RESEARCH ARTICLE OPEN ACCESS

Collision Avoidance Mechanism Using Multi-Layered Collision Detection Model For Vehicular Networks

Harjinderjeet Singh [1], Manuraj Moudgil [2]
Department of Computer Science and Engineering [1]
Department of Information and Technology [2]
PTU Jalandher
India

ABSTRACT

VANETs (Vehicular Ad-hoc Networks) are the emerging network technology for the moving vehicles and emerged as a popular research area. This emerging vehicular network technology is taking the world into a new age of automatically driven vehicles. These automatically driven vehicles will communicate with other vehicles digital medium of VANETs. The collision becomes the common problem in the case of automatically driven vehicle clusters. We present a security method to protect the VANET nodes from the collisions. We are going to use location aware fixed nodes to prevent from collision. In this paper, we have proposed the framework for VANET cluster for the collision free movement in the case of collision, natural hazard or any other hazard. The proposed solution has been designed to overcome the problems of the existing scheme. The proposed model results would be evaluated in detail by using several parameters.

Keywords:- Collision-free VANETs, Collision detection, Hazard routing, Point of collision, Probability of collision.

I. INTRODUCTION

VANET is a vehicular ad hoc network. VANET is a technology creates a mobile network in which moving cars act as nodes. In VANET every participating car behaves like wireless router or node, every node create a wide range network. The nodes are detecting to each other approximately 100 to 300 meters range. If cars or nodes faraway to the given range the signal drop out from the network and on the other hand new cars or nodes can detect the other and join into the network, that's by a mobile Internet is created. It is estimated that the first systems that will detect the emergency alerts or swear levels like (police vehicles, ambulance, fire brigade) that communicate with each other for safety purposes and helps to choose the less traffic ways [1].VANET is prime technology that use in current era to develop the efficiency of the transportation systems, improve the safety, security and enable new mobile applications and services for the travelling public. Vehicular networks fulfil the future need and manage the future intelligent road traffic management system. Future intelligent road traffic management systems are better than current traffic management systems. The main key advantages is that, VANET system based on a real time traffic systems, that detect the signals of new nodes that connects with the network directly or indirectly and help to reduce the vehicular emission. From the last decade Vehicular Ad hoc Networks (VANET) is the challenges for communications engineering and traffic management safety systems.

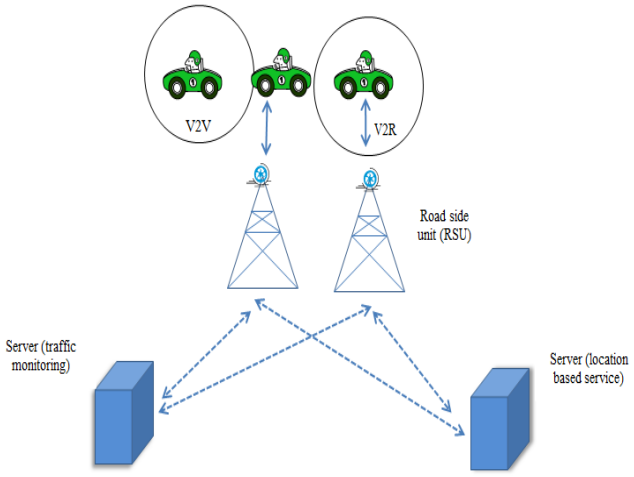

Fig 1.1 Architecture of Intelligent of Transport System

VANET's is a self-organizing and intelligence autonomous system which can manage the traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UMTS (Universal Mobile Telecommunication System), LTE (Long Term Evolution) and Wi-MAX

networks. The VANET has several advantages likeself-organization, lower local information dissemination time, low cost of implementation and low cost of maintenance, VANET is subgroup of MANET. VANET has wireless interface in which vehicle interconnected with each other. The vehicle can easily provide the required power for wireless communication, and adding antennas or additional communication hardware. The main aim of VANET is to develop the vehicular communication system to provide the secure and cost-efficient for the benefit of passenger safety and comfort. Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward (Delay Tolerant Networking) 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 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.

II. INTELLIGENT TRANSPORTATION SYSTEM (INTELLIGENT VANETS)

Vehicular ad-hoc network or VANET is also known as intelligent transportation system (ITS). Intelligent transportation system (ITS) has two types. In first one the vehicles communicate with each other called vehicle to vehicle communication (V2V) or inter vehicular communication and in second one vehicles communicate with the road side equipment's called as vehicle to road communication (V2R). In intelligent transportation systems, each vehicle that lies in active network act as sender, receiver, and router to broadcast information to the vehicular network or transportation agency plays an important role in the network session to secure, safe the data that travels from one node to another node and free flow of traffic.

- **Vehicle to vehicle communication (V2V)**

Vehicle to vehicle (V2V) communication perform the operation (sender, receiver and broadcasting) between vehicles. In vehicle to vehicle or inter vehicular communication has two types of message forwarding. First one is Naïve broadcasting and another one is intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. In this method broadcast message generated by the in front vehicle and the receiving vehicle sends its own broadcast message to other vehicles behind it. The prime disadvantage of this method is that the large number of collision occurs due to the broadcasting message by this the whole process and the delivery of message becomes slow. In intelligent broadcasting, if the vehicle detecting that they receives the same message from behind, it assumes that at least one vehicle in the back has received it and stop broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles.

- **Vehicle-to-Roadside Communication**

The vehicle-to-roadside communication configuration is responsible for a single hop broadcast where all equipped vehicles receive a broadcast message from the roadside equipment in the surrounding area. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside equipment for the reliable traffic flow. The distance between the two roadside units may be up to one kilometer or less, In heavy traffic the road side unit provides the high data rates to be maintained. For instance, when broad casting dynamic speed limits, according to its internal timetable and traffic rules the roadside equipment will determine the appropriate speed limits. The roadside unit send the broadcast message periodically when it detect the speed limit and will compare any geographic location or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the surrounded area. If a vehicle violates the speed limit that given in timeline database then the road side unit deliver the message in the form of auditory or visual warning to request the driver, they should reduce their speed.

III. LITERATURE REVIEW

Razzaque Mohammad Abdur et al.(2014)[2] have proposed the Mobility Pattern Based Misbehaviour Detection to Avoid Collision in Vehicular Adhoc Networks. This paper presents a misbehaviour detection scheme (MDS) and corresponding framework based on the mobility patterns analysis of the vehicles in the vicinity of concerned vehicles. Initial simulation results demonstrate the potential of the proposed MDS and framework in message's correctness detection, hence its corresponding applications in collision avoidance.

Zhang Linjuan et al. (2013)[3] has proposed a multilevel information fusion approach for road congestion detection in VANETs. In this paper, the authors have proposed a multilevel information fusion approach by combining the

fuzzy clustering based feature level information fusion (FCMA) and the modified Dempster–Shafer evidence reasoning-based decision level information fusion (D-SEMA). The FCMA can extract the key features from atomic messages, thereby greatly reducing the network traffic load. Furthermore, the D-SEMA mechanism is used to judge whether the road congestion event occurs.

Ghaleb F. et al.(2013)[4] proposed a mobility pattern based misbehaviour detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehaviour), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse or denial of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives :(i) physical movement and (ii) information security perspectives. This paper includes algorithms by which the misbehaviour can be detected.

Samara G. et al. (2010) [5] proposed various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, and Pranksters.

Seuwou.P et al. (2012) [6] proposed VANET as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst them (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in VANET, according to him the attacks are classified into two broad categories physical attack and logical attack.

Qian.yi et al.(2008)[7] proposed an overview on a priority based secure MAC Protocol for vehicular networks and he assume that the MAC Protocol can achieve both QOS and security in vehicular networks. In this paper he proposed that the MAC Protocol is having massages with different priority for different application to access DSRC (Dedicated short range communication channel) Chanel.

Javed.M.A. et al. (2010)[8] proposed "A Geo casting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management". In this paper he proposed the geo casting packet transmission technique to transfer safety message in a vehicular network. He uses OPNET based simulation model to analyses the performance of proposed protocol .According to him the VANET can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. The proposed protocol select the furthest vehicle for the rebroadcast with the help of new back off window design which reduces the number of packet transmission thus lowring the contention levels.

Hung c.c. et al. (2008)[9] proposed traditional ad hoc routing protocols are not well suited for this high dynamic network. In this paper they propose a new Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing for HVN. According to paper HVN integrates Wireless Metropolitan Area Network (WMAN) with VANET technology and reserves advantages of better coverage in WMAN and high data rate in VANET. Vehicles in HVN can communicate with each other and access Internet ubiquitously. They mainly focus on the routing issue for HVN, because the routing protocol for HVN is different from those used in MANET or VANET.

Dias .A.J. et al. (2011)[10]proposed a tested performance evaluation of DTN-based routing protocols applied to VDTNs(vehicular delay tolerant networks). The objective is to evaluate and understand how popular routing strategies perform in sparse or partitioned opportunistic vehicular network scenarios. This paper based on Spray and Wait protocol. The idea behind using this protocol is to exploit the physical motion of vehicles and opportunistic contacts to transport data between disconnected parts of the network.

Sumra A.I. et al.(2011)[11] proposed a key component of security in vehicular application if any component behave unexpectedly then it would be harmful for other users of the network. In this paper, they are proposed three different trust levels in peer to peer vehicular network. Purpose of proposed trust levels to discuss in detail is the functionality of different component of network which circumvents the attacker and emphasizes the role of trusted users in peer to peer vehicular communication. According to this paper Trust is combination of expectancy, belief in expectancy

and willingness to be vulnerable for that belief. This paper divide trust in three levels which are: zero trust level, weak trust level, strong trust level.

IV. OBJECTIVES

1. To study the literature of various collision detection and avoidance techniques in the VANETs.
2. To study the shortcomings and advantages of the existing solutions.
3. To design the mechanism for detection of point of collision.
4. To design the mechanism for the collision prediction using the movement analysis of vehicle node.
5. To design the mechanism to avoid the prediction collision by altering the movement vehicular.
6. To implement the new security mechanism in Network Simulator 2 (NS2).
7. To obtain and analyze the results.

V. METHODOLOGY

- We will start our research project by conducting a detailed literature review on the prankster attack in case of selfish driver in VANETs to know the problem in detail.
- A detailed security mechanism would be designed to prevent the prankster attack 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.
- Waterfall methodology comprises the following steps: working out system requirements, drawing up and approving the specification; design and prototyping; development; delivery; analysis and finalization.

VI. CONCLUSION

The proposed model has been designed to offer the collision free movement in the VANET cluster. The proposed model has been designed to work in the three layered model which comprised of point of collision detection, probability of collision calculation and collision avoidance methods. The proposed model is intended to solve the maximum problems arising in the VANETs in the case of collisions. The expected outcome must be obtained in the form of collision rate, probability of detection, probability of false alarm, etc. The experimental results are expected to solve the problems of collision and to overcome the problems in the existing model.

REFERENCES

[1] http://en.wikipedia.org/wiki/Vehicular_ad_hoc_network.

[2] Razzaque, Mohammad Abdur, Fuad A. Ghaleb, and Anazida Zainal. "Mobility Pattern Based Misbehavior Detection to Avoid Collision in Vehicular Adhoc Networks."In Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services, pp. 300-303. Springer International Publishing, 2014.

[3] Zhang, Linjuan, Deyun Gao, Weicheng Zhao, and Han-Chieh Chao. "A multilevel information fusion approach for road congestion detection in VANETs." Mathematical and Computer Modelling 58, no. 5 (2013): 1206-1221.

[4] Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin "Security and Privacy Enhancement in VANETs using Mobility Pattern" (IEEE, 2013).

[5] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures "Security Analysis and Challenges of Vehicular Ad Hoc Networks (VANET)" (IEEE, 2010).

[6] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)" (2012)

[7] Yi Qian ,Kejie Lu, and Nader Moayeri "PERFORMANCE EVALUATION OF A SECURE MAC PROTOCOL FOR VEHICULAR NETWORKS" (IEEE, 2008) .

[8] Muhammad A. Javed and Jamil Y. Khan "A Geocasting Technique in an IEEE802.11p based Vehicular Ad hoc Network for Road Traffic Management". (2010).

[9] Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks" (IEEE WCNC 2008).

[10] João A. Dias, João N. Isento, Vasco N. G. J. Soares, Farid Farahmand, and Joel J. P. C. Rodrigues "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" (2011 IEEE).

[11] Irshad Ahmed Sumra, HalabiHasbullah, J.AbMananMohsanIftikhar,Iftikhar Ahmad, Mohammed Y Aalsalem "Trust Levels in Peer-to-Peer (P2P) Vehicular Network"2011 IEEE.

[12] Steffen Moser, Simon Eckert and Frank Slomka "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE.

[13] Irshad Ahmed Sumra, HalabiHasbullah, Jamalul-lailAbManan, "VANET Security Research and Development Ecosystem", 2011 IEEE.

[14] Lu Chen, Hongbo Tang, Junfei Wang, "Analysis of VANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China pp.134-138.

[15] M. Khabazian, M. K. Mehmet Ali, "A Performance Modeling of Vehicular Ad Hoc Networks (VANETs)", 2007 IEEE.