ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Providing Secure Multihop Broadcast Solutions for Intervehicular Communication

Md. Ashraf Ali
M.Tech Student,
Lords Institute of Engineering And Technology.

T. Manohar
Associate Professor,
Lords Institute of Engineering And Technology.

Abdul Majeed,
HoD & Associate Professor,
Lords Institute of Engineering And Technology.

ABSTRACT

Intervehicular communication (IVC) is an important emerging research area that is expected to considerably contribute to traffic safety and efficiency. In this context, many possible IVC applications share the common need for fast multi-hop message propagation, including information such as position, direction, and speed. However, it is crucial for such a data exchange system to be resilient to security attacks. Conversely, a malicious vehicle might inject incorrect information into the intervehicle wireless links, leading to life and money losses or to any other sort of adversarial selfishness (e.g., traffic redirection for the adversarial benefit). In this paper, we analyze attacks to the state-of-the-art IVC-based safety applications. Furthermore, this analysis leads us to design a fast and secure multi-hop broadcast algorithm for vehicular communication, which is proved to be resilient to the aforementioned attacks.

Keywords— VANETs, Emergency Warning Messages, Abnormal Vehicles

INTRODUCTION

INTERVEHICULAR COMMUNICATION (IVC) is among the most promising and challenging applications of vehicular ad hoc networks (VANETs). Many applications are possible in this context, yet local danger warning systems remain the most prominent ones. Most of these safety-related applications, including state-of-the-art ones, share properties that put them into the same class of solutions: IVC-based vehicular safety applications.

These common properties are listed as follows.

1) Communication is generally vehicle-to-vehicle (V2V), without infrastructure.

2) Vehicles exchange messages that contain their position, direction, speed, and possible dangers.

3) Broadcast messages have to be propagated as quickly as possible within a certain area of interest, even though multi-hop forwarding.

4) Specific algorithms are employed to choose as few forwarders as possible over the multi-hop path to fasten the propagation of alert messages.

5) Vehicles' information such as position, direction, speed, and transmission range is used to feed the forwarder selection algorithm.

The Vehicular Ad hoc Network (VANET) is a technology having the art of integrating ad hoc network, wireless LAN and cellular technology to achieve intelligent Inter-Vehicle Communications (IVC) also known as Vehicle-to-Vehicle(V2V or C2C) communications and Roadside-to-Vehicle Communications (RVC or R2V) [1]. Vehicular Ad hoc Network (VANET) is a type of Mobile Ad hoc Network in which communicating nodes are vehicles and roadside communication equipments. In VANETs nodes can communicate with each other without the use of central access points, means that vehicular nodes are treated as "computers on wheels" or "computer networks on wheels". The FCC (Federation of Communication Consortium) allocated a frequency spectrum for V2V and V2R or R2V wireless communication in 1999. The commission then established Dedicated Short Range

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Communication(DSRC) services in 2003 using frequency band of 5.850—5.925 GHz. Some of the characteristics of VANETs which differentiates it from other mobile ad hoc network are frequent changing topology and high mobility, no power constraint, geographical positioning availability, hard delay constraints and modeling mobility and corresponding prediction. Fig.1 below explains the structure of VANET.

VANETs provide us the valuable concept for improving efficiency and safety of future transportation. For building VANETs, the basic infrastructure requirements are equipment of radios working in unlicensed band and sensors in the vehicles for V2V communication, deployment of info stations (access-points) for V2I communication provides a way for internet access [2]. Info stations cannot be used for latency critical applications e.g. safety applications. Communication Standards like 2G, 2.5G, 3G, 4G and Wi-Fi is also one of the basic infrastructure requirements but there is trade-off between data rate and data mobility for communication standards e.g. the Wi-Fi supports high data rate carrying capacity but low or no mobility support. Now a day's 4G promises to supports high data rate and high mobility but it costs more. So, the main challenge in choosing communication standard for VANETs is to choose such a standard that could support both high mobility and high data rate with low cost.

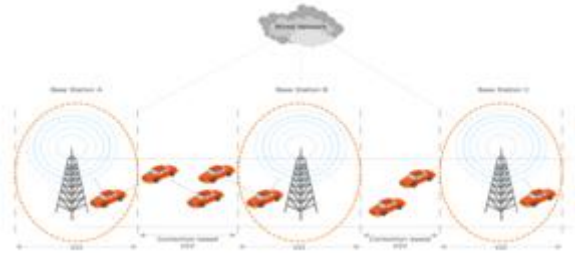

Fig: Intervehicular communication

VANETs system architecture from the network architecture view [1] includes related protocols in Physical Layer(deals with the frequency spectra used by different IVC apart from issues such as the antenna and modulation), MAC Layer (used for avoiding transmission collision and onboard infotainment services in VANET), Network Layer (provides multi-hop communication based on geographic addressing and routing and executes functions like congestion control) and application Layer (there are various application classes based on the vehicle's role). Major challenges in the field of VANET research are IVC Security, Position Verification Approaches, Scalability problem and MAC protocols, Availability of DSRC spectrum (5.9 GHz) and its channelization, Congestion Control & Performance Surveillance application of IVC through vehicular Sensor Networks. The introduction of IEEE 802.11 along with advanced wireless ad-hoc networks and location-based routing algorithms makes vehicle-to-vehicle communication viable. Applications for inter-vehicle communication include intelligent cruise control, lane access and emergency warning systems among others. Vehicular systems employ wireless ad-hoc Networks and GPS to determine and maintain the inter-vehicular separation necessary to ensure the one hop and multi hop communications needed to maintain spacing between vehicles. Location based routing algorithms are flexible and efficient enough with regards inter-vehicular communication so, they form the basis of any VANET [3].

LITERATURE REVIEW

Since, the evolution of VANETs various techniques and concepts have been used in order to overcome the above depicted problems while propagating security alerts or emergency warning messages. These techniques and concepts are as:

A. Simple Broadcast [7] It is the simplest protocol used in propagation of safety alert messages mainly during accidents to all the vehicles moving towards the accident site. According to this protocol when a vehicle receives a broadcast message for the first time, it retransmits the message, after that ignores all subsequent broadcast messages with same ID from other vehicles. The main features against using this

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

protocol is that because of flooding there are too many redundant rebroadcast messages and also every host in the close proximity will contend for the access to the medium.

B. p-Persistence [7] This mechanism uses the probabilistic method to decide the vehicle(s) that will rebroadcast the alert message so as to remove the problem of broadcast storm. This means that once a vehicle has received the message for the first time it will rebroadcast the alert message with random probability p.

However, there are high chances of loss of message due to the reason when none of the nodes that receive message decide not to rebroadcast.

C. Weighted p-Persistence [8] In this case, distance between the sender and receivers along with transmission range of node are used as weighted factors to determine the forwarding rebroadcast probability which is calculated on per packet basis. The main issue of this technique is that there is high probability of collision as multiple vehicles simultaneously decided to rebroadcast though with different probabilities.

D. Slotted 1-persistence [8] This technique is based on the concept of division of transmission band into sub-bands and assigns different sub-bands for transmission to different distance ranges from the transmitting node. Each sub-range will be assigned its own WAIT TIME to rebroadcast the message. Once a node receives an alert message from a neighboring node for the first time, it retransmits with probability 1 after expiration of WAIT TIME, otherwise it discards the packets. This approach uses same logic as weighted p-persistence but it uses the GPS information to calculate the waiting time to retransmit. This approach falls behind in scenarios when there is more than one vehicle in the farthest slot ready to transmit messages simultaneously, this leads to collision of packets.

E. Slotted p-persistence [8] This is the improvement over 1-persistance protocol. In this case, the node upon receiving the packet checks packet ID and rebroadcasts with a pre-determined probability p at the assigned time slot, if it receives it for the first time and has not received any duplicates before its assigned time slot expires. Otherwise it discards the packet. In order to prevent the message die out each node buffers the message for a certain period of time. But here also the performance depends on value chosen for reforwarding probability p, which is chosen randomly.

F. TLO [9] This approach finds the vehicle most suitable to rebroadcast alert message when there is an accident or any other event by choosing the farther most vehicle in the transmission range from the victimized or abnormal vehicle with the help of TLO algorithm as the node for retransmission. All other vehicles will wait for a threshold time interval in order to take decision about rebroadcast. When the threshold waiting time expires and other vehicles do not receive the same alert message again, there is a problem in rebroadcasting.TLO is run again to find the next candidate as last node. This is repeated until a successful rebroadcast is done. This protocol is somewhat different in its approach from the above ones to control VANET performance parameters. But this protocol doesn't guarantee retransmission by the last node as it may not receive the main message which it has to retransmit also it is suited to 1D scenarios only.

G. VCWC Protocol [10] A vehicle to vehicle communication for cooperative collision warning as proposed by Xue Yang et al is known as Collision Warning Communication (VCWC) protocol which supports the following application challenges: Stringent delay requirements immediately after the emergency. Differentiation of emergency events and elimination of redundant EWMs. Support of multiple co-existing Abnormal Vehicles Avs over a longer period. It uses Active approach i.e. when a vehicle on the road acts abnormally, e.g. deceleration exceeding a certain threshold, dramatic change of moving direction, major mechanical failure, etc. It becomes an abnormal vehicle (AV), Only when an abnormal event occurs, the correspondingly AV actively generates

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Emergency Warning Messages(EWMs),which include the geographical location, speed, acceleration and moving direction of the AV, to warn other surrounding. The protocol consists of Message differentiation mechanism by implementing 802.11e EDCF (Enhanced Distributed Coordinated Function), supporting multiple priorities of data to be transferred. Another component of VCWC Protocol is Congestion Control policies (CCP) for reducing emergency warning delivery delay, determined by both waiting time and retransmission delay.

H. APAL Broadcast Protocol [11] Adaptive Probability Alert (APAL) protocol is originally derived from VCWC Protocol as the equation which depicts VCWC protocol for the (re)transmission rate [10] is adapted to certain specific observed range of the parameters or variables for achieving better retransmission rate (i.e. minimum delay, redundancy and collision of packets) of alerts or EWMs for inter-vehicle communication. APAL doesn't need the location information about the every vehicle. According to this approach, the vehicles which receive an alert message adaptively decide whether to rebroadcast it or not which in turn depends on certain conditions like random waiting time (traffic intensity dependent) interval after a node receives a EWM for the first time. Suppose the node doesn't receive any duplicate message until expiration of this waiting time it will broadcast it with initial probability in the range of 0.7—0.9.otherwise the vehicle refrains from rebroadcasting and counts the duplicate messages for updating its next retransmission probability and waiting time

I. Data Aggregation [12] Data aggregation for adaptive delay control proposed by Bo Yu et al is a methodology or technique for merging information from various sources into a set of organized and refined information to reduce redundant data and to improve communication efficiency. Data aggregation is based on action reward concept. For reducing redundancy adaptive delay control scheme is used which dynamically changes the forwarding speed of nearby reports so that they have better chance to meet each other and aggregate together [12].This scheme is based on distributed learning algorithm (i.e. learning from local neighbors about adapting delay) so as to aggregate the nearby reports from neighboring vehicles. However, the noted feature of this scheme it takes much processing time for calculating adaptive delay at each node so as to remove redundancy of message alerts/reports due to complex mechanism of distributive learning algorithm, which hinders it from achieving its main goal of reducing delay.

J. Receiver Consensus (ReC) Protocol [13] According to this approach, it is the receiving node which will decide for selection of nodes as message forwarder. This scheme proposed by Junliang Liu et. al. It consists of two components: Acknowledgement-based Neighbor Elimination which Guarantees reliability while reducing the number of retransmissions considerably.

For each warning message, each node divides its neighbor nodes into three sets (with respect to message according to their reception status: Rm (affirmatively received, nodes that attach ACK in their beacons), Pm (potentially received), and Nm (not received, nodes without ACK in their beacons). Potentially received is a transient status before receiving ACK. Receiver node computes each neighbor's distance to the sender. Neighbors' inside the communication range of the sender, i.e. whose distance to sender are less than sender's communication radius, are marked as potentially received and moved into set Pm. Location-based Ranking – (enables fast propagation at every hop without unnecessary waiting time): The ideal location for the next hop forwarder is the centroid O of all nodes in Nm (the point having average coordinate values of ―not received neighbors). ReC protocol is totally dependent on GPS for locating centroid of nearby neighboring nodes, as it is found GPS is 66% accurate in locating nodes in the transmission range of 15m .So, this along with the limited redundancy control are the factors which are hindering it from achieving efficient VANET performance.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

EXISTING SYSTEM

Inter vehicular communication (IVC) is an important emerging research area that is expected to considerably contribute to traffic safety and efficiency. In this context, many possible IVC applications share the common need for fast multi-hop message propagation, including information such as position**,** direction, and speed. However, it is crucial for such a data exchange system to be resilient to security attacks. Conversely, a malicious vehicle might inject incorrect information into the inter vehicle wireless links, leading to life and money losses or to any other sort of adversarial selfishness (e.g., traffic redirection for the adversarial benefit).

- Traditional traffic management systems are based on centralized infrastructures where cameras and sensors implemented along the road collect information on density and traffic state and transmit this data to a central unit to process it and make appropriate decisions.
- At. few places the work is done manually as well, which requiers man power.

Drawbacks:

- One or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions.
- Transmission of a false position message by a malicious vehicle that pretends to be at a claimed position. Such attacks include aggressive transmission of fake messages like accident or traffic jam or emergency vehicle.

PROPOSED SYSTEM

- In this paper we have scratched the surface of what is promising to be a new and fertile area of research in IVC security. Communication is generally vehicle-to-vehicle (V2V), without infrastructure.
- We describe FMBA—the case study chosen to represent IVC-based vehicular safety applications in detail.
- The aim of FMBA is to reduce the time that is required by a message to propagate from the source to the farthest vehicle in a certain area of interest.
- To achieve this goal, FMBA exploits a distributed mechanism for the estimation of the communication range of vehicles.

IMPLEMENTATION

1.Routing in Vehicular Networks

Due to high mobility, efficient routing represents a crucial technical challenge in vehicular communications, thus attracting the attention of researchers [11], [13], [14]. In general, topology routing protocols use the link state within the network to transmit the packet from the source to the destination, whereas this approach would fail in the presence of highly variable connectivity among nodes. Because vehicular communication can deal with not only a large number of vehicles but also with interest for local information, geographic routing may embody an efficient approach [13]. Routing that is based on geographic location exploits nodes' knowledge about their position and their neighbors' position, which is obtained through services such as the Global Positioning System (GPS). Forwarding decisions are taken based on the geographical positions of neighbors and of the destination. Geographic routing protocols are not required to maintain explicit routes, thus scaling well even with dynamic networks.

2. Fast Broadcast in Safety Applications

Several IVC applications require multi-hop broadcast to inform vehicles (and drivers) about road data, delivery announcements, traffic congestion, proximity with other vehicles, accidents, And even entertainment-related information [3]–[8], [15].The simplest broadcasting mechanism is flooding, where messages are rebroadcast by each receiving node. Although very simple, this technique may lead to high message collision probability and data redundancy, thus becoming rather inefficient. When a message is disseminated to receivers beyond the transmission range, multi-hopping could be used. However, multi-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

hop broadcast can consume a significant amount of wireless resources for unnecessary retransmissions. Ad hoc multi-hop broadcast and urban multi-hop broadcast are proposed in [8] for vehicular networks. These protocols are designed to address the broadcast storm, hidden node, and reliability problems in multi-hop broadcast. FMBA aims at reducing the number of hops that were traversed by a message to minimize the propagation delay of a message [3].

In more detail, in [27], the attacks on vehicular communications were classified as follows.

• Bogus information. One or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions. To cope with such misbehavior, the received data from a given source should be verified by correlating and comparing them with the data received from other sources.

• Cheating on positioning information. Injection of a false position by a malicious vehicle that pretends to be at acclaimed position.

• ID disclosure of other vehicles. This is to track their location. A global entity can monitor trajectories of targeted vehicles and use these data for many purposes, and we could take the example of some car rental companies that track their own cars.

• Denial of Service (DoS). The attacker may want to bring down the IVC or even cause an accident. Examples of attacks include channel jamming and aggressive injection of dummy messages.

• Masquerade. The attacker claims to be another vehicle by using false identities.

In this paper, we analyze the security of a representative algorithm for state-of-the-art IVC-based safety applications and propose countermeasures to handle the security threats. In particular, we focus on one of the main threats to safety application: the possibility of attacking the protocol to impede its useful service. For ease of exposition but without loss of generality, we particularly focus on FMBA, because it embodies both a state-of-the-art solution and a representative example of the IVC-based vehicular safety applications class possessing althea five properties mentioned in Section I. Indeed, problems and possible countermeasures that were identified for FMBA can also be adapted to other protocols/algorithms that belong to the same general class of applications sharing the aforementioned set of properties.

3. Fast and Secure IVC in Future Trends of Vehicular Networks

For completeness, we present in this section a brief discussion on fast and secure message transmission, considering research trends in vehicular networks. Vehicles are an important source of computing and sensing resources for drivers. These resources are increasingly underutilized. The idea of vehicular clouds comes in handy to solve this problem [30], [31]. In fact, the aim of this technology is to let vehicles share resources such as computational power, storage, and Internet connectivity. Security issues that are encountered in vehicular clouds are very specific [31]; the high mobility and position information of vehicles make the problem very novel and challenging. In addition, the attackers are physically moving from place to place, because vehicles are mobile nodes. Compared with a static network, it is much harder to locate the attackers. Moreover, in a vehicular cloud, attackers and their targets may be physically co-located on one machine. For example, an attacker can obtain confidential information and tampering with the integrity of information and the availability of resources.

CONCLUSION

In this paper, we have analyzed various schemes or techniques for efficient transmission of emergency warning messages in VANETs so as to counter affect the challenging problems like collision, delay and redundancy etc. We compared these existing solutions for their performance degradation and also identify drawbacks of each of these solutions. So, we can say

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

that this paper can be used as reference by researchers which are trying to build a technique for efficient transmission of emergency warning messages in VANETs. Currently, we are working on developing an effective V2V Communication protocol having capability of coping up with the communication challenges of collision, delay and redundancy while transmitting emergency warning messages in VANETs.

FUTURE ENHANCEMENT

The accurate and realistic simulation and modeling of IVC protocols and applications is the basis for almost all developments in this area. As field tests are always limited in size and scope, basic research in IVC relies on analytical models and simulation. Much progress can be seen in various aspects such as the development of adequate mobility models, the use of more precise metrics besides classical networking aspects, and even in the modeling of non-technical parameters such as the human driver behavior.

REFERENCES

[1] M. L. Sichitiu and M. Kihl, "Intervehicle communication systems: A survey," IEEE Commun. Surveys Tuts., vol. 10, no. 2, pp. 88–105, 2nd Quart., 2008.

[2] C. Wu and Y. Liu, "Queuing network modeling of driver workload and performance," IEEE Trans. Intell. Transp. Syst., vol. 8, no. 3, pp. 28–537, Sep. 2007.

[3] C. E. Palazzi, S. Ferretti, M. Roccetti, G. Pau, andM. Gerla, "How do you quickly choreograph intervehicular communications? A fast ehicle-tovehicle multihop broadcast algorithm, explained," in Proc. IEEE CCNC, Jan. 2007, pp. 960–964.

[4] A. Amoroso, M. Ciaschini, and M. Roccetti, "The farther relay and oracle for VANET: Preliminary results," in Proc. IEEE WICON, 2008,pp. 1307–1311.

[5] M. D. Felice, A. Ghandour, H. Hartail, and L. Bononi, "Enhancing the performance of safety applications in IEEE 802.11p/WAVE vehicular networks," in Proc. IEEE WOWMOM, Jun. 2012, pp. 1–9.

[6] C. E. Palazzi, M. Roccetti, and S. Ferretti, "An intervehicular communication architecture for safety and entertainment," IEEE Trans. Intell. Transp. Syst., vol. 11, no. 1, pp. 90–99, Mar. 2010.

[7] J. Luo and J.-P. Hubaux, A Survey of Research in Intervehicle Communications. New York, NY, USA: Springer-Verlag, 2006, pp. 111–122,Embedded Security in Cars–Securing Current and Future Automotive IT Applications.

[8] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, "Urban multihop broadcast protocols for intervehicle communication systems," in Proc. ACM Workshop VANET, Oct. 2007, pp. 76–85.

[9] L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "New developments and research trends for intelligent vehicles," IEEE Intell. Syst., vol. 20, no. 4, pp. 10–14, Jul./Aug. 2005.

[10] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T.Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[11] F. Qu, F.-Y. Wang, and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," IEEE Commun. Mag., vol. 48, no. 11, pp. 136–142, Nov. 2010.

[12] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of intervehicle communication protocols and their applications," IEEE Commun. Surveys Tuts., vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.

[13] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[14] Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, "Routing protocols in vehicular ad hoc networks: A survey and future perspectives," J. Inf. Sci. Eng., vol. 26, no. 3, pp. 913–932, May 2010.

[15] A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, "A new approach to urban pedestrian detection for automatic braking," IEEE Trans. Intell. Transp. Syst., vol. 10, no. 4, pp. 594–605, Dec. 2009.

[16] M.-T. Sun, W.-C. Feng, K. Fujimura, T.-H. Lai, H. Okada, and K. Fujimura, "GPS-based message broadcasting for intervehicle ommunication," in Proc. ICPP, Aug. 2000, pp. 279–286.

[17] M. Roccetti and G. Marfia, "Modeling and experimenting with vehicular congestion for distributed advanced traveler information systems," in Computer Performance Engineering. New York, NY, USA: Springer- Verlag, 2010, pp. 1–16.

[18] N. Ravi, S. Smaldone, L. Iftode, and M. Gerla, "Lane reservation for highways (position paper)," in Proc. IEEE ITSC, Sept. 30, 2007–Oct. 3, 2007, pp. 795–800.

[19] C. E. Palazzi, M. Roccetti, S. Ferretti, G. Pau, and M. Gerla, "Online games on wheels: Fast game event delivery in vehicular ad hoc networks," in Proc. IEEE V2VCOM, Jun. 2007, pp. 1–8.

[20] M. Fazio, C. E. Palazzi, S. Das, and M. Gerla, "Facilitating real-time applications in VANETs through fast address autoconfiguration," in Proc. IEEE CCNC, Jan. 2007, pp. 981–985.