IPHV8I1028X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

A SECURE INCENTIVE ROUTING PROTOCOLS FOR MOBILE ADHOC NETWORKS

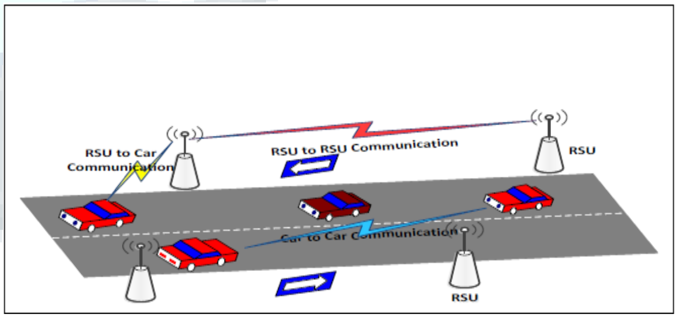
[#1]D.SHANTHI KUMAR, M.Tech Student,
[#2]S.NAVEEN KUMAR, Associate Professor,
[#3]PEDDI KISHOR, Associate Professor& HOD,
Dept of CSE,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, T.S., INDIA.

Abstract: To detect the position forging attacks in vehicular ad hoc networks (VANETs) and to improve vehicle passenger safety by means of inter vehicle communication. In the existing system, it presents a model for the performance evaluation of safety message dissemination in VANETs with two classes. In particular, considering the IEEE 802.11 broadcast protocol and 2D Markov modeling. Then the result is used to drive the average dissemination delay of high priority messages in the presence of the low –priority traffic in the network. This paper presents Inter Vehicular Collision Avoidance System on Highways to ensure that the vehicles perform safety communication with each other for which can alert the drivers before accidents. This can be done by defining a critical "Inter Vehicular Distance" to be maintained between and any two vehicles on highways. Moreover, certain vehicles such as ambulance, fire service vans, police patrols need to be given a high priority, as their requirements are crucial during emergency situations. By giving vehicular priorities and providing group communications, our proposed System results vehicular collision avoidance in Inter Vehicular Ad-hoc Network. Another objective of this paper is to secure the information passing via Inter-Vehicular ADHOC wireless Network and protect it from intruders. For this a Secure-Pre warning Collision Algorithm (S-PWCA) is implemented in firmware to make the IVAN message more secure.

Keywords: IVC, IVAN, S_PWCA, VANETs, Emergency Warning Messages, Abnormal Vehicles.

I.INTRODUCITON

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 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. 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].

II. RELATED WORK

In [1], to improve the safety, efficiency and comfort of every day road travel. Several major classes of applications and the types of the services they require from an underlying network. A complex networking protocol is a drawback. To analyse existing networking protocols in a bottom-up fashion, from the physical to the transport layers, as well as security aspects related to Inter Vehicle Communication (IVC). In [2], to detect collision avoidance in an emerging vehicular safety application. The concept of CCA, which is implemented by Medium Access Control (MAC) and the routing layer. Mobile ad hoc networks are not directly applicable for CCA. The safety performance of CCA using simulated vehicle crash experiments.

In [3], to enable the transmission of warning messages (alarms) between vehicles without additional roadside infrastructure. Messages can be sent faster than through base stations. Unnecessary repetition of warning messages and transmission to inapplicable respondents is the problem.

Proposed this problem using blind flooding to broadcast alarms and two Lanes are used. Warning messages are routed by AODV protocol.

In [4], multihop data delivery through vehicular ad hoc networks. A moving vehicle carries the packet until a new vehicle moves into its place and forwards the packet. Proposed this problem using Vehicular-Assisted Data Delivery protocol. To forward the packet to the best road with the lowest data delivery delay.

In [5], when the traffic increases and the highways become gathered it affects the safe and efficient movement of traffic. A wireless sensor network is required as a solution of reduction of these more saddening and reprehensible statistics. Vehicular ad hoc and sensor networks are self-organizing network comprised of a large number of sensor nodes.

In [6], the aim is to improve safety in driving conditions. It is referred in Dedicated Short Range Communication (DSRC). It is weak in message size; transmission rate retransmission strategies and network routing. It is proposed in VANET beaconing solution. represents a small packet transmitted in a particular time period. It considers the probability of packet reception (PPR) in a critical event. It measures traffic safety rules also.

In [7], this is proposed in a dynamic power adjustment protocol. It is used to send the safety message periodically. If the beacon based on the channel status depending on the channel jamming. If the Beacon Power Control is used to sense the channel jamming. It is used to decrease the channel jamming and improve its performance. In [8], to broadcasting a safety message using a flooding algorithm. But a large number of vehicles in topmost hour, the flooding leads to packet collision during the transmission. So these papers proposed broadcasting a safety message in dynamically adjust waiting time for a vehicle based on source and destination. So that the performance leads to reachability and reliability. In [9], providing for vehicle-to infrastructure and vehicle-to-vehicle radio communication. It is proposed using an IEEE 802.11p MAC protocol focusing on vehicleto- infrastructure communication. Here window size is calculated by centralizing approach and distributed approach. These schemes are used in dynamic situations. In [10], low latency while transferring a message in vehicle to vehicle communication. So proposed this model using an ALOHA-based randomized routing algorithm. It is used to calculate the end-to-end delay transmission and achieving a high throughput-delay. In [11], the aim is to broadcasting a safety message in VANETS. Here MAC protocol is used. But it is challenging for high mobility, traffic and low delay. So we proposed a topology for transparent broadcasting protocol. It is used to find out the success and average delay for broadcasting communication.

In [12], Link-based Distributed Multi-hop Broadcast is used. This is fully distributed and each vehicle receives the emergency message, first it calculates the waiting time before it sends that message. So it is guaranteed for reliable broadcasting communication in VANETs.

III.IMPLEMENATAION

Traffic accidents have been taking thousands of lives each year, outnumbering any deadly diseases or natural disasters. Studies [4] show that about 60% roadway collisions could be avoided if the operator of the vehicle was provided warning at least one-half second prior to a collision. So, based on these statistic figures, researchers and scientists switch to computerize and automate the vehicular transportation system so as to reduce the road accidents which in estimation takes lives of about 1.2 million people per year worldwide [5], and injures about forty times of this number, as the human driver suffers from following problems:

- ***Line-of-sight limitation of the brake lights*:** Typically, a driver can only see the brake light from the vehicle directly in front.
- ***Large processing/forwarding delay for emergency events*:** Driver reaction time typically ranges from 0.7 seconds to 1.5 seconds which results in large delay in propagating the emergency warning [6].

So, VANET is one of the solutions to remove these problems but that too needs a mechanism so as to avoid collision, achieve congestion control and low latency in delivering of emergency warning messages.A vehicle to vehicle communication for cooperative collision warning provides such facilities to a large extend but the wireless communication used is unreliable due to channel fading, packet collisions, and communication obstacles, can prevent messages from being correctly delivered in time. The main problems while propagating Emergency Warning Messages (EWMs) in Vehicular Ad hoc Networks are:

1) Presence of Redundancy in EWMs while propagating them in VANETs.
2) Delay in propagating and delivering of EWMs.
3) Collision of data traffic whenever there in congestion in vehicular traffic.
4) Broadcast Storm.

The *sole reason* behind all these challenging problems includes *Packet loss* or the *Communicating Nodes may be Out-of-Range.* So, in order to remove or control these challenging problems, there is a need for effective mechanism that could:

1) Control the redundancy of EWMs to an optimum acceptable level.
2) Provide an efficient EWM dissemination scheme for controlling delay and collision in VANETs.
3) Handle message forwarder node failure in VANETs.
4) Provide an efficient data dissemination scheme to choose the warning message forwarder.

IV. PROPOSED SECURE TECHN IQUE FOR COLLISION AVOIDANCE

Securing any type of communication links involves three key requirements. First, the links must be protected from eavesdropping, so that unauthorized persons can’t access private information. Second, the end users must be authenticated before anything is sent to or received from them. Third, the communication links must be protected from tampering by hackers. Therefore before the deployment of any vehicular communication system, security and privacy issues have to be resolved. In this paper, for achieving secure and privacy preserving communications for collision avoidance, an easily implementable Block Cipher technique is proposed. For broadcasting the secure message from vehicle in IVC network RC6 algorithm is defined which provides the secure communication Network between V2V. With the help of this technique Secure Pre-warning Collision Avoidance Algorithm is proposed in this paper. A. Block Cipher RC6 RC6 is a block cipher based on RC5 and designed by Rivest, Sidney, and Yin for RSA Security [15]. Like RC5, RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable; again, the upper limit on the key size is 2040 bits [16].RC6 was designed to meet the requirements of the Advanced Encryption Standard (AES) competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits, but, like RC5. RC6 can be viewed as interweaving two parallel RC5 encryption processes. It uses an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word. B. Secure Pre-Warning Collision Avoidance (S-PWCA) System In order to ensure proper operation of safety-related applications the security of safety messages should be guaranteed even in the presence of persistent attackers. As a wireless communication technology, Inter – vehicular Network is highly vulnerable to abuses and attacks. An adversary may inject a false information in order to mislead the target vehicles or with tampering the on board unit, implement an impersonation attack. He may also, by recording the messages of a target vehicle, track the vehicle’s location and collect private information about the vehicle. To facilitate communications, two distinct wireless channels are considered to exchange signaling messages to formulate vehicles’ clusters and to issue/forward warning messages, respectively. The vehicles’ clusters are formed with different parameters such as direction of vehicle movement, and its speed. Each vehicle is considered to have knowledge on its maximum wireless transmission range. Depending on its wireless transmission range, vehicle direction and speed, which has highest priority then would elected as a cluster head. The S-PWCA system inside each vehicle continuously carries out the following algorithm: 1. Information Collection: In this all the vehicles' gather's the information from GPS like position and time. Then each vehicle obtains its speed and acceleration from the vehicle speed meter. In order to ensure synchronization between all vehicles, current-time is obtained from the GPS. All the information is placed in a packet which is stamped with the vehicle identification number of the vehicle. The structure of the packet is as shown in following figure3.

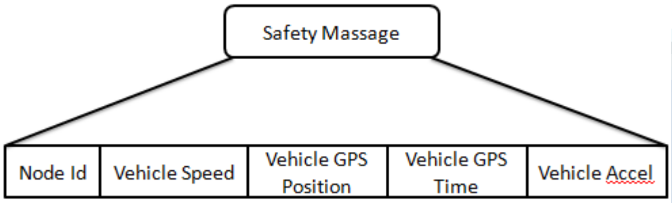


Figure4: Packet Structure

2. Generating Secure Message: Following are the steps for creating secure message listed below.

a. Secure Hardware module receives safety message generated by On Board Unit according to the received data from other node.

b. Secure Hardware module adds time stamp to message.

c. Then secure hardware module uses v-node's private key & digital signature on safety message is encrypted to create secure message.

d. The secure packet is broadcasted to nearby vehicles through multi-hop IVCs.

e. On the receiving side, secure message is passed to secure hardware module by on board unit.

f. Secure hardware module validates the signature of the sender by using public key of the anonymity key set.

g. If the signature is valid, secure hardware module extract original safety message. Otherwise discards the message.

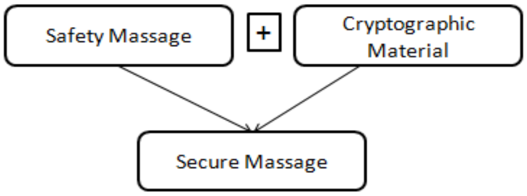


Figure 5: Generating secure message

Generated secure message is periodically broadcasting in IVAN network using broadcasting wireless unit is installed at each vehicle should have the wireless unit which can communicate with another vehicle shown in figure4. Vehicles do not know position, speed, acceleration, time of neighbour vehicles. With the help of S-PBM message every vehicle get the status of the signal, to avoid collision. For Transmission of packets interval time is assumed to be small enough to ensure safety.

A. S-PWCA algorithm Assumptions: - The collision Warning and Avoidance system is installed at on board unit. In this system, it is assumed that every vehicle is equipped with a system which is able to get the geographical position of the vehicle and having wireless transceiver. The proposed S-PWCA algorithm will work for both V2V and V2I.

Step1: -Start originating secure message periodically.

Step2: -Secure message arrives at a vehicle.

Step3:-After receiving the status of vehicle, distances are calculated.

Step4: -Calculate Distance Get Val of DV1 as VNode, Val of DV2 as VNode X = DV1.X - DV2.X Y = DV1.Y - DV2.Y DV1, V2 = √ X*X + Y*Y

Step5: - If the distance between two or more vehicle is less than 5m in our simulation, then warning message is generated and broadcasted to the nearby vehicles to avoid the possibility of collision. If Dv1, v2 < 5m Then Collision Detected, Broadcast Secure Warning Message in Network. Else Data Transfer to other Node in Network related to traffic Information End

Step6: - After receiving secure message to avoid collision, one of the vehicle will increase the speed with prior communication related to position, speed, time & another vehicle speed measure set to slow.

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 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. The last component consists of

Rate Decreasing Algorithm (RDA) a multiplicative rate decreasing algorithm as described in [7] is used in order to remove trade-off between (re)transmitting EWMs too fast or too slowly. This algorithm describes that the EWM transmission rate is decreased by a factor of a after every L transmitted EWMs. The results as observed by Xue Yang et al shows that value of a=2 is adequate in achieving low EWM delivery delay for a wide range of co-existing Avs. Apart from this CCP also consists of *state transition mechanism* to ensure EWM coverage for the endangered regions and to eliminate redundant EWMs. This protocol is to a large extend successful in achieving its main motive both in 1D and 2D scenarios but the delay is still gradually increasing for transmission of EWMs with the increased number of co-existing vehicles which in turn makes the transmission rate dependent on initial probability of accessing the VANET communication medium.

V.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 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.

REFERENCES

[1] G Yuen Liu, Jun Bi, Ju Yang, ‖*Research on Vehicular Ad Hoc Networks* —,2009 Chinese Control and Decision Conference (CCDC 2009),978-1-4244-2723-9/09/2009 IEEE.

[2] J Gayathri Chandrasekaran,‖*VANETs: The Networking Platform for Future Vehicular Applications*‖.

[3] R.A.Santos,A.Edwards,O.Álvare,—*Towards an Inter-vehicle Communication Algorithm*‖, In proceeding of: Electrical and Electronics Engineering, 2006 3rd International Conference.

[4] C. David Wang and James P. Thompson, —*Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network*‖,1997, US. Patent No. 5,613,039.

[5] http://www.who.int/features/2004/road_safety/en

[6] Marc Green, ——*How Long Does It Take to Stop?" Methodological Analysis of Driver Perception-Brake Times*‖, Transportation Human Factors, vol. 2, no. 3, pp. 195–216, 2000.

[7] Ozan Tonguz, Nawaporn Wisitpongphan, Fan Bai, Priyantha Mudalige and arsha Sadekar, —*Broadcating in Vanet,*‖ in Proc. ACM VANET, Sep 2007, pp.1-6.

[8] Ozan Tonguz, Nawaporn Wisitpongphan, Fan Bai, Priyantha Mudalige and arsha Sadekar, —*Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks,*‖ in IEEE WIRELESS.

[9] Kanitsorn Suriyapaiboonwattana, —*An effective safety alert broadcast Algorithm for VANET*‖, ISCIT Oct. 2008.

[10] Xue Yang, Jie Liu, Feng Zhao and Nitin H. Vaidya, ‖*A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning*‖,in proceeding of 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2004), Networking and Services, 22-25 August 2004, Cambridge, MA, USA.

[11] Kanitsorn Suriyapaiboonwattana, Chotipat Pornavalai, and Goutam Chakraborty, —*An Adaptive Alert Message Dissemination Protocol for VANET to Improve Road Safety*‖, FUZZ-IEEE 2009,Korea.

[12] Bo Yu, Cheng-Zhong, Xuand Minyi Guo, —*Adaptive Forwarding Delay Control for VANET Data Aggregation* —,IEEE Transactions on Parallel and Distributed systems, vol. 23, no. 1, january 2012.

[13] Junliang Liu, Zheng Yang,Ivan Stojmenovic,‖*Receiver Consensus:On-time Warning Delivery for Vehicular Ad-hoc Networks*—,1063-6927/12 2012 IEEE DOI 10.1109/ICDCS.2012.41.