is the function of authentication.

In VANETs, the privacy concern surrounds information privacy and communication privacy. VANETs allow for disclosure of vehicle location information a malicious node eavesdropping on all traffic in an area is able to reconstruct long traces of the where about of majority of vehicles within the same area show that this problem is addressed by providing privacy enhancing mechanisms. This presents developers of the VANET systems a unique opportunity to develop an entirely new system that could rival or supplement the already existing cellular system by offering unique and competitive services. With the development of 802.11p version of popular wifi standard, altered specifically to accommodate the needs of vehicular communication and commercial players. The main and initial appeal of VANET systems is in notion that replacing warning response systems currently based mostly on human senses (eyes, ears, muscle reflexes). There is a reason why road-ways vehicle are not allowed to run at speeds of their dedicated-path counterparts. When reliable wireless communication becomes available across machine interfaces in vehicular nodes, the speed of nodes can be increased without loss of safety.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

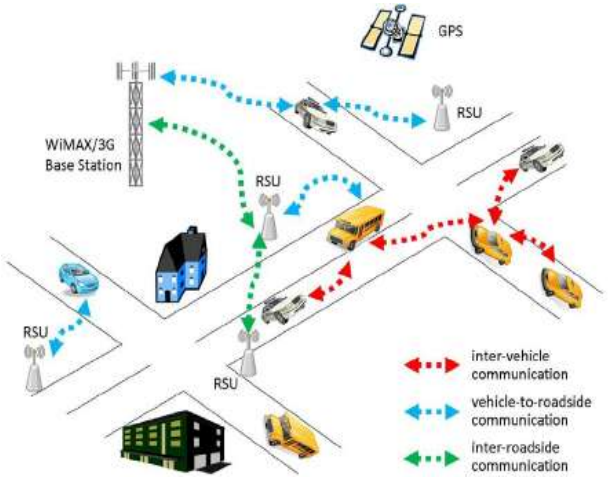


Fig 1: A typical VANET scenario

Vehicular networks (VANET) are emerging as a prominent form of mobile ad hoc networks (MANETs), where the mobile nodes are the vehicles with a restricted mobility pattern with dedicated units for communication that are installed in vehicles allowing them to exchange data, whereas the fixed nodes are the roadside units (RSU) deployed in critical locations . Communications in VANETs is of the form of vehicle-to-vehicle communication (v2v) and vehicle-to-infrastructure (v2i) communication typically using global positioning system (GPS) to exchange messages with the RSU, and can be single-hop and/or multi-hop and broadcasting or multicasting, if the range limitations are satisfied.

VANETs, which are made up of mobile nodes (vehicles), can be considered as a special case of MANETs. They are both characterized by the movement and self-organization of the nodes, but they also differ in some ways such as network infrastructure components and a highly dynamic topology. Figure 1 shows the possible domains that a VANET network consists of. These include the Ad hoc, infrastructure and Interne domains. This figure also shows the different forms of communication in such networks: inter-vehicle communication V2V, in which the vehicles can communicate with each other in an ad hoc fashion, and vehicle-to-roadside communicationV2I, where the road-side-units (RSUs) are used as access points to connect moving vehicles to the network infrastructure which is connected to the Internet Moreover, a 4 vehicle can communicate with the Internet directly through Hotspot devices installed along the road.

Each vehicle is equipped with two devices: an On Board Unit (OBU), and an Application Unit (AU). The OBU is used to exchange information with RSUs or with other OBUs in the ad hoc domain, whereas the AU executes applications that can use the communication capabilities of the OBU.

VANETs are able to significantly reduce the delay in propagating emergency warnings. The vehicles exchange messages to inform each other about events and dangers on the road. A vehicle is able to recognize a dangerous situation and is able to quickly warn neighboring vehicles. This allows for a faster reaction to the situation. The information for these warning messages comes from the information derived from sensors in the vehicle: ABS, ESP, etc. Information about traffic congestion can also be sent. , a warning message that the vehicles can send is

Emergency Electronic Brake Lights. This allows for sudden braking of vehicles in the forward path to be highlighted as a hazard, asking vehicles to slow down and helping to prevent multi vehicle pile-ups and other accidents. The vehicles connect to RSUs in an ad-hoc manner, as and when needed. The Infrastructure Domain consists of the RSUs and the CA. The CA is connected to the RSUs and allow for the RSU to act as a proxy to the CA.

2. Medium Access Control In VANETS

A Medium Access Control (MAC) protocol specifies the mechanism in which nodes share the channel. There are many MAC issues in VANET like prioritized access, unpredictable response and reliability. All these are needed because these are basic requirements of safety applications. To provide a reliable broadcast communication can be difficult in wireless networks due to hidden terminal and exposed node problems. A key challenge of VANET is that there are frequent changes in the network topology because the vehicles travel at a high velocity. So, VANET MAC protocols have to care about the rapid topology changes, and for safety applications, there is a need to reduce the medium access delay. In this work, we have categorized the MAC protocols for VANET in three categories. These are:

- Contention-Based Protocols
- Delay Bounded/Contention Free
- Hybrid MAC Protocols

3. Particle swarm optimization

Particle swarm optimization (PSO) is an optimization technique to solve a problem by iteratively process to improve a solution with respect to a given measure of quality. Problem can be resolved by having a population of candidate solutions, here labelled particles, by the movement of these particles in the search space according to a mathematical formula over the velocity and particle's position

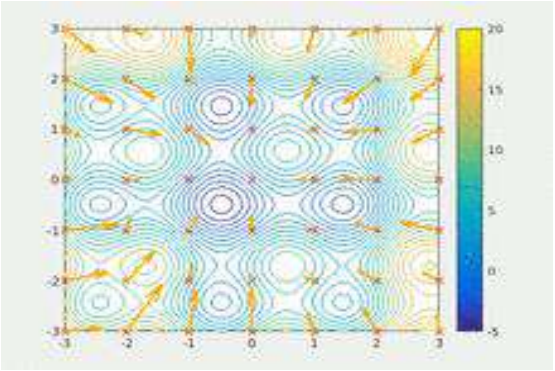


Fig. 2: A particle swarm searching for the global minimum of a function

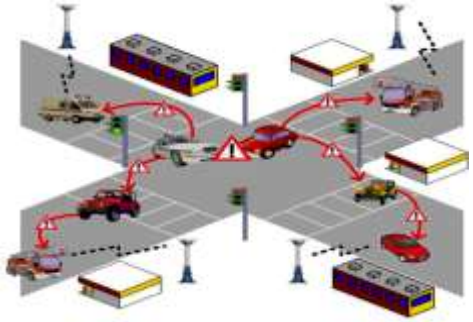


Fig 3: Vehicles travelling through crossing

Each particle's movement is decided by its local best known position, but it also guide toward the best known positions in the search space, which are being updated as per the better positions which are found by other particles. This will decide the particle movement toward the best solutions.

4. Result and Discussion

Previously the work has been done only for one node entering in the RSU unit travelling with a constant speed but in this work we

are dealing with multiple node travelling at same time travelling in any direction on road.
Table 1 shows how many collisions occur after taking random no of vehicles on the VR road, HR road and on the crossing.

Table.1: vehicle travelling without RSU

Total vehicle on VR road	total vehicle on HR road	total collision on VR	total collision on HR	total collision on crossing
10	10	0	0	0
20	20	0	0	0
30	30	0	0	0
40	40	0	0	0
50	50	2	2	0
60	60	2	2	0
70	70	6	6	0
80	80	6	6	0
90	90	6	9	0
100	100	14	14	0
150	150	34	34	0
200	200	54	56	0
250	250	68	60	0
300	300	100	120	1

Table 2: vehicle travelling with RSU

No of vehicle on VR road	No of vehicle on HR road	No of VR collision =0 in which iteration	No of HR collision =0 in which iteration	No of crossing collision=0 in which iteration
10	10	0 in first iteration	0 in first iteration	0 in first iteration
20	20	0 in first iteration	0 in first iteration	0 in first iteration
30	30	0 in first iteration	0 in first iteration	0 in first iteration
40	40	0 in 4th iteration	0 in 4th iteration	0 in 4th iteration
50	50	0 in 5th iteration	0 in 5th iteration	0 in 5th iteration
60	60	0 in 9th iteration	0 in 9th iteration	0 in 9th iteration
70	70	2 in 9th iteration	0 in 9th iteration	0 in 9th iteration
80	80	0 in 12th iteration	0 in 12th iteration	0 in 12th iteration
90	90	2 in 10th iteration	0 in 10th iteration	0 in 10th iteration
100	100	0 in 15th iteration	0 in 15th iteration	0 in 15th iteration
150	150	0 in 28th iteration	0 in 28th iteration	0 in 28th iteration
200	200	8 in 30th iteration	8 in 30th iteration	0 in 30th iteration
250	250	10 in 30th iteration	10 in 30th iteration	0 in 30th iteration
300	300	100 in 30th iteration	100 in 30th iteration	1 in 30th iteration

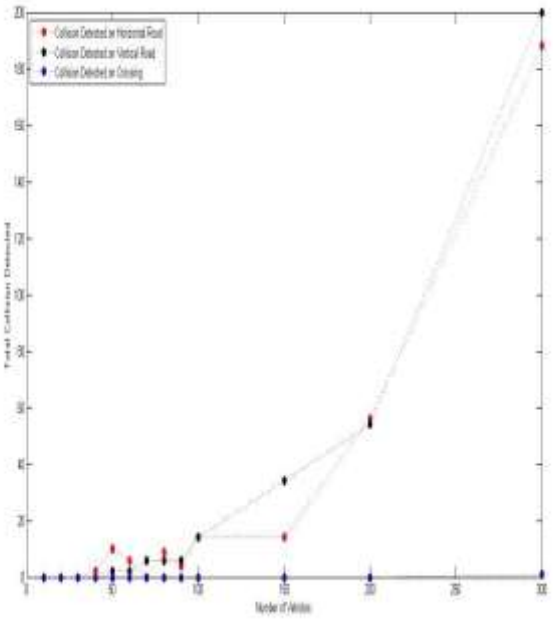


Fig. 4: Graph Of No Of Vehicles (Nodes) V/S Total No Of Collision.

In Figure 4 rRed dot represents collision detected on HR road, Black dot represents collision on VR road and Blue dot represents collision on crossing.
The approach is to minimize the road side and vehicle to vehicle (v2v) collision using MATLAB.
These results are for- 10, 20, 30 …… up to 300.
After applying the RSU and PSO, it gives all the information to the RSU unit it will then calculate the speed of the vehicles and if collision is there on HR, VR and on crossing it will send the optimum speed to the vehicles to maintain their speed so that no collision occur the result of such system in which RSU and PSO are playing role are as above in the tables.

5. Conclusion

The primary purpose of this work is to design an efficient routing algorithm in VANET environment to improve the performance of existing position based routing approaches in VANETs. Common scenarios of VANET nodal locomotion were identified and simulated for this work, with the increase in number of iteration it will always results in 0 collision on the road. The above results is for only 50 iteration and in which collision were minimum as compared to the previous results when don't had any RSU units.

Future work

Authority of India (NHAI) is planning to replace manual toll collections at plazas with electronic toll collection (ETC) systems across the country. The ETC system will be based on radio frequency identification (RFID), which will be complemented by a wireless on-board unit (OBU) on a vehicle, as well as a stationery roadside unit (RSU) at the toll plaza. There are lots of future aspects from VANET some are as follows-
If we knows where the collision occur we can directly send a message to the ambulance within range. Collision avoidance and give the maximum speed to the vehicle on the road Work as internet of things This work is focused on VANET using mac protocol and particle swarm optimization. The work is done for more than one nodes travelling on the crossing area because previously the work on VANET using MAC protocol has been done for only single nodes. In future the work it can be extended for n number of vehi-

cles travelling from both the sides on one way and more no of nodes travelling at a single time and the number of collision get reduced.

- As mobile ability are familiar and used in our day to day life, similarly the future of VANETs is undoubtedly secure. It has become the part of the government projects. In India, National Highways (IOT), like if we are coming to home to office we can command to home appliances to do the certain things like make a cup of tea / coffee , open gate some time before etc…..
- VANETs are promising additions to our future intelligent transportation systems that have captured worldwide attention from auto companies, academics, and government agencies. Realizing V2I and V2V communications will enable many safety and infotainment applications that can revolutionize the transport infrastructure.
- Active Prediction: It anticipates the upcoming topography of the road, which is expected to optimize fuel usage by adjusting the cruising speed before starting a descent or an ascent. Secondly, the driver is also assistance.

References

[1] Dr. Tae-Hoon Kim,and Dr. Lash B. Mapa, "Investigating the Effect of Temperature in RFID Technology" *American Society for Engineering Education*, 2017

[2] Umar Hasan Khan , Bilal Aslam,Muhammad Awais Azam, Yasar Amin,"Compact RFID Enabled Moisture Sensor" *Radioengineering*, Vol. 25, NO. 3, September 2016.

[3] Li Zhenzhong1, Mrad Nezih, Xiao George, Ono Yuu, Liu Guocheng, Ban Dayan," Effects Of Temperature And Humidity On Uhf Rfid Performance" *Smart Materials, Structures & Ndt In Aerospace Conference NDT In Canada* 2011.

[4] J. Britton" An investigation into the feasibility of locating portable medical devices using radio frequency identification devices and technology" *J Med Eng Technol*, 31 (6) (2007), pp. 450-458

[5] W.H. Dzik "New technology for transfusion safety" *Br J Haematol*, 136 (2) (2007), pp. 181-190

[6] M.T. Egan, W.S. Sandberg "Auto identification technology and its impact on patient safety in the operating room of the future"*Surg Innov*, 14 (1) (2007), pp. 41-50

[7] J. Kannry, S. Emro, M. Blount, M.R. Ebling "Small-scale testing of RFID in a hospital setting: RFID as bed trigger" *AMIA Annu Symp Proc* (2007), pp. 384-388

[8] A. Macario, D. Morris, S. Morris "Initial clinical evaluation of a handheld device for detecting retained surgical gauze sponges using radiofrequency identification technology" *Arch Surg*, 141 (7) (2006), pp. 659-662

[9] R.A. Marjamaa, P.M. Torkki, M.I. Torkki, O.A. Kirvela "Time accuracy of a radio frequency identification patient tracking system for recording operating room timestamps"*Anesth Analg*, 102 (4) (2006), pp. 1183-1186

[10] H.J. Meyer, N. Chansue, F. Monticelli "Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI)" Forensic Sci Int, 157 (2–3) (2006), pp. 168-171

[11] P. Nagy, I. George, W. Bernstein, et al. "Radio frequency identification systems technology in the surgical setting" Surg Innov, 13 (1) (2006), pp. 61-67