ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com

Research Article

EFFICIENT WAY OF EMERGENCY MESSAGE DISSEMINATION AND RELIABLE BROADCAST IN VEHICULAR AD-HOC NETWORK

Maheswari. R*, Dr.T.V.U.Kiran Kumar**
*Research Scholar, Bharath Institute of Higher Education and Research, Bharath University, Chennai.
**Professor, Bharath Institute of Higher Education and Research, Bharath University, Chennai.

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

In this paper, for a wide range of vehicular scenarios a efficient protocol for vehicular ad hoc networks has been proposed. Safety related message may transmission is an effective way to contain life critical information, it is a necessity that the sender as well as the message are authentic. which only employs local information acquired via periodic beacon messages, containing the both acknowledgment and emergency detection mechanisms of the circulated broadcast messages. However it is fraught with fundamental challenges such as message redundancy, hidden terminals and broadcast storms, which greatly degrade network performance. This is being tested with implemented at the road intersections without any need to even recognize inter sections .First, as no acknowledgment (ACK) mechanism is applied for broadcast messages in the medium-access-control (MAC)layer, message loss due to packet collisions or poor channel conditions cannot be easily detected. To other vehicles as fast and reliable as possible , the traditional broadcasting scheme without an (ACK) mechanism is not suitable for emergency message delivery in IVC, due to the limited transmission range, message relaying from intermediate nodes is required to reach remote vehicles. Therefore the objective of the research is to survey broadcast in vehicular networks. We analysis the different protocols and simulation using NS-2.

Keywords: Broadcast storm; Message redundancy; Reliability; Beaconing; Medium-access-control; Efficiency; Vehicular network.

I. Introduction

A vehicular ad hoc network (VANET) uses moving cars as nodes in a network to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

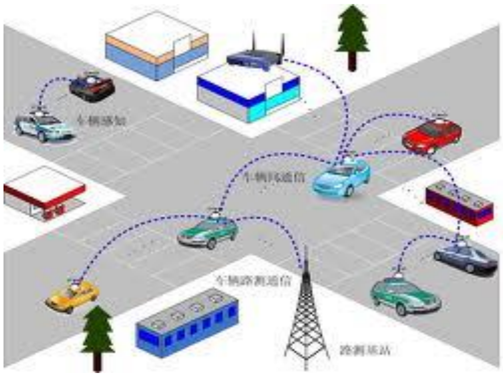


Fig.1.Moving nodes in VANET.

Able to exchange information within these networks without permanent infra structure. The excessive retransmission problem is first formulated as an optimization problem and show that it is NP-hard even if the upper layer service is periodical beacon exchange.

II. Characteristics of Vanets

Compared to standard ad hoc networks, VANETs have several properties that introduce particular security challenges, which are not of major concern in other mobile ad hoc networks. Some major properties of VANETs:

Offline-infrastructure - Communication to a fixed infrastructure is possible, but it is unlikely that there is a permanent connection to this infrastructure. Infrastructure gateways are supposed to be located at gas stations, parking lots or even on selected points at the road side but not everywhere along the road side. We call this type of fixed infrastructure an offline-infrastructure, since in contrast to what we call online infrastructure, it is not available all the time but only during (from the vehicles point of view) random periods of time. Dynamic topology - One important characteristic of VANETs is that nodes move with high speed in respect to each other, which results in a very high rate of topology changes. Whereas for example during a conference people carrying PDAs ”move” with a speed of 2ms with respect to each other, cars on a highway normally easily achieve 55mswhen taking into account oncoming traffic.Critical application requirements - Another important property is that applications within VANETs are often safety critical and time-critical (e.g. alert messages, warnings, see section III for further details). Ad-hoc networks that mainly serve to distribute data do not underlie these aspects.Auxiliary information - Furthermore, nodes in VANETs are context aware, they have access to additional data such as car sensor data or GPS. The usage of these so called ”side-channel” information can be valuable when evaluating data obtained through communication with other nodes in the VANET.Beside the specific properties, the application scenario of VANETs requires the achievement of special (security) goals. Privacy - In some cases services in a VANET are related to personal data, such as current location or current speed, which requires anonymity in order to protect a driver’s privacy. On the other hand, other services require identification and traceability. Integration - Vehicles are not computers, applications or services in VANETs must work without interaction. Drivers cannot act as administrators. For VANET nodes, battery power is not an issue (at least while driving).

III. Inter-Vehicle Communication Networks (IVCN)

The Inter Vehicle Communication systems are a new paradigm of networking. Largely related to mobile ad hoc networks and their distributed, self-organizing structure, they also introduce new threats.

The IVCN has some characteristics that are different of the conventional wireless local area:

Base station: The autonomous distributed IVCN does not have any base station. Each vehicle transmits its cruising information and receives another vehicle’s information.

- **Communication among unknown and unspecified vehicles:** Each vehicle communicates with unknown and unspecified vehicles accidentally neighbouring on the road.
- **Importance of the distance between vehicles:** The cruising information that a vehicle needs differs from what another vehicle needs. Therefore, the importance for a vehicle of another vehicle’s information grows with decreasing the distance between the vehicle and another vehicle.

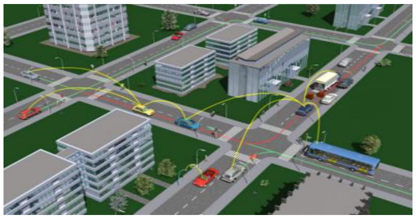


Fig 2.IVCN.

In Intelligent Transport Systems (ITS), it has exchange necessity information between vehicles such as position and speeds in order to guarantee an efficient trip and insurance. Through the IVCN, each vehicle it can change to such information with its neighbours. In IVCN the security and the privacy are critical factors and challenges to have in account throughout all the phases of project. In the ITS technology, inter-vehicle communication (IVC) system with a capability of multi hop connection has received a significant amount of attention. Multi hops communication can offer a number of benefits such as overcoming dead-spots, reduction of transmitting power, and increasing system capacity even when no assistance of backbone infrastructure is available. In IVCN the frequent topological changes can provoke undesirable disconnections of radio links, for example, the sudden change of the band of set of wheels of a vehicle heavy (such as a truck and/or bus) can introduce a shade zone and, consequent loss of signal in the communication between fast vehicles, and an increase of distance between vehicles can reduce the power of the signal required in the reception. Fig. 3 represents multi hops.

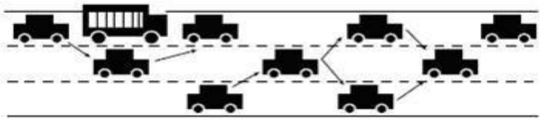


Fig. 3 Multi hops communication.

The problems of security in IVCN are similar those finding in typical Ad hoc networks. However, the developed protection mechanisms for ad hoc networks are not directly applicable in IVCN. The messages related with the road traffic and the acknowledgments of the danger are the aspects most important in a Vehicle-to-Vehicle communication, in a scene where the Inter vehicle communication is supported by infrastructures of support to the road traffic (Access Points). These scenes (Vehicle-to-Infrastructure) can be white of attacks of badly intentioned we. It considers, for example, that "they had contaminated" a parcel of the net with the false information: an only knot can transmit acknowledgments false of the danger (for example, icing in the roads), for its neighbours and, consequently, the remains we of the network. Or same a vehicle that forges the emergency messages to take off advantage, in situations of bottling of the road traffic. Figure Illustrates the transmission of message of inexistent accident.

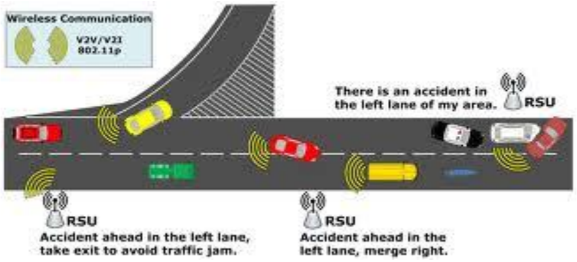
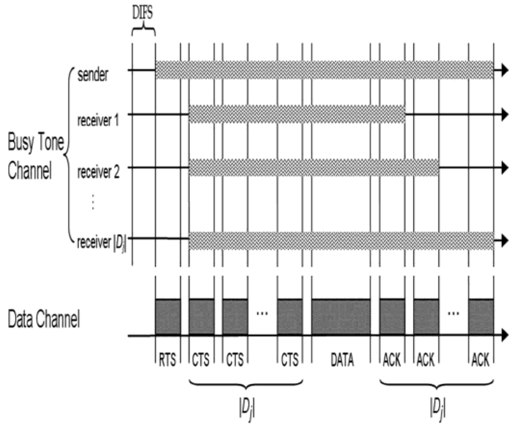

Wireless Communication
V2V/V2I
802.11p
There is an accident in the left lane of my area.
RSU
RSU
Accident ahead in the left lane, take exit to avoid traffic jam.
RSU
Accident ahead in the left lane, merge right.

Fig.4.Route Map on the highway.

IV. Related works on broadcast protocol

The IEEE802.11 broadcast protocol which is based on Carrier sense multiple access with collision avoidance (CSMA/CA)

1. They include broadcast support multiple access (BSMA)
2. Broadcast medium window (BMW)
3. Batch mode multicast MAC(BMMM)
4. Location aware multicast MAC(LAMM)



The objective of MAC extension design is to maximize the probability (minimize the PRF) that a safety message is received by all vehicles within the message range within the message lifetime. The strategy explored here is to repeat the message a certain number of times within its lifetime. We explore six variations on the repetition idea. We examine synchronous and asynchronous designs, repetition with and without carrier sensing, fixed number, and p-persistent repetition.

We eschew reliability by RTS/CTS or ARQ protocols. These require unicast communication and achieve reliability by receiver feedback. The sender needs to learn the network addresses of its receivers. When there are many receivers or the network is highly mobile, i.e., the set of receivers can change a lot, learning identities may themselves require significant communication.

Therefore, we have chosen to evaluate ways to enhance reliability without receiver feedback. The above figure illustrated the idea of repetitive transmission. It shows two transmitters within interference range of one receiver each generating a message at the same time. Every repetition of the message is a new packet. At each transmitter, the protocol evenly divides the message lifetime (τ) into n =_τ/t trans_ slots, where _x_ is the largest integer not greater than x, τ is the lifetime, and ttrans is the time needed to transmit one repetition as well as the slot duration. We randomly pickan y k (1 ≤ k ≤ n) slots to repetitively transmit the message.

If any one or more of the packets corresponding to the message are received by that receiver without collision at a given receiver, the message is received within its useful lifetime and is considered successful. On the other hand, the message fails at the receiver if all its repetitions are lost due to collisions.

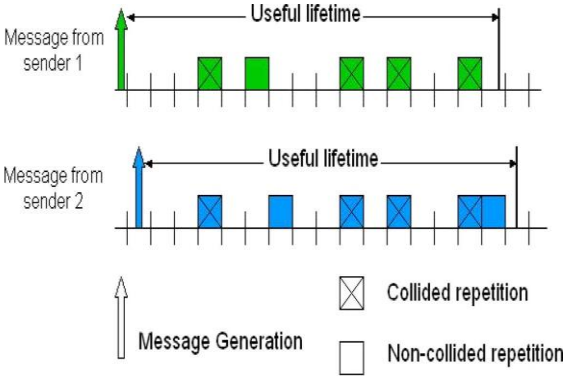


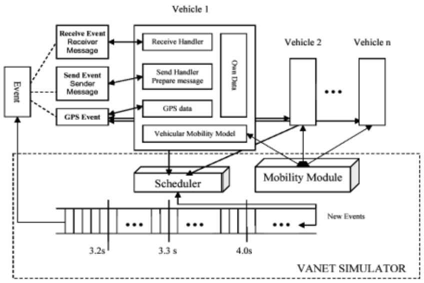
Fig.5. Concept of repetitive transmission.

V. Acknowledgment Based Broadcast Protocol for Reliable and Efficient Data Dissemination

A broadcast algorithm suitable for a wide range of vehicular scenarios, which only employs local information acquired via periodic beacon messages, containing acknowledgments of the circulated broadcast messages. Each vehicle decides whether it belongs to a connected dominating set (CDS). Vehicles in the CDS use a shorter waiting period before possible retransmission. At time-out expiration, a vehicle retransmits if it is aware of at least one neighbor in need of the message. To address intermittent connectivity and appearance of new neighbors, the evaluation timer can be restarted. Our algorithm resolves propagation. At road intersections without any need to even recognize intersections. It is inherently adaptable to different mobility regimes, without the need to classify network or vehicle speeds. In a thorough simulation-based performance evaluation, our algorithm is shown to provide higher reliability and message efficiency than existing approaches for non safety applications. We develop the Acknowledged Broadcast from Static to highly Mobile (ABSM) protocol [3], a fully distributed adaptive algorithm suitable for VANETs with all mobility scenarios The parameter less broadcast in static to highly mobile(PBSM) adhoc networks protocol

VI. Urban multi hop broadcast protocol(UMB)

ABSM has turned out to be a very robust and reliable protocol, that extremely reduces the number of transmissions needed to complete a broadcasting task. The developing standards like DSRC. The protocol will also be analyzed when infrastructure nodes also take part in data messages dissemination. The Broadcast Storm in Ad hoc Wireless network Routing protocols developed for ad hoc wireless networks use broadcast transmission to either discover a route or disseminate information. More specifically, reactive routing protocols has to flood the network with a route request (RREQ) message in order to find an optimal route to the destination. Several applications developed for vehicular ad hoc wireless networks (VANET), which is a subset of MANET, rely on broadcast to propagate useful traffic information to other vehicles located within a certain geographical area. However, the conventional broadcast mechanism may lead to the so-called broadcast storm problem.



In this paper, we explore how serious the broadcast storm problem is in both MANET and VANET by examining how broadcast packets propagate in a 2-dimensional open area and on a straight road or highway scenarios. In addition, we propose three novel distributed broadcast suppression techniques; i.e., weighted p-persistence, slotted 1-persistence, and slotted p-persistence schemes. Our simulation results show that the proposed schemes can achieve up to 90% reduction in packet loss rate while keeping the end-to-end delay at acceptable levels for most VANET applications.

VII. A Multi-Channel Token Ring Protocol (MCTRP)

A multi-channel token ring media access control (MAC) protocol (MCTRP) for inter-vehicle communications (IVC). Through adaptive ring coordination and channel scheduling, vehicles are autonomously organized into multiple rings operating on different service channels. Based on the multi-channel ring structure, emergency messages can be disseminated with a low delay. With the token based data exchange protocol, the network throughput is further improved for non-safety multimedia applications. An analytical model is developed to evaluate the performance of MCTRP in terms of the average full ring delay, emergency message delay, and ring throughput. Extensive simulations with ns-2 are conducted to validate the analytical model and demonstrate the efficiency and effectiveness of the proposed MCTRP.

VII. Simulation: Simulation was made comparison to evaluate the performance of BPBT with BMW and BMM for three network –layer services

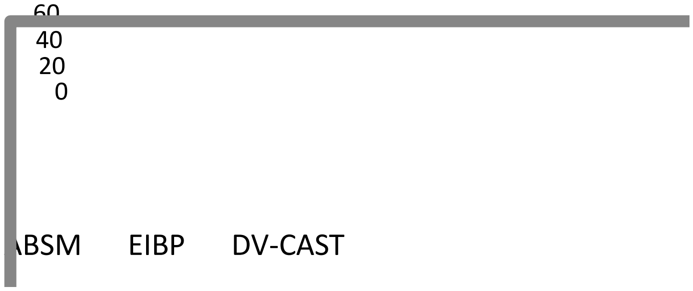


Fig.6. Comparison Result Average delay vs No.of Vehicles.

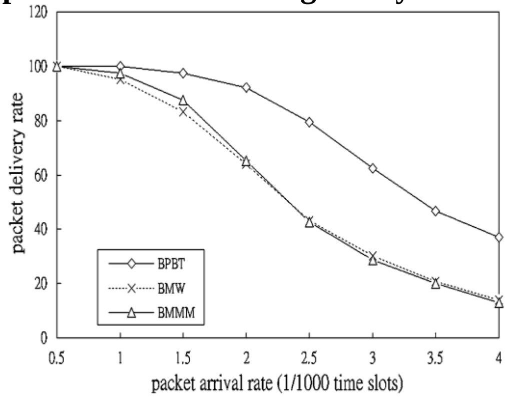


Fig.7 Packet delivery rate of multicasting streams with different packet arrival rates.

VIII. Conclusion

The technologies that uses moving cars as nodes in a network to create a specific mobile network able to exchange information to prevent broadcast storm by selecting a subset of neighbouring nodes to forward the message the next step is using CLBP it can minimize the broadcast message redundancy quickly and reliable deliver in IVC & next WTRP was proposed for intelligent Transportation system(ITS).In vehicular Ad-hoc networks are expected to support the diverse infrastructure based commercial services ,including internet access, real-time traffic concerns, video streaming and content distribution, one of the greatest advantage of using protocol ERBP using NS-2 tool can minimize the message redundancy and broadcast storm this can be reconfigured when necessary to improve performance.

References

1. Yuanguo Bi, Lin X. Cai.” Efficient and Reliable Broadcast in Intervehicle Communication Netwoks: Across-Layer Approach” IEEE Transactions on Vehicular Technology, Vol.59, No.5,June 2010.
2. Y. Bi, K. H. Liu, L.X. Cai. X. Shen, and H. Zhano, “ A multi-channel token ring protocol for Qos provisioning in inter_vehicle communications”, IEEE Trans. Wireless Commun.,vol.8.no.11,pp.5621-5631,Nov.2009.
3. Y. -C. Tseng, S. -Y. Ni, Y.-s Chen, and J. -p. sheu, ” The broadcast storm problem in a mobile ad doc network,” Wireless Network., vol.8, no.2/3, pp.153-167, Mar.2002.

4. M. Raya and J.Hubaux., “Ack based – broadcast protocol for Reliable & Efficient Data Dissemination” 2012.

5. A.solanas,J.Hubaux,, ”A multi-channel Token ring Protocol for Qos Provising in Inter-Vehicle Communications” vol..8.No.11 ,.Nov.2009.

6. K. Tang and M. Gerla, “MAC reliable broadcast in ad hoc networks,” in Proc. IEEE MILCOM, Oct. 2001, pp. 1008–1013.

7. M. T. Sun, L. Huang, A. Arora, and T. H. Lai, “Reliable MAC layer multicast in IEEE 802.11 wireless networks,” in Proc. IEEE ICPP, Aug.2002, pp. 527–536.

8. S. T. Sheu, Y. Tsai, and J. Chen, “A highly reliable broadcast scheme for IEEE 802.11 multi-hop ad hoc networks,” in Proc. IEEE ICC, May 2002, pp. 610–615.

9. J. Kuri and S. K. Kasera, “Reliable multicast in multi-access wireless LANs,” in Proc. IEEE INFOCOM, Mar. 1999, pp. 760–767.

10. S. K. S. Gupta, V. Shankar, and S. Lalwani, “Reliable multicast MAC protocol for wireless LANs,” in Proc. IEEE ICC, May 2003, pp. 93–97.