ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

A Survey on V2V Collision Avoidance in VANET

Bhagyashree Borse[1], Natasha Naik[2], Mrunalini Gavphale[3]

Assistant Professor, Department of Electronics & Telecommunication Engineering, A.C.Patil Engineering College, Kharghar, Navi-Mumbai, India[1]

Assistant Professor, Department of Electronics & Telecommunication Engineering, A.C.Patil Engineering College, Kharghar, Navi-Mumbai, India[2]

Assistant Professor, Department of Electronics & Telecommunication Engineering, A.C.Patil Engineering College, Kharghar, Navi-Mumbai, India[3]

ABSTRACT:During the last few years VANET has attracted alot of attention due to the many new applications. VANET is the emerging wireless communication technology. The main aim of the paper is to avoid V2V collision by using safety messages. Regularly secure messages are broadcasted by the vehicles which give beneficial information to other nodes using secure method. The Secure message which contains the vehicles information such as position, speed, direction, acceleration, time. The V2V distance is calculated, collision between vehicles is avoided by broadcasting secure message. For this Secure-Pre warning Collision Avoidance Algorithm (S-PWAA) is proposed**.**

KEYWORDS:IVC, IVAN, V2V, PKI, S-PWAA..

I. INTRODUCTION

In VANET, vehicles act as a node through V2V communication, a vehicle can detect the position and movement of other vehicles up to certain kilometers. Inter-Vehicle Communication (IVC) has become an emerging technology in network research, opening up new research challenges well beyond those of classical Mobile Ad Hoc Network (MANET) research[9].There are many accidents happening on highways which results when vehicle are leaving the road or travelling unsafely through interactions. VANET is used to provide safety, where we collect all the information of the vehicles. VANET and IVC can be controlled by protocol known as Dedicated Short Range Communication (DSRC) protocol, IEEE 802.11p, Bluetooth is provided with On-Board Unit (OBU). The applications of V2V and V2I come under two services [1]. Vehicles are now working as computers or networks on wheels. In this, vehicle detection is done, the system gives warning to nearby vehicles if the condition occurs or takes action through braking or steering. Collision is avoided by braking for low speed vehicles and for high speed vehicles collision is avoided by steering.Multi hops are used for the communication of the nodes that are out of the reach of transmission of the radio.

II. RELATED WORK

The vehicle collision warning system that finds the car crash and warns the risk to drivers, this work was done by Sehun Kim et. al in [5]. In [6] Samaneh Khakbaz et. al implemented an approach using sensors and GPS system to send a message among highly mobile hosts like vehicles in road traffic. This method uses unreliability that can occur in same. Nadra Ben Romdhane et. al in [7] proposed an obstacle detection module through digital images processing. M. R. Hafner et. al in[8] present pagination anywhere in the paperaverage of the outputs of these filters

Ali et al[19], implemented a collision detection system to minimize accidents caused by road traffic. Using VANET data it calculates the break response time of the driver and gives solution for falsealarm. The system works on the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

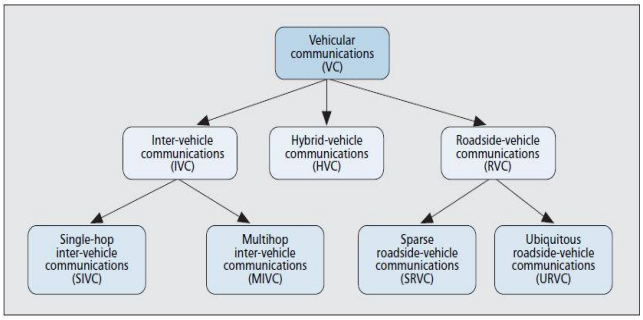
Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

algorithm and detects false alarm. This helps drivers to safe drive on roads and safety measures will take place. IVC systems are important for knowing the background of IVC systems.

III. V2V COMMUNICATION

The radio system for the V2V Communication is derived from the standard IEEE 802.11, also known as Wireless LAN. If more than one vehicle are in radio communication range, they connect automatically and establish an ad-hoc network. Every vehicle contains a router which allows sending messages over long distance vehicles. The vehicles can handle fast changes of an ad-hoc network topology based on routing algorithm.



.

IV. VANET APPLICATIONS

There are many applications of V2V and V2I communications which can provide a wide range of information to drivers and travellers. Network are interfaced on on-board devices which consist of different GPS receivers and sensors, grant vehicles the ability to collect process and disseminate information about itself and its environment to other vehicles nearby to it. That has led to enhancement of road safety and the provision of passenger.

V. IVC ATTACKS

There are several possible attacks that can be launched in IVC [14]

1) Jamming / Interference: - A malicious vehicle can causecommunication interference to prevent other vehicles from communicating. Consequently, some vehicles will not receive urgent safety information, leading to loss of lives.

2) Sybil Attacks:- Multiple fakenodes are created with the help of Sybil attack which is used for broadcasting wrong information

3) Node Impersonation: - It is used to send messages after modification and claims that the message comes from originator for the unknown purpose.

4) Sending False Information:-It means Sending wrong information from one node to another node.

5) ID Disclosure:-The nodes disclose the identity inthe network and track the location of the target nodes. Target nodes are supervised by the monitors and will send a virus to the neighbors of the target nodes.

B. Security Goals

1) Authentication: - Driving decision must be decided basedon safe messages. Thus, vehicle has to be authenticated in order to transmit any safety messages.

2) Integrity:-Even though the transmitter remains authenticated, integrity is required to guarantee correctness of messages.

3) Non-Repudiation:- Once the accident takes place, it should be identified for the purpose oflaw investigation, i.e., transmitted messages should not be denied by the sender.

4) Messages Freshness: - Even if a sender and a message canbe proved to be legitimate, the received information may be stale, by message replaying. Information and update can be sent by freshness.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

5) Anonymity: - Privacy of each driver should be safe, from unauthorized observers. To meet this challenge, anonymity is required to all vehicles. Since safety message is public information, confidentiality is provided by encryption in the communication system.

VI. METHODS FOR AVOIDING ACCIDENTS

There are three main requirements for acquiring several type of communication links involves.

1) To protect from eavesdropping the links must be secured from the unauthorized persons so that they cannot access the private information.
2) Before sending or receiving any message the users must be authenticated.
3) The link has to be protected from hackers.

A. PKI METHOD

A PKI collects all users' identities from certificate authority (CA). CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA. After registration Certificate Authority enters user to a list and updates its list of users' identities and their assigned public keys. CA keeps alternate list of user's information

Each node is registered with one local CA. During the registration a certificate is issued which contain identity of the user and information like validity and a pair of public and private key. Local Ca's is responsible for cancelling the compromised certificates. [15].The PKI method is used to authenticate two network users through encryption. Since, the mechanism of password exchange is very dangerous wireless medium. So it is been avoided. Nobody can perfectly tell, whether a network can be secure or not. Therefore, PKI has many advantages. Sender encrypts a message using private key. Receiver only can decrypt messages using his private key.

B. COLLISION AVOIDANCE SYSTEM

The system within each vehicle continuously brings out the following algorithm:

1) Collection of Information

Each vehicle obtains its speed and Acceleration from the vehicle speed meter. The system inside each vehicle collects the information from GPS like position and time. All the information is placed in a packet which has the vehicle identification number of the vehicle. The following diagram of the packet is as shown in following Fig2.

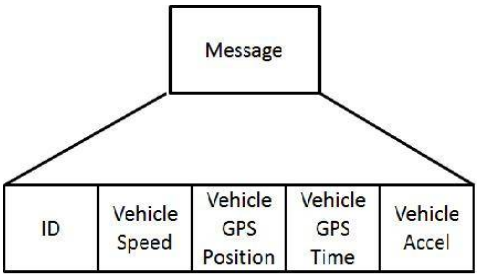


Fig 2 Collection of Information

2) SAFETY MESSAGE GENERATION

Following are the steps for creating safety message listed below.

a. Safety message generated by On Board Unit are sent to Hardware module according to the received data from other node.

b. Hardware module adds time stamp t to safety message.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

c. Then hardware module uses v-node's private key & digital signature on safety message is encrypted to create secure message.
d. The collection of information is transmitted to nearby vehicles with the help of multi-hop IVCs.
e. On the receiving side, message is passed to hardware module by on board unit.
f. Hardware module validates sender's signature using public key of the privacy key set
g. Hardware module contains original safety message, of the user if the signature is valid. Otherwise discards the message.

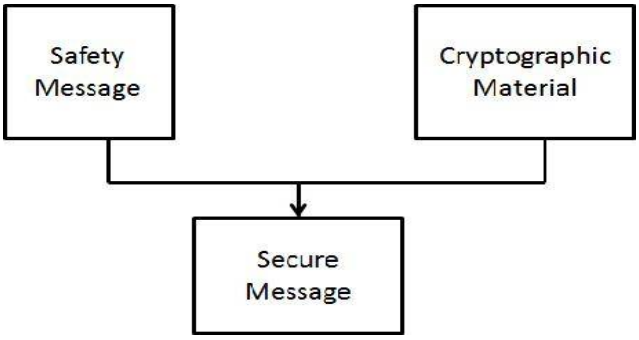


Fig 3 Message generation by cyrptography

3) S-PWCA Algorithm

The SPWCA algorithm will work as per the following steps-

Step1: -Generates secure message periodically. Step2: - Message arrives at a vehicle.
Step3:-After collecting the data 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 = $\sqrt{}$ X*X + Y*Y
Step5: - The distance between the two vehicles is calculated and found to be less than 5m; a warning alert is broadcasted to the vehicles to avoid the possibility of collision.
If Dv1, v2 < 5m Then
Collision Detected, Broadcast Secure Warning Message in Network. Else, in V2V network, data is transmitted related to traffic information.
Step6: - To avoid collision a secure message is generated, one of the vehicles will increase the speed with prior communication related to position, speed, time & another vehicle speed measure set to slow.

In this algorithm, the messages are generated according to their priority and will be processed one by one. As the message is received, the distance (Srel) between the vehicles is calculated and if the distance is negative, the message is discarded and will not be processed further.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

C. ALGORITHM FOR ACCIDENT AVOIDANCE

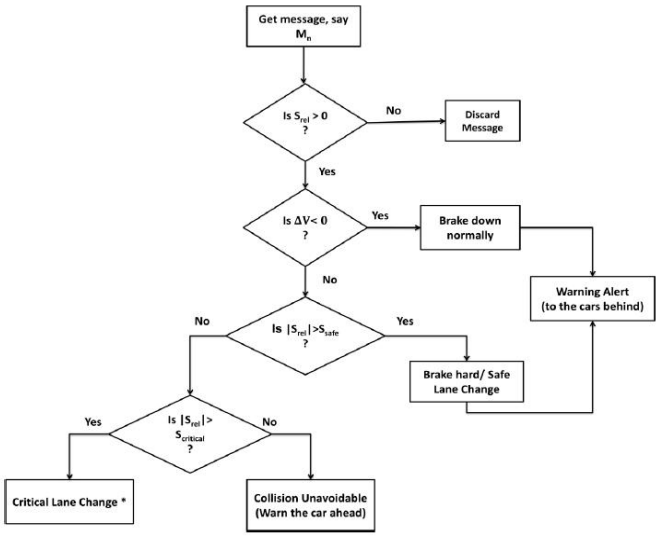


Fig 4 Algorithm for Accident Avoidance [2]

The probability is maximum when the host car collides with nearest front cars and collisions which take place from will not be considered. Host car decision to avoid collision will totally depend on parameters of front and the back cars, this will form a chain. Once the relative distance is calculated, the velocity (ΔV) is compared , and if it is true then the driver will break down normally and will also alert through the message to the cars behind it, but if it is positive the comparison is carried between safe distance and relative distance to check if the car is safe or not

VII. CONCLUSION

The secure message which will be broadcasted will improve the V2V collision avoidance which will improve accident rate in now-a-days life. Algorithm will calculate and compare the relative distance and relative velocity in V2V communication. This paper intention was to show the collision avoidance in V2V communication in VANET for the populated countries

REFERENCES

[1] Dinesh V. Jamthe, S. S. Dorle, Megha Chakole ―Secure Technique for Collision Avoidance in Inter – Vehicular Adhoc Network‖ 2012 Fifth International Conference on Emerging Trends in Engineering and Technology.
[2]Tanwee Kausar, Priyanka Gupta, Deepesh Arora2, Rishabh Kumar ―A VANET based Cooperative Collision Avoidance System for a 4-Lane Highway**”.**
[3]L. Xiaodong, L. Rongxing, Z. Chenxi, Z. Haojin, H. Pin-Han, and S. Xuemin, "Security in vehicular ad hoc networks," IEEECommunications Magazine, Vol. 46, pp. 88-95, Feb. 2008.
[4]University INTER-VEHICLE COMMUNICATIONSYSTEMS: A SURVEY 2ND QUARTER 2008, VOLUME 10, NO. 2 IEEE Communication Surveys Broadcasting at Intersections in Vehicular Adhoc Networks‖ 2010 International Conference on Electronics and Information Engineering (ICEIE 2010
[5] Mihail L. Sichitiu, North Carolina State University Maria Kihl, Lund University INTER-VEHICLE COMMUNICATION SYSTEMS: A SURVEY 2ND QUARTER 2008, VOLUME 10, NO. 2 IEEE Communication Surveys
[6] Sehun Kim, Sunghyun Lee, Inchan Yoon, Mija Yoon and Do-Hyeun Kim, Department of Computer engineering Jeju National University Jeju, Korea ―The Vehicle Collision Warning System based on GPS‖ 2011 First ACIS/JNU
[7] Samaneh Khakbaz, Iran University of Science and Technology Tehran, Iran Mahila Dadfarnia, Amirkabir University of technology Tehran, Iran―The Challenge of International Conference on Computers, Networks, Systems, and Industrial Engineering.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

[8] Nadra Ben Romdhane, Mohamed Hammami and Hanêne Ben-Abdallah ―A Generic Obstacle Detection Method for Collision Avoidance‖ 2011 IEEE Intelligent Vehicles Symposium (IV) Baden-Baden, Germany, June 5-9, 2011 [9]Vaishali D Khairnar et al ,Int.J.Computer Technology & Applications,Vol 3 (1), 370-373

[10]M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing vehicularcommunications," IEEE Wireless Communications,Vol. 13, pp. 8-15, Oct. 2006.

[11]Mihail L. Sichitiu, North Carolina State University Maria Kihl, Lund University INTER-VEHICLE COMMUNICATION SYSTEMS: A SURVEY 2ND QUARTER 2008, VOLUME 10, NO. 2 IEEE Communication Surveys[12]―Security Analysis in VANETs: A Survey‖ International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012 ISSN: 2278-0181

[13]M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, Vol. 13, pp. 8-15, Oct. 2006.

[14] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan ―Classes of Attacks in VANET‖ 2011 IEEE

[15] Albert Wasef And Rongxing Lu, ―Complementing Public Key Infrastructure To secure Vehicular Ad Hoc Networks‖ IEEE Wireless Communications, October 2010

[16] Sasikumar P, Vivek C, Jayakrishnan P ―Key Management Systems in Vehicular Ad-Hoc Networks‖ International Journal of Computer Applications (0975 – 8887) Volume 10– No.1, November 2010