International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.086-089
DOI: http://dx.doi.org/10.21172/1.81.011
e-ISSN:2278-621X

ADAPTIVE MULTIPLE COLLISION AVOIDANCE IN THE VEHICULAR NETWORK WITH MOBILITY AWARE LOCATION TRACKING

Bohar Singh[1] and Poonam[2]

Abstract—The mechanically driven vehicle based mostly networks (VANETs) square measure susceptible to numerous routing hazards. The collisions on the roads, different hurdles like tree falling, road damages to external stimulae block the roads and don't leave anyplace for vehicles to tolerate. In such cases, it becomes essential to route the vehicles through the backup methods so as to avoid the dangerous hurdles created on the roads because of any reason. During this paper, we've planned the new paradigm within the dangerous routing protocol for the mechanically driven vehicle based mostly VANETs. The planned model would be evaluated on the premise of accuracy, route persistence, likelihood of detection, likelihood of warning, etc.

Keywords: hazard routing, collision area bypassing, automatically driven vehicles based VANETs, backup path selection.

I. INTRODUCTION

The inter connectivity of vehicles and road side units are required to complete a network in vehicular network. The node-to-node to RSU architecture is an idea which is used to connect the not-in-range nodes with the in-range nodes so that they can be provided with the hazardous messages earlier and hence, in other words, we are increasing the coverage area. Thus, if the not-in-range nodes are receiving the information about the hazardous earlier they can change their route on time and hence, performance of VANET is improved by enhanced connectivity schemes.

To create a mobile network, a Vehicular Ad hoc NETwork, or VANET uses moving cars or vehicles as nodes in a network. A VANET allows cars approximately 100 to 300 meters from each other to connect by turning each participating car into a wireless node or router and hence, creates a network with a wide range. Whenever any car falls out of the signal range and leaves the network, other cars can join in and create a mobile network. The estimations say that the first system that will integrate with this technology are police and fire vehicles that will communicate with each other for safety purposes. Vehicular networks are developed to improve the safety measures for the transportation and providing them with new mobile applications and services so that they can move with greater efficiency to avoid the traffic. Vehicular networks are becoming a crucial component for the future intelligent road traffic management systems where future

[1] *Department of Computer Science and Engineering SBSSTC, FEROZEPUR, PUNJAB, INDIA*
[2] *Department of Computer Science and Engineering SBSSTC, FEROZEPUR, PUNJAB, INDIA*

intelligent road traffic management systems are expected to offer several features as compared to the current traffic management system.

The features or advantages provided by the future intelligent road traffic management systems are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers are working for more than a decade to develop a suitable Vehicular Ad hoc Networks (VANETs) for traffic safety systems. VANETs are considered as the intelligent systems which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UTMS, Wi-MAX networks and these advantages are self-organization, low cost of implementation and maintenance and lower local information dissemination time. VANETs can be said as the practical implementation of MANETs in future. This vehicular network is made up of the vehicles which have wireless interface and are interconnected to transfer information. The vehicles can easily provide power for connection for wireless communication and if other communication hardware like antennas are required, they can also be used without causing any major problems. The focus of VANET is to provide cost-effective and timely information to the vehicles or passengers so that they can commute without any disturbances on the way because of hazardous.

Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e., a contact) arises. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery. Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination (eventually and over time).

The main difference between VANET and MANET are its mobility model. When a vehicle is moving on a road, its mobility pattern must include with the topology of the road. This constraint is called as mobility. In addition, the behaviour of different drivers are different as in a normal condition, their speeds can vary from 60 km/hr to 130 km/hr. So, we can’t apply any random mobility model on all of the drivers. The mobility model will always be dynamic, not static. And, the relative speeds of the vehicles will always be higher especially when moving in different directions.

II. LITERATURE REVIEW

Ghaleb F. et al. proposed the paper which presents a mobility pattern based misbehaviour or hazardous situation detection in VANETs. This paper differentiates the attacker into 2 categories- insiders and outsiders where insiders is a legitimate node which might intentionally or unintentionally make misbehaviour or unauthorized actions, such as modify, fabricate or drop the message in order to impersonate other node identities. And, outsider is a kind of intruder aim to interfere the communication among VANET nodes. Misbehaviour can be viewed as following two perspectives in VANETs- (i) physical movement and (ii) information security perspectives. This paper includes algorithm to detect the misbehaviour which is Location-Aided Routing for MANET (ALARM) and relies on location information and routing time. Sharma G. et al. proposed the paper which includes analysis and discussion for various types of security problems

and challenges in VANETs and also the solutions for these problems and challenges. According to this paper, each vehicle has 2 devices OBU (On Board Unit) and TPD (Tamper Proof Device) where OBU connects vehicles with RSU via DSRC and TPD hold the vehicles secrets like keys, driver identity, trip details, route, speed etc. Various attacks discussed in this paper are DOS, Fabrication Attack, Alteration Attack, Replay attack and various attackers are Selfish Drivers, Malicious Attackers and Pranksters. According to this paper various vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non Repudiation, Privacy, Integrity and Confidentiality. Seuwou P. et al. proposed VANET as a technology that uses moving cars as nodes in a network to create a mobile network. VANET enables two types of communication- vehicle to vehicle (V2V) and vehicle to road-side infrastructure (V2I). This converts every participating car into a wireless router or node which allows connection between other cars in a radius approximately 100 to 300 meters, thus creating a network of wide range. In this paper author proposed various issues of effective security in VANETs. Also, he discussed various attacks in VANETs. He classified attacks into two broad categories- (i) physical attach which occurs because of two problems- tamper proof device and event data recorder, and (ii) logical attack which occurs because of virus, Trojan horse and protocol weak spot. Qian.yi et al. proposed an overview on a priority based secure MAC protocol for vehicular networks and he assumes that the MAC protocol can achieve both QOS and security in vehicular networks. According to this paper the MAC protocol is having messages with different priority for different applications to access DSRC (Dedicated Short Range Communication) channel. And, the proposed secure MAC protocol will use a part of IEEE 1609.2, security infrastructure including PKI and ECC, the secure communication message format of vehicular networks, and the priority based channel access according to the QOS requirement of the applications.

III. PROBLEM FORMULATION

The existing model is meant to unravel the matter of knowledge dissemination or broadcast within the cluster concerning the obstacles created attributable to fall of trees, landslide, maintenance work, etc. Such data is incredibly significantly to be delivered to any or all of the nodes move towards the hurdle so as to alter their route of travel effectively. The planned model is employed to avoid the traffic jams and accidents attributable to latter represented obstacles. The vehicle route improvement or route modification is kind of necessary to stay the uninterrupted transport movement on the roads. within the existing answer, the most important objective is to broadcast the knowledge concerning the hurdle (so known as hazard within the existing work) within the VANET cluster, which might be employed by the vehicles to require safety action to avoid the dangerous locations.

The planned protocol, DHRP (direction based mostly hazard routing protocol), takes associate account on the geographic location of the nodes and also the hazard to stay the nodes updates, which is able to square measure move towards the dangerous location. the present model contains numerous issues. At first, it doesn't take the not-in-range nodes under consideration. It suggests that the nodes that don't seem to be in vary would be not delivered (or secured delivered) the printed message concerning the hazard once they're going to be part of associate RSU. Such drawback should be taken under consideration to avoid the danger on the lifetime of the folks move in any such vehicle that is out of reach throughout the message broadcast. The node failure within the existing theme also can cause dangerous things. The node failure will

cause collision, traffic chaos or alternative movement connected hazards. The node failures are often lined up mistreatment the unicast question messages.

IV. CONCLUSION

This research project will start with a detailed literature review on the various VANET mobility and collision avoidance and coverage schemes. Then, a detailed coverage and connectivity mechanism would be designed to prevent the issue of non-connected nodes and to provide the maximum message reach in VANETs. The simulation would be implemented using Network Simulator (NS2). The obtained results would be examined and compared with the existing security mechanism to address the similar issues. Waterfall development method is ideal for projects with clear task formalization and fixed scope of work like this research work, i.e. for small and medium-size projects.

REFERENCES

[1]. Ghaleb, Fuad A., M. A. Razzaque, and Ismail Fauzi Isnin. "Security and privacy enhancement in vanets using mobility pattern." In *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, pp. 184-189. IEEE, 2013.

[2]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pp. 393-398. IEEE, 2010.

[3]. Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." In *Road Transport Information and Control (RTIC 2012), IET and ITS Conference on*, pp. 1-6. IET, 2012.

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

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

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

[7]. 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." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 36-41. IEEE, 2012.

[8]. Sumra, Irshad Ahmed, Halabi Hasbullah, J. A. Manan, Mohsan Iftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pp. 708-714. IEEE, 2011.

[9]. Sumra, Irshad Ahmed, Halabi Hasbullah, and J-L. A. Manan. "VANET security research and development ecosystem." In *National Postgraduate Conference (NPC), 2011*, pp. 1-4. IEEE, 2011.

[10]. Chen, Lu, Hongbo Tang, and Junfei Wang. "Analysis of VANET security based on routing protocol information." In *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, pp. 134-138. IEEE, 2013.

[11]. Khabazian, Mehdi, and M. K. Mehmet Ali. "A performance modeling of vehicular ad hoc networks (VANETs)." In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 4177-4182. IEEE, 2007.

[12]. Qian, Yi, Kejie Lu, and Nader Moayeri. "Performance evaluation of a secure MAC protocol for vehicular networks." In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-6. IEEE, 2008.