INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Review paper on power control technique in VANET for catastrophe message broadcasting protocol

Naincy Duhan
dnaincy@gmail.com
CBS Group of Institution, Jhajjar, Haryana

Tarun Dalal
tarundalal88@gmail.com
CBS Group of Institution, Jhajjar, Haryana

ABSTRACT

Effectively broadcasting extremity messages in vehicular ad hoc networks is an important issue in VANETs. Real-time good fare message interchange is one of the most crucial subjects in VANET, and well fare message interchange mostly happens between close neighbors. By using this characteristic, we will give power control technologies which depend on connectivity, which diminish the access delay of safety packets. The dominant desire of VANET is to furnish life safety on the road. To obtain this, vehicles make use of two types of safety messages, first one is periodic safety messages in which vehicle speed and location will be given and another one is event-driven messages, which will telecast in case of an emergency environment for example accidents, hard-braking and many more. Our research work will be based upon to control power in control in extremity condition because power is one of the important parameters which we need to utilize efficiently so that optimum result can be achieved. Beside this, we deeply studied diverse routing protocol which will be useful to control power in an emergency situation, attack, and challenges which we have to face in implementing VANET.

Keywords—*VANET, RSU, NS-2 Network simulation, Traffic simulation, GPVR, OBU*

1. INTRODUCTION

Vehicular ad-hoc networks abbreviated as VANETs are a novel class of wireless networks that use moving the vehicle as nodes in a network to create a mobile network. It changes every participating vehicle into a wireless link, allowing each vehicle roughly 200 to 300 meters from each other to link and, in turn, form a network with a wide range. As vehicle drops out of the transmission range it drops out of the network, other vehicles can join in, connecting vehicles to one another so that a network is created. It is assessed that the first organization that will incorporate this knowledge can be police and fire vehicles to connect with each other for protection purposes. The main idea behind VANET is providing communication among vehicles and also among vehicles and a number of static equipment located on the road. Several research projects have focused on this exciting and useful area in order to implement it in the best possible way. The main objective is to increase vehicle as well as passenger safety and ease. Among its services crash warnings, road sign alarms and automatic toll/parking payment can be discovered.

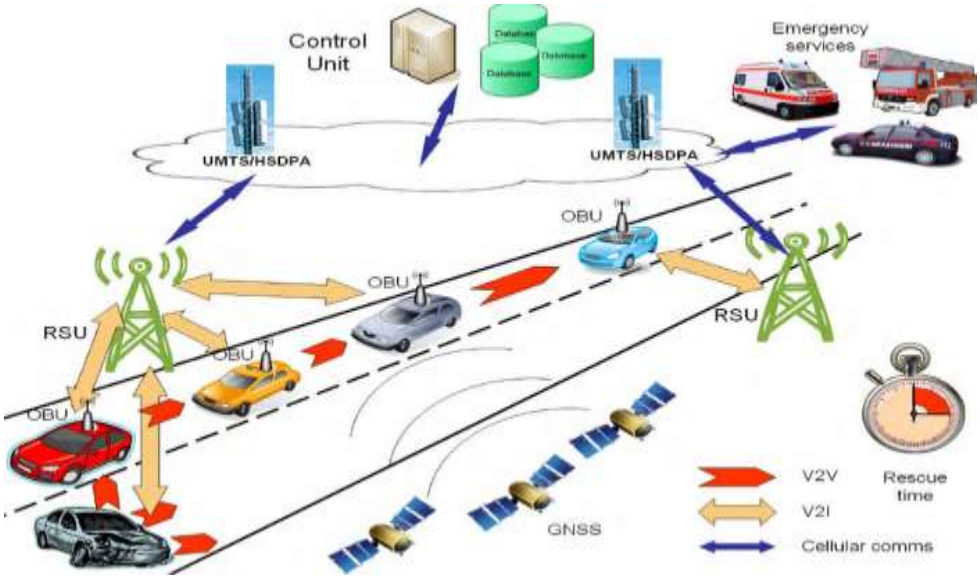

Fig. 1: VANET communication V2V and V2 I

Vehicular ad hoc networks (VANETs) are expected to support a large spectrum of mobile distributed applications that range from traffic alert dissemination and dynamic route planning to the context-aware advertisement and file sharing. Considering a large number of nodes that participate in these networks and their high mobility, debates still exist about the feasibility of applications that use end to end multi-hop communication. The main concern is whether the performance of VANET routing protocols can satisfy the throughput and delay requirements in diverse applications.

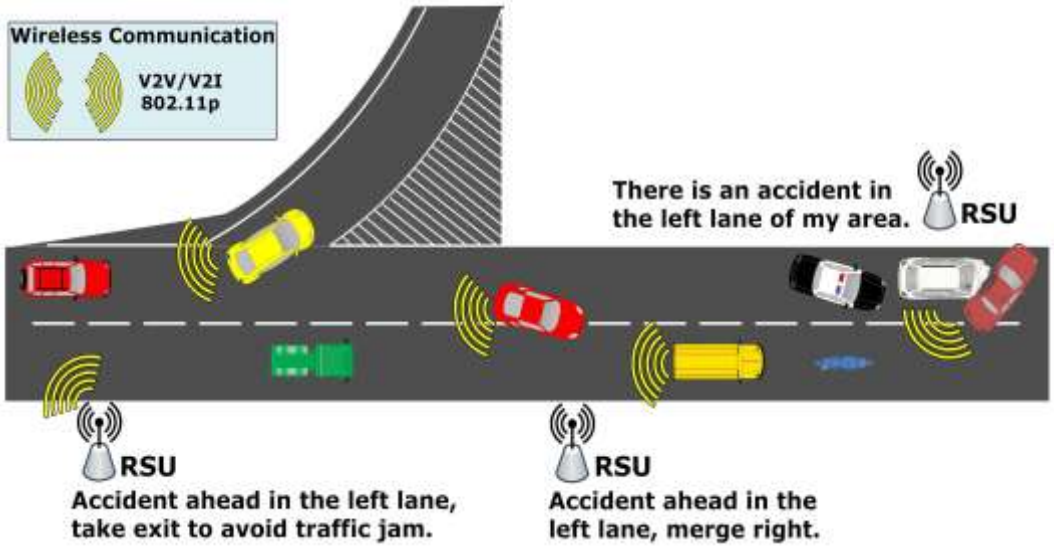

Fig. 2: Application of VANET to avoid the accidental area and traffic jam

2. RELATED WORK

Yuzhong Chen, et al: In this study, a novel multi-hop clustering scheme for VANETs, which generates cluster heads (CHs) via neighborhood follow the relationship between vehicles, is proposed. The scheme is based on a reasonable assumption that a vehicle cannot certainly identify which vehicle in its multi-hop neighbors is the most suitable to be its CH, but it can easily grasp which vehicle in one-hop distance is the most stable and similar to it, and thus, they most likely belong to the same cluster. Consequently, a vehicle can choose its CH by following the most stable vehicle. The relative mobility between two vehicles combining the gains based on the followed number and the historical following information enables a vehicle to select which target to follow. Extensive simulation experiments are conducted to validate the performance of the proposed clustering scheme [7]. Lina Bariah, Det al: VANETs are of an increasing importance as they enable accessing a large variety of ubiquitous services. Such an 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 providing a structured and comprehensive overview of the recent research advances on VANETS security services, surveying the state-of-the-art on security threats, vulnerabilities and security services, while focusing on important aspects that are not well-surveyed in the literature such as VANET security assessment tools [8]. Tasneem Darwish et al: Vehicular ad hoc networks (VANETs) are gaining tremendous interest among researchers and industries. Although the main reason for developing VANETs is traffic safety, many applications such as traffic status monitoring, road traffic management, routing and distribution of data, have emerged. VANETs exploit multi-hop communications among vehicles to deliver data packets. However, with fast mobility and intermittent link connectivity between vehicles, efficient and reliable routing in VANETs is becoming a challenging task. In order to make routing protocols robust to frequent communication disruptions and aware of unstable traffic and network conditions, several new routing metrics have been integrated with routing protocols. Such protocols are called traffic-aware routing (TAR) protocols as their routing decisions are influenced by traffic and network status. The goal of this paper is to review the most recent traffic-aware routing protocols while emphasizing traffic and network conditions awareness issues [9]. Le Zhang et al: This paper presents the cooperative POC-based forwarding (CPF) protocol for highway vehicular networks, which extends the repetition-based POC-MAC protocol for multi-hop transmissions. At each forwarding hop, multiple cooperating relays form a virtual relay and schedule their transmissions to correspond to a single POC codeword, thereby adhering to the POC-MAC. CPF exploits spatial diversity while mitigating the effect of hidden terminals. By allocating separate POC-based schedules for multi-hop packets and the periodic broadcast of safety heartbeat packets, the CPF protocol reduces the interference between the two. The performance of the CPF protocol is studied through analysis using a Markov model and through ns-2 simulations [10].

3. ROUTING PROTOCOL IN VANET

The protocols of routing employed in VANETs may be broadly categorized into three.

- Proactive or Table-driven protocol of routing
- Reactive or On-Demand Routing protocol
- Hybrid protocol

Every protocol has distinct advantages and limitations of its own. In the highly mobile network topology of VANETs precise choice of the protocol would become a dire necessity considering the hectic conditions of traffic, several inherent problems of the dynamic network and the conservation of available wireless bandwidth.

3.1 Proactive Routing Protocol: Proactive routing protocol maintains certain distinct features related to the routing information in the background, such as the next forward hop, irrespective of the communication requests. There is a continuous broadcast of the control packets to the point of flooding the nodes in order to maintain the routes or the state of links between pairs of nodes, in spite of the fact that certain paths are hardly used. Then, a table is constructed inside the node itself in such a way that any entry in the table signifies the next hop node in the direction of a specific destination. The greatest advantage of this routing protocol is the very absence of route discovery, as the background constantly maintains the path towards the destination which is available anytime upon lookup and providing low latency for real-time applications.

3.2 Reactive Routing Protocol: Reactive routing is a requirement-based on-demand protocol. The route is made available only when the node needs to transmit to another node. It has a great advantage of the gross reduction in the burden of the network, as it maintains only such routes which are used at any point in time. Consequently, the reactive routing obviously contains the phase of route discovery, where the query packets in search of a route flood the network. When the required route is discovered the phase is auto-terminated. The general approaches of reactive routing include the protocols such as Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector routing (AODV) etc.

3.3 Hybrid Protocol: Hybrid protocol result out of a judicious fusion of the best features in the proactive as well as the reactive routing as in Regional Routing Protocols (RRP) and Secure Link State Routing Protocol (SLSP). In certain contexts, for instance, a node could be employing a proactive routing protocol to communicate with its proximate node and at the same time could be using the reactive routing protocol in order to communicate with a node distant from it. That is to say that proactive routing protocols are preferable when a node attempts to reach another node within the certain geographical location and similarly reactive protocols are preferable in reaching the other nodes outside the specified geographical area. In dealing with such nodes having high mobility as in VANETs, the reactive protocols are more suited with their on-demand routing nature.

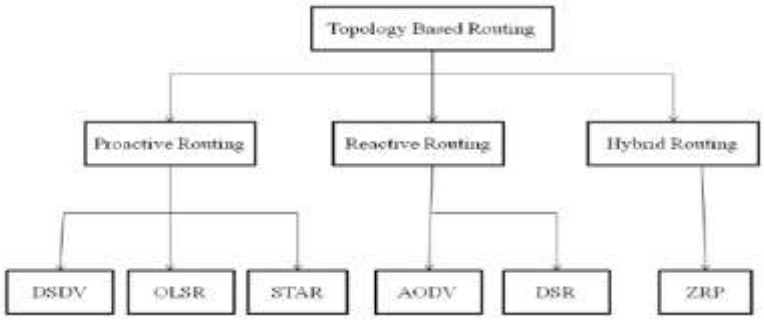

Fig. 3: Classification of routing protocols

4. ATTACK AND CHALLENGES IN VANET

4.1 Attacks in VANET

Besides having advantages of the proxy re-encryption method for authentication, there are still some attacks that can be possible that are explained as follows:

- Denial of Service (DoS) attack
- Eavesdropping
- Key Bootstrapping and Rekeying

Attackers may seek to initiate excessive un-authentication requests in order to exhaust the resources of the Access Point (AP). A general solution would be to limit the number of authentication requests which can be processed in a unit of the time period. This method can guarantee that the server is not overwhelmed by DoS. But this could also delay a request. The implementation of the schemes must take such trade-offs into consideration. In eavesdropping: since the session key is calculated based on the nonce's contributed by the car and the AP respectively. Both of the car's nonce and the AP's nonce are encrypted by the public key of the SP during transmission. The attacker can reveal the session key if he/she got the SP's private key, or an appropriate re-encryption key/private key pair. Anonymous keys are preloaded by the transportation authority or the manufacturer, but with different consequences. Moreover, while ELPs (Electronic license Plate) are fixed and should accompany the vehicle for a long duration (potentially its life cycle), anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired. This renewal can be done during the periodic vehicle checkup (typically yearly) or by similar procedures. In addition to the ElP and anonymous keys, each vehicle should be preloaded with the Certificate Authority's (CA) public key.

4.2 Challenges in VANET

- Mobility and Volatility
- Privacy VS Authentication
- Privacy VS liability
- Network Scalability
- Location Awareness

The basic idea from Ad Hoc Networks is that each node in a MANET is mobile, and can move from one place to another within the coverage area, but the mobility speed is limited. But, in Vehicular Ad Hoc Network nodes moving with high speed, vehicles make a connection with other vehicles which are available inside its communication range, and this connection exists for only a few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is

a hard problem. Liability will give a good opportunity for legal investigation and this data cannot be denied (in case of accidents), on the other hand, the privacy must not be violated and each driver must have the ability to keep his personal information from others (Identity, Driving Path, and Account Number for toll Collector etc.). The scale of this network in the world approximately exceeding the 750 million nodes, and this number is growing, another problem arises when there is no global authority to govern the standards of this network, for example, the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles are deferent from the BMW one.

4.3 Software NS 2

We proposed a data Aggregation model and that improves the performance parameters of the system. In our research work, we will show how the protocol performs better in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN. There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol. To carry out research work we will use NS-2 (2.35), a network simulation tool to simulate a wireless communication network. NS2 is a discrete event simulator developed. It provides a good platform for WSN simulation. The random waypoint model is selected as a mobility model

5. CONCLUSION

During in recent years, Intelligent Transport Systems have experienced a tremendous growth in academic as well as industrial. Main focus of ITS is to enhance safety and power control in emergency situations. In this types of networks, every node represents intelligent vehicles that can transfer either between themselves to interchange traffic information or with the roadside unit (RSU) to distribute or request crucial information. Therefore, the overcrowding control remains one of the most tedious complications of these networks. In our review paper, our main target is to use utilization of power in the adverse situation. The main idea behind VANET is providing communication among vehicles and also among vehicles and a number of static equipment located on the road. Vehicle density assessment is a lead factor for n-way search system to find the farthest vehicle in VANETs. An effective technique can be used to analyze the vehicle density by controlling the transmission power strength. In these days IoT, artificial intelligence also in huge demand, therefore, we can integrate it with VANET to get a more appropriate result.

6. REFERENCES

[1] Preeti Rawat, Shikha Sharma, “Deep: Density-aware emergency message extension protocol for VANETs,” IEEE Transactions on Wireless Communications, vol. l2, pp. 2926–2940, 2016

[2] Neha Kushwah, Abhilash Sonker, “The broadcast storm problem in a mobile ad hoc network,” in Proceedings of the ACM International Conference on Mobile Computing and Networking (MOBICOM), 2016, pp. l53–l67

[3] Ramesh C. Poonia, Deepshikha Bhargava., “Survey of position based routing for Inter-Vehicle Communication system”, Distributed Framework and Applications, 2008. DFmA 2016, First International Conference on, pp.l74-l82, 2l-22 Oct. 2008

[4] Samiksha, Anit Kaur, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks." Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Tel Aviv, Israel, March 2000, p. 3–l2.

[5] Mayank Bhatt, Shabnam Sharma, Aditya Prakash, Dr. U.S.Pandey, Dr. Kiran, "IEEE standard 802.l6: A technical overview of the wireless MANTM air interface for broadband wireless access", IEEE Communications Magazine, vol. 40, no. 6, Jun 2016, pp. 98–l07.

[6] Mohammad Fathian, Ahmad Reza Jafarian-Moghaddam. “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks,” IEEE Personal Communications, vol. 6, no. 2, pp. 46–55, 2015

[7] Yuzhong Chen, Mingyue Fang, Song Shi “Stationary of Random Direction Direction models”, 20l5 Second International conference on network security, wireless communications and trusted computing.

[8] Lina Bariah, Dina Shehada, Ehab Salahat and Chan YeobYeun Simulation-based performance evaluation of theSNDP protocol for infrastructure WMNs. In Proc. 24th IEEE Int Advanced Information Networking and Applications (AINA) Conf, pages 90{97, 2015

[9] Tasneem Darwish · Kamalrulnizam Abu Bakar A highly adaptive distributed routing algorithm for mobile wireless networks. In Proc. IEEE Sixteenth Annual Joint Conf. of the IEEE Computer and Communications Societies INFOCOM '97, volume 3, pages l405-l4l3, 2014.

[10] Le Zhang, Behnam Hassanabadi, ShahrokhValaee In Proc. Second IEEE Workshop Mobile Computing Systems and Applications WMCSA '99, pages 90{l00, 2014

[11] Z. Hasan, H. Boostanemehr, and V. K. Bhargava, "Green Cellular Networks: A Survey, some research Issues, and Challenges," Communications Surveys & Tutorials, IEEE, vol.l3, no.4, pp. 524-540, Fourth Quarter 2011.

[12] P. Bianzino, C. Chaudet, D. Rossi and J. l. Rougier, “A Survey of Green Networking Research,” Communications Surveys & Tutorials, IEEE, vol.l4, no.l, pp. 3-20, First Quarter 2012.

[13] W. A. Moreira, R. Lopes Gomes, and A. J. Gomes Abelem. A multiple metric approaches for routing in wireless mesh networks. In Proc. IEEE Int. Symp. a World of Wireless, Mobile, and Multimedia Networks & Workshops WoWMoM 2009, pages l-6, 2009.

[14] F. Farnoud and S. Valaee, “Reliable broadcast of safety messages in vehicular ad hoc networks,” in Proceedings of the IEEE INFOCOM, the Annual Joint Conference of the IEEE Computer and Communications Societies, 2009, pp. 226–234.

[15] L. Zhang, B. Hassanabadi, and S. Valaee, “Cooperative positive orthogonal code-based forwarding for multi-hop vehicular networks,” IEEE Transactions on Wireless Communications, vol. l3, pp. 39l4–3925, 20l4

[16] Y. Bi, H. Zhao, and X. Shen, “A directional broadcast protocol for emergency message exchange in inter-vehicle communications,” in Proceedings of the IEEE International Conference on Communications (ICC), 2009, pp. l–5.

