Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.497 – 502

RESEARCH ARTICLE

Secure Technique for Collision Avoidance in Vehicle-to-Vehicle Communication

Ashwini Nibrad[1], Akshta Kadbajiwar[2], Sneha Bhagwat[3], Manjusha Nagula[4], Pratiksha Manchalwar[5], Ankit Khobragade[6]

CE Department, BD College, Sewagram RTM University Nagpur, MS (INDIA.)

ABSTRACT: Inter-Vehicular Ad-hoc Network (IVAN) does not have a fixed network topology but is highly dynamic. The topology of the network changes frequently because wireless links are established and broken down due to certain factors such as the velocity of the vehicles, their mobility patterns and their spatial density. These high dynamics also cause very short times for data transfer. 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

I. INTRODUCTION

Recently much attention has been devoted to the research in the field of Inter-Vehicular Adhoc Network (IVAN) communications. Indeed, the advances in wireless technologies are making it possible to deploy new services: some of the most interesting ones aim at increasing safety over highways and streets by delivering warning messages, or through cooperative or assisted drive. The goal of the Automotive Collision Avoidance Systems (ACAS) is to detect and warn the driver of potential hazard conditions. Inter - Vehicular Ad Hoc Networks (IVAN) are emerging wireless networks established between vehicles, and can enable many safety applications. One of these safety applications is a collision warning avoidance system. The architecture for a reliable vehicular collision avoidance system on highways that operates in VANETs is developed in this paper. The system relies on GPS for position information and the vehicle's speed information [1]. Each vehicle broadcasts this information using the Inter Vehicle Communication Network to all vehicles in the neighborhood [2]. Each vehicle broadcast, periodic broadcast message which represent the position, speed, acceleration & time information of vehicles. With this messages every vehicles calculate and scanned for proper distance between vehicles. Finally, vehicles having less inter vehicular distance then warning messages are broadcast to predict collisions few seconds beforehand on highways.

In this paper, inter vehicular collision avoidance system is proposed on highways to maintain Inter-Vehicular Distance. The Inter Vehicle Collision Avoidance system relies inside each vehicle to obtain its position from the GPS, its speed and acceleration from other vehicle respectively. Furthermore, the system uses VANETs to broadcast speed and position information to all vehicles that are in the area. Similarly, the rest of the vehicles in that area will gather and broadcast their respective information. Hence, all vehicles in an area store the information about all vehicles in that area. This information is constantly updated; moreover, the vehicles constantly check for inter-vehicular distance as well as intersecting vehicles. In Inter Vehicular Collision Avoidance system constantly

proceeds in calculating distance segments from the received information (each segment represents a vehicle). Road segments that intersect and none intersect with each other are noted. These distance segments signify possible colliding vehicles and broadcast warning message to the possibly colliding vehicles. It becomes necessary that on highways the vehicles exchange dynamic information such as speed, acceleration, position and direction in real time. Wireless communications do not require line-of-sight. Thus, using wireless communication technologies, the vehicles can inform each other about how far they are from the distance of vehicle and receive the dynamic information of the signal lights and the status of the intersection as well as on highways. The goal of inter vehicular collision avoidance protocol is to warn the driver about the condition of the vehicle and the signal to avoid the collision.

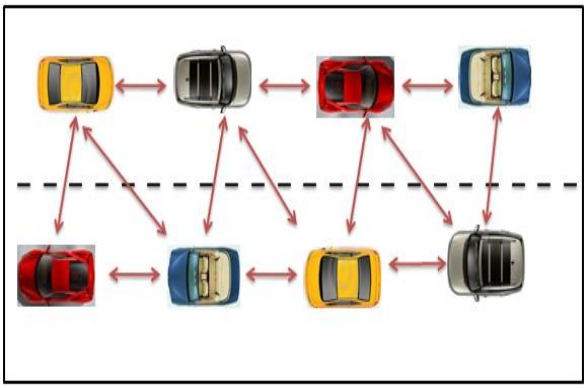

Figure1: V2V communication

II. RELATED WORK

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 [3].

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 [4].

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 [5].

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 [6].

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 [7].

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. A beacon 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 [8].

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 [9].

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 [10].

Providing for vehicle-to infrastructure and vehicle-to-vehicle radio communication. It is proposed using an IEEE 802.11p MAC protocol focusing on vehicle to infrastructure communication. Here window size is calculated by centralizing approach and distributed approach. These schemes are used in dynamic situations in [11].

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 [12].

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 [13].

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 in [14].

III. PROBLEM DEFINITION

The Inter Vehicular automotive collision warning and avoidance systems will be very effective for reducing fatalities, injuries and associated costs. In such systems it is very challenging to find the safe distance between the nearby vehicles. And this distance should be periodically broadcasted to other nearby vehicles. The best way to indentify the position of the vehicles is by using GPS. The on-board unit in the vehicle should consist of a GPS unit, which is always tracking the position of the vehicle and this position details are broadcasted to other nearby vehicles. A central processing unit which is present on the on-board unit of the vehicle will always process the GPS coordinates broadcasted by the other nearby vehicles and calculates the distance between current vehicles with respect to the nearby vehicles. Not only has the distance the processor had to calculate speed, direction and acceleration of the vehicles. At the same time the processor has to drive a graphical LCD to display the nearby vehicle information to intimate the driver about the safe distance and important information. In order to develop an Inter Vehicular automotive collision warning and avoidance system, it is necessary that the vehicles should be able to exchange in actual time their dynamic information such as speed, acceleration, direction, relative position, etc. The only way to exchange the vehicles dynamic information will be through wireless communications. The communication links among vehicles must be secured. Otherwise, hackers may inject some misleading data into the inter-vehicle messages to make the vehicle systems malfunction as shown in figure2.

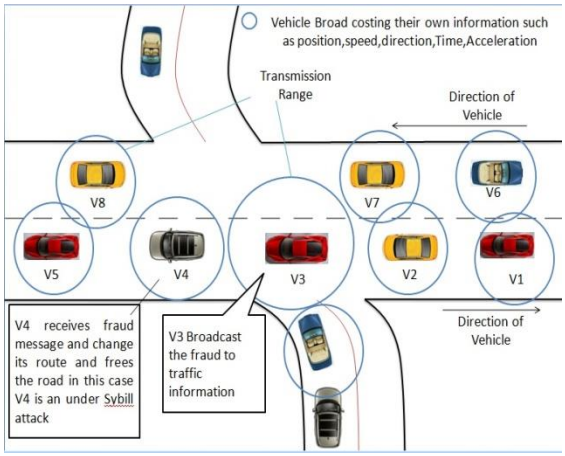

Fig2. In this example of Sybil Attack, attackers (V1 and V3) broadcast false information to affect the decisions of other vehicles (V4) and thus clear the way of attacker V5.

There is a challenge in balancing security and privacy needs. On the one hand, the receivers want to make sure that they can trust the source of information. On the other hand, the availability of such trust might contradict the privacy requirements of a sender. A radio-based V2V collision warning system operates by using either periodic or emergent-event-driven V2V communications. Each vehicle on the roads is assumed to be equipped with a radio (such as an IEEE 802.11(b)-based radio). Vehicles on the roads form a mobile ad-hoc network. Exchanging messages in such a network is not reliable because message collisions and link breakage are likely to occur due to high mobility of moving vehicles. Using such an unreliable message exchanging mechanism greatly degrades the performances of V2V – communication-based Collision Warning System. The IVAN is highly dynamic and the topology of the network changes frequently because wireless links are established and broken down with dynamic topologies. These high dynamics also cause very short times for data transfer.

Therefore this paper presents a technique for exchanging vehicles dynamic information in a secure mode in IVAN. Vanet application decisions can be a matter of life or death decisions, therefore, securing these application is very crucial to the implementation for this technology. This is to ensure that the vehicles should perform safety communication with each other, by defining a critical "inter-vehicular distance" to be maintained between and any two vehicles. It is also feasibility of implementing secure inter vehicle communication links using today's technology. So that current technology will allow us to build such a system for collision avoidance secure technique in Vanet

IV. PROPOSED SECURE TECHNIQUE 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.

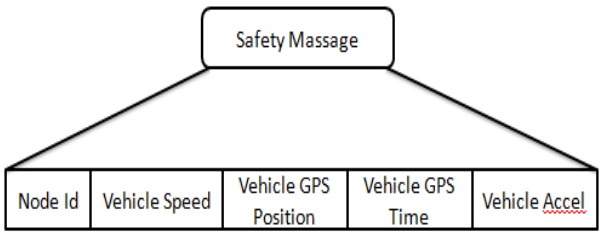

Figure4: Packet Structure

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.

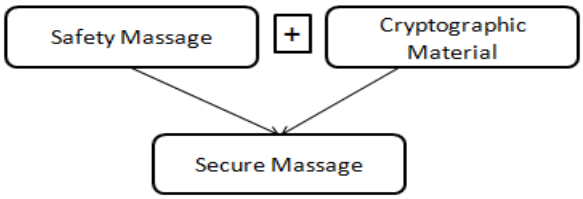

Figure 5: Generating secure message

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.

V. CONCLUSION

The deployment of vehicular communication networks is rapidly increasing. In this paper Block Cipher based secure technique for collision avoidance is presented for exchanging vehicles dynamic information in a secure. The secure technique is designed to guarantee the fresh message, message authentication, integrity, non-repudiation, privacy. Also the work has been carried out to avoid the collision, Secure – Pre Warning Collision Avoidance (S-PWCA) algorithm is proposed. Our Simulations result shows that the broadcasting secure message will improve the nearby collision avoidance to improve highway safety.

REFERENCES

[1] The Vehicle Collision Warning System Based On Gps Sehun Kim, Sunghyun Lee, Inchan Yoon, Mija Yoon And Do-Hyeun Kim 2011 *First Acis/Jnu International Conference On Computers, Networks, Systems, And Industrial Engineering* .

[2] Increasing Broadcast Reliability In Vehicular Ad Hoc Networks Nathan Balon And Jinhua Guo University Of Michigan – Dearborn 2006.

[3] Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A survey,"IEEE Comm. Surveys and Tutorials, vol. 10, no. 2, pp. 88- 105, May-Aug. 2008.

[4] S. Biswas. R. Tatchikou, and F. Dion,"Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,"IEEE Comm., Vol. 44, no. 1, pp. 74-82, Jan.2006.

[5] Enhancement of Delivery of Warning Messages for Mobile Networks. Chi-Sheng Tasi and Wun-Kai Du Department of computer science and engineering. Taipei, Taiwan.

[6] VADD: Vehicle-Assisted Data Delivery in vehicular ad hoc networks, Jing Zhao and Guohong Cao Department of computer science and engineering.

[7] Sensor, Ad hoc and Sensor Networks; Principles and Challenges, Mohammad Jalil Piran1, G. Rama Murthy2, G. Praveen Babu 3.

[8] Balancing Safety and routing Efficiency with VANET Beaconing Messages. Scott E. Carolina State University, Raleigh, NC, USA. In Partial Fulfillment of the Requirements of Computer Networking (CSC 570, Fall, 2013), David Thuente, Ph.D

[9] Safety Message Power Transmission, Control for vehicular Ad hoc Networks.1 Ghassan Samara. 1 sureswaran Ramadas and 2 Wafaa A.H. A1 Salihy 1National Advanced IPv6 center, 2 School of Computer Science, University Sains Malaysia, Penang, Malaysia. Journal of Cs 6 (10): 1027-1032, 2010.ISSN 1549-3636

[10] Dynamic Broadcasting in Vehicular Ad hoc Networks. Sara Najafzadeh, Norafidas Ithnin, Shukor Abed Razak and Ramin Karimi, International journal of computer theory and engineering, Vol.5, No 4, August 2013.

[11] IEEE 802.11p Performance Evaluation and Protocol Enhancement.Yi Wang, Akram Ahmed, Bhaskar Krishnamachari and Konstantinos psounis Viterbi School of Engineering university of Southern California, Los Angeles, CA 90089, USA. Proceedings of the 2008 .IEEE International Conferences on Vehicular Electronics and Safety Columbus, OH< USA. September 22-24, 2008.

[12] Distributed Routing in Vehicular Ad Hoc Networks: Throughputdelay Tradeoff. Ali Abedi Majid ghaderi Carelu Williamson, Department Of Computer Science, University of Calgary.

[13] Reliable Broadcast of Safety Messages in Vehicular Ad Hoc Networks. Farzad Farnoud and Shahrokh Valaee. The direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings.

[14] A Multi-hop Broadcast Scheme for the propagation of Emergency Messages in VANET. Qiong Yang, Lianfeng Shen, National Mobile Communications Research Laboratory Southeast University, Nanjing, 210096, China.

[15] Ronald L. Rivest,"THE RC6 Block Cipher" RSA Laboratories, 2955 Campus Drive, Suite 400, San Mateo, CA 94403, USA.

[16] "What are RC5 and RC6","rsa.com". Available at: http://www.rsa.com/rsalabs/node.asp?id=225

