RESEARCH ARTICLE OPEN ACCESS

Hardware Implementation of Collision Avoidance in Inter–Vehicular ADHOC Network Using Zigbee and Stellaris ARM Cortex-M4

J. Deeksha1, N. Radha2, U. Yedukondalu3
[1]Assistant Professor, [2]Senior Assistant Professor, [3]Head of the Department E.C.E.
[1]Aditya Engineering College, [2]Aditya Engineering College, [3]Aditya Engineering Col

Abstract
To avoid accidents on highway roads, it is necessary to maintain safe distance between vehicles referred as "Inter-Vehicular Distance". A warning system should be employed inside the vehicle, so that the vehicle could sense the distance between other vehicles by using GPS co-ordinates and ADHOC wireless network and then intimate it to the driver. The main objective of this paper is to implement the Inter Vehicular Adhoc network (IVAN) using Zigbee technology and developing the control circuit using Texas Instruments Stellaris launch pad which uses LM120XL ARM Cortex M4 processor. A graphical LCD is used to display the nearby vehicles dynamic information like position, speed of the vehicle, acceleration, door lock status, break failure, etc., The Zigbee wireless technology itself provides features like data Integrity, low power consumption, low cost, wide coverage area, large network up to 65536 nodes when compared with other wireless technologies. 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. The implementation results show the Zigbee technology is best suit for the IVAN by taking advantage of Low power and coverage area.
Keywords- IVC, IVAN, IVCN, PKI, S_PWCA

I. INTRODUCTION

Recently Inter-Vehicle Communication (IVC) has become an extremely hot topic in network research, opening up new research challenges well beyond those of classical Mobile Ad Hoc Network (MANET) research. The management and control of network connections among vehicles and between vehicles and an existing network infrastructure is currently one of the most challenging research fields in the networking domain. In terms of Vehicular ADHOC Network (VANET), Inter-Vehicle Communication(IVC), Car-2-X (C2X), or Vehicle-2-X (V2X), many Vehicular Ad-hoc Networks (VANETs) are wireless communication networks that provide interesting roadside services such as vehicular safety, traffic congestion, alternate routes, estimated time to destination, and in general improves the efficiency and safety on the road such as Collision Warning, collision avoidance, automatic control are also expected to result in a reduction of traffic accidents. Many conferences and venues have seen an increased research activity related to VANETs [2] [3] [4] [5]. Vehicular networks have been developed to improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public. The communications are controlled by interesting and challenging applications have been envisioned and realized. Dedicated Short Range Communication (DSRC) protocol, IEEE 802.15.4, ZIGBEE which is equipped with On-Board Unit (OBU). The ZIGBEE protocol got very good advantages when compared with Bluetooth in terms of power, bandwidth, cost, etc., V2V and V2I applications fall into two categories: Safety-related Information and Infotainment services. Only the security issues of safety-related applications are focused for collision avoidance in this paper as they are lying at the core of IVAN concept and bring challenging problems, since its matter of saving lives by preventing traffic accidents. The main characteristic of the IVAN is the infrastructure absence, such as access point or base stations. The communication between the nodes that they are beyond of the reach of transmission of the radio is made in multi hops through the intermediate nodes contribution as shown in figure1.

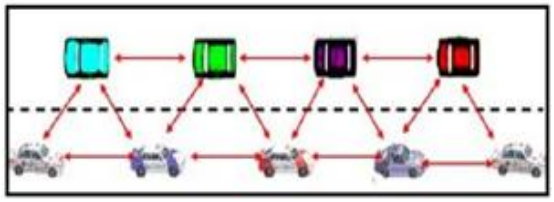


Figure1: V2V communication

II. 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.

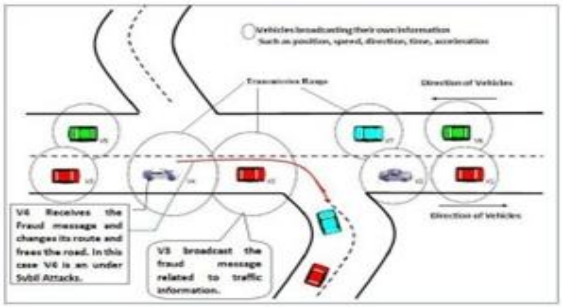


Figure2: In this example of Sybil Attack, attackers (V1 and V3) broadcast false information to affect the decisions of other vehicles (V4) and thus clear the way of attacker V5.

There is a challenge in balancing security and privacy needs. On 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. Each vehicle on the roads is assumed to be equipped with a radio (such as an IEEE 802.15.4-based or DSRC-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. Therefore the on-board unit processor should also capable to run the security algorithm to secure the broadcast message along with dynamic parameter calculations like, distance speed and acceleration.

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. So the delay in the broadcasting of message is highly unaccepted.

The above described problems, addressing the need of the high speed processor. Therefore this paper implements the on-board unit with help of ARM cortex-M4 processor (LM4F120XL) from Texas Instruments. The VANET application decisions can be a matter of life or death, any missing of message or slow updating of distance information because of slow processing may lead to huge damage to human life and their properties.

III. SYSTEM ON-BOARD UNIT HARDWARE DESIGN.

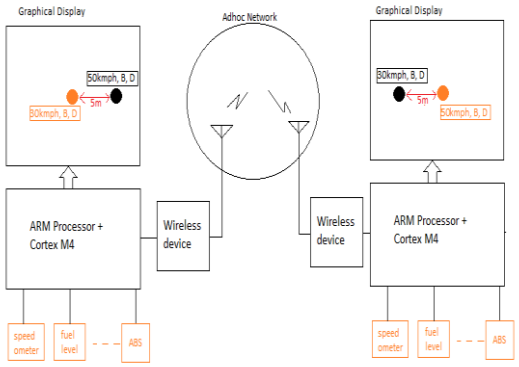


Figure 3: Block diagram of the On-Board Unit

The block diagram of the On-Board Unit is shown in figure4. The ARM Cortex-M4 (LM4F120XL) from Texas Instruments is used as the central processing unit with 80MHz clock frequency. A GPS device is attached to the processor unit, and always tracks the position of the vehicle. Now the processor filters the data coming from the GPS device and extracts the position coordinates, speed and time. A wireless Zigbee device is used to transmit or receive the information to or from the other nearby vehicles. When the processor receives the other nearby vehicle information via this wireless medium then calculates the distance by using the current vehicle position coordinates. A graphical LCD - JHD622-12864E is used to display the distance and other information like speed, acceleration, etc. If the distance calculated between the vehicles falls below the safe distance then a warning message is displayed on the screen to alert the driver. This high speed processor will ensure that no delay in the broadcasting of messages to nearby vehicles.

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 PKI-based technique is proposed. For broadcasting the secure message from vehicle in IVC network RSA 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. Public Key Infrastructure Technique

A PKI is an arrangement that binds public keys with users' identities through a certificate authority (CA). CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA. After registration the CA adds this user to a list and updates its list of users' identities and their assigned public keys. In addition to the registered users, CA will keep another list of the users with revoked certification. Meaning, the ones who were registered before, and for a reason, they should not trusted anymore. Each node is registered with only one local CA. In registration process, local CA issues a certificate, containing unique identity and validity period information of the node, and a public-private key pair. Local Ca's is responsible for revoking the compromised certificates. [17] The technique PKI allows two network vehicle users to authenticate each other to exchange using encryption. Therefore, password exchange mechanism can avoided, which can be very dangerous wireless medium. Since nobody can guarantee that a network is completely secure. Due to smooth and easy logic PKI infrastructure is advantageous. In this sender will sign a message, encrypt it using his private key. Similarly the receiver decrypts with the public key of the sender. It is also feasible for the sender to encrypt something the sender encrypts the message with the public key of the receiver. Then only the receiver can decrypt the message using his private key. For creating the secure communication between V2V RSA is used in this paper. RSA is a public-key cryptosystem that supports both encryption and digital signatures (authentication). Like all public key cryptography models, the RSA cryptosystem encrypts and decrypts a message using a pair of keys known as public key and private key [18]. Its security is based on the difficulty of factoring large integers. Presently, most implementations of the RSA algorithm employ the use of 512-bit numbers. Cracking such a system requires the ability to factor the product of two 512-bit prime numbers. Factoring a number of this size is well beyond the capability of the best current factoring algorithms.

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.

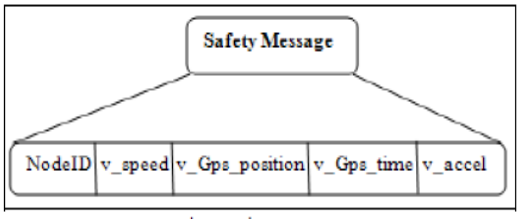


Figure4: Packet Structure

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.

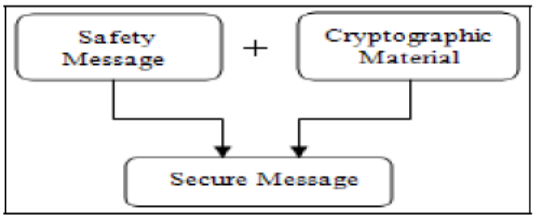
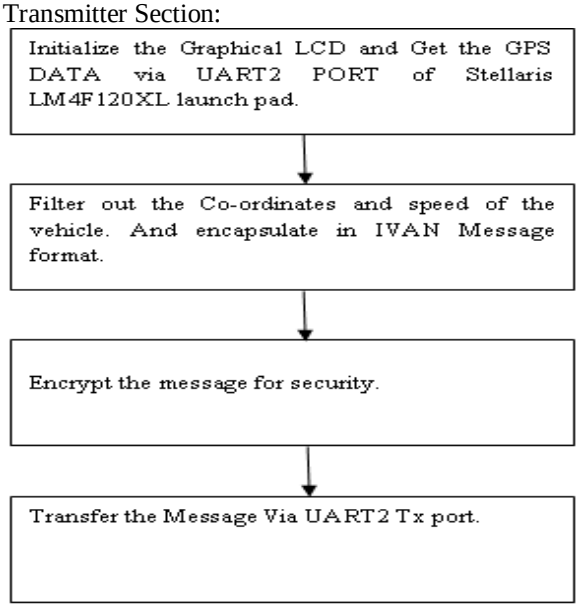


Figure 5: Generating secure message

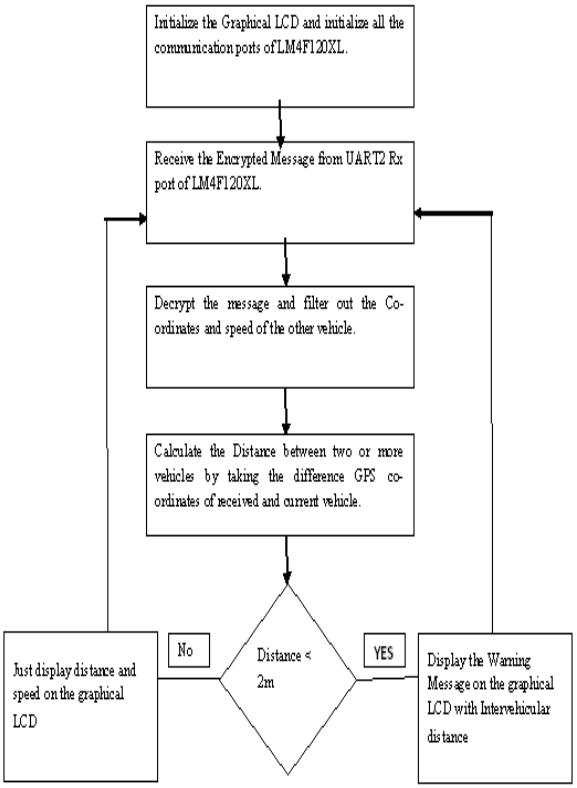
Generated secure message is periodically broadcasting in IVAN network using broadcasting wireless unit is installed at each vehicle should have the wireless unit which can communicate with another vehicle shown in figure4. Vehicles do not know position, speed, acceleration, time of neighbour vehicles. 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.

3) S-PWCA Algorithm: 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.

Transmitter Section:



Receiver Section:



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 project "Hardware Implementation of Collision Avoidance in Inter-Vehicular ADHOC Network using Zigbee and Stellaris ARM Cortex-M4"had been successful designed and tested. It has been developed by integrating features like High speed processor, so that it can be able to self drive the devices like GPS Interfacing, graphical LCD etc., Every module is placed carefully. Using very high speed processor "ARM Cortex-m4" the project is successfully implemented for sharing the messages from the network and other details like petrol consumption and break failure detection from vehicle which is in among the network.

REFERENCES

[1] Falko Dressler_, Frank Kargly, J¨org Ottz, Ozan K. Tonguzx, Lars Wischhof "Research Challenges in Inter-Vehicular Communication" – *Lessons of the 2010 Dagstuhl Seminar.*

[2] P. Krishnamurthy, "Information dissemination and information assurance in vehicular networks: A survey," *in A Conference Poster in iConferenc 08`, Los Angeles, Feb. 2008.*

[3] L. Xiaodong, L. Rongxing, Z. Chenxi, Z. Haojin, H. Pin-Han, and S. Xuemin, "Security in vehicular ad hoc networks," *IEEE Communications Magazine, Vol. 46, pp. 88-95, Feb. 2008.*

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

[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 International Conference on Computers, Networks, Systems, and Industrial Engineering*.

[7] Samaneh Khakbaz, Iran University of Science and Technology Tehran, Iran Mahila Dadfarnia, Amirkabir University of technology Tehran, Iran "The Challenge of Broadcasting at Intersections in Vehicular Adhoc Networks" *2010 International Conference on Electronics and Information Engineering (ICEIE 2010).*

[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] M. R. Hafner1, D. Cunningham2, L. Caminiti2 and D. Del Vecchio3 "Automated Vehicle-to-Vehicle Collision Avoidance at Intersections" *This work has been in part funded by NSFGOALI Award CMMI0854907.*

[10] Tarik Taleb, *Member, IEEE,* Abderrahim Benslimane, *Senior Member, IEEE,* and Khaled Ben Letaief, *Fellow, IEEE "*Toward an Effective Risk-Conscious and Collaborative Vehicular Collision Avoidance System" *IEEE Transactions On Vehicular Technology, Vol. 59, No. 3, March 2010.*

[11] Juan-Bautista Tomas-Gabarron, Esteban Egea-Lopez, Joan Garcia-Haro, Rocio Murcia-Hernandez "Performance evaluation of a CCA application for VANETs using IEEE 802.11p" Department of Information Technologies and Communications Technical University of Cartagena. *2010 IEEE.*

[12] Huang Zhu & Gurdip Singh "A Communication Protocol for a Vehicle Collision Warning System" *2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing.*

[13] Zaydoun Yahya Rawashdeh and Syed Masud Mahmud "Intersection Collision Avoidance System Architecture" *IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2008 proceedings.*

[14] Shouzhi XU, Huan Zhou, Chengxia Li, Yu Zhao "A MULTI-HOP V2V BROADCAST PROTOCOL FOR CHAIN COLLISION AVOIDANCE ON HIGHWAYS" *Proceedings of ICCTA2009 IEEE.*

[15] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan "Classes of Attacks in VANET" *2011 IEEE.*

[16] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux "Secure Vehicular Communication Systems: Design and Architecture".

[17] Albert Wasef And Rongxing Lu, "Complementing Public Key Infrastructure To secure Vehicular Ad Hoc Networks" *IEEE Wireless Communications, October 2010.*

[18] 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.*

[19] M. raya, A. Aziz, and J. Hubaux, "Efficient Secure Aggregation in VANETs". *The 3rd ACM International Workshop on vehicular Adhoc Networks(VANET06), September 2006.*