Design Approach for Implementation of Vehicle to Vehicle Communication Using Control and Warning Packets

[1] Pooja Kothe, [2] V. N. Katkare

[1, 2] Department of Computer Science and Engineering, Nagpur University,
G. H. Raisoni Institute of Engineering and Technology for Women, Nagpur
Nagpur, Maharashtra 440028, India

Abstract- One of the key requirements of Vehicular Ad hoc Network (VANET) is to provide secure communications between vehicles on the road. In this paper, we explain our work on the secure transmission of control and warning messages which are transmitted between the vehicles to avoid any traffic jam, accident, bad weather, etc. Our proposed module implements an algorithm which processes the received message packets and ensures that the message is from an authorized sender before acting on the message. The expected outcome of the system will be to develop a complete prototype vehicle model which will demonstrate secure communications in vehicular networks.

Keywords - *Vehicular ad hoc network (VANET), control and warning messages, secure communication.*

1. Introduction

Driving means frequently changing location. This means a frequent requirement for information on the current location and the data regarding traffic, routes, etc. This information can be grouped in several classes. The most important class is to fulfill driver needs on road side and car safety. To support this class many different things required such as data forwarded from other cars. One could think of warning about sudden break alert from preceding car, warning about dangerous distance between cars and collision warning, information about road condition, data about weather forecast, forewarning about traffic jams, alerting about an accident behind the next curve, complete information about an accident in order to guide the rescue team and many other things.

We can also think about car navigation system or an assistant so that we can follow the preceding car activity. Another class is infotainment for passengers or drivers. For example accessing internet, exchanging information (chatting or gossip type conversation) and can play interactive games between cars close to each other.

In the communication process there are many security threads, that disturbs the communication and this leads to many misunderstanding. If we focus on the field of security thread in VANET, many safety algorithm are developed. If security thread is not get considered during communication then the communication may be get disturb by third party attacker. Therefore it's also an important consideration in the communication process.

The key feature of this system is that it is focusing on message types and how they can be differentiated from each other so that the driver will take precautionary action to avoid any critical situation or follow the same path followed by the vehicle moving in same direction.

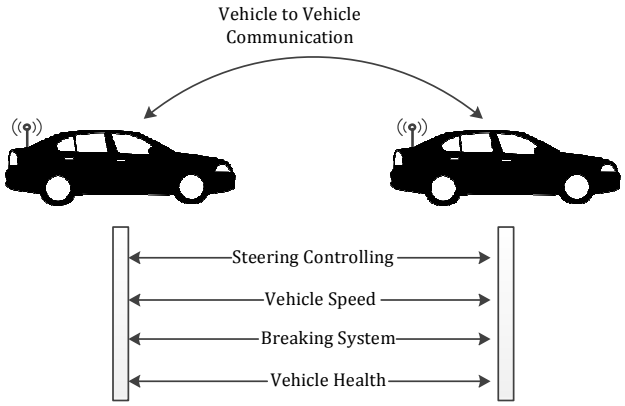

Fig.1 Messages Transferred Between Vehicles.

Fig. 1 shows the types of messages will be transferred between the vehicles. Steering control is the control type of message that indicated the controlling scenario to get indicated for the indicator signaling. Similarly the vehicle control and breaking system is the warning type of messages that helps to warn other vehicles to take

precautionary action against the accident or any avoidable condition.

This paper is divided into four sections; Section 2 presents the related views about the communication in VANET, Section 3 describes the proposed methodology, Section 4 and Section 5 shows the working of test beds i.e. communication module and Identification of fake packet/ message respectively and Section 6 concludes the paper.

2. Literature Review

In [1], a novel approach has been developed that helps to improve safety messages transmission in VANET using vehicles group. It shows the mechanism that allows formation a group and then depending on priority how the messages will get broadcasted. The priority is decided depending on the type of messages i.e. Simple safety message or Event driven safety message. The result shows the performance of scheme based on packet delivery ration and back-off count for multi-hope broadcast communication.

In VANET exchange of information can be done in various ways specified in [2], [3]. The problem with the existing protocol is collision of messages and stability problem in VANET communication require an adaptable protocol that can be easily adjustable in any condition in VANET. This functionality has been proposed in [2] via APAL rebroadcast protocol which overcomes all the problem of existing protocol related to rebroadcasting, security and performance. Since we are working in VANET where multi-hope broadcasting of messages is key technique but this leads to the congestion when multi-hope simultaneously re-broadcasts emergency or warning messages. This condition faces loss of messages as well as power of transceiver channel. To overcome this problem the various scheme [4],[5] has been developed that helps to achieve high delivery rate and fast transmission of emergency and warning messages by keeping way simultaneous collision.

In Vehicular Ad Hoc Network collision avoidance is the most important application area. In real time collision between vehicles due to any reason is not new thing. The cases of accident can be reduced if prior information about the collision or the cause of collision is known. The analytical model has been proposed in [6] that show the numerical result based on the three models specified in it helps to analyze the situations as well as provides analysis model for emergency message reception and accidental proportionality. This helps to integrate flow theory in VANET analysis which will lead to the intelligent transportation in future. In the recent years extensive accident warning test has been taken to identify the working of Inter-vehicular communication [7] that shows the experimental outputs to support extensive accidental warning messages. If the vehicles want to exchange information i.e. they are trying to communicate via direct communication process. But direct communication is highly vulnerable to interference and a physical obstacle doesn't allow them to exchange localization information therefore the protocol has been developed [8] to provide the security in Non-line-of-site situation and helps in location verification. This protocol shows the improvement in neighborhood awareness in non-line-of-site condition.

If in communication process channel is busy i.e. not accepting messages and still the messages are broadcasted simultaneously then message loss increases and performance of messages delivery decreases. This thing is not tolerable in VANET or in wireless communication. The proposed scheme shown in [9] helps to overcome this problem faced by vehicles on road side. In [10], we developed an analytical model that shows the performance of safety message transmission in VANET based on two priority classes. The developed model helps to analyze better tradeoff between network parameter. In the communication process there are a chances of various attacks specified in [11] (Monitoring attack, Social Attack, Timing Attack, Application Attack, Network Attack). Here various classes of attacks are defined and specified how they affects the communication in VANET. Here DOS (Denial of Services) is an important attack that needs to be stopped.

3. Proposed Research Methodology

Step 1:- Develop a communication module to transfer and receive messages.

Step 2:- Identify the un-authenticated fake packet from third party.

Step 3:- Create messages depending on the analysis of control and warning related information. For that we are proposing a packet format based on awareness information which will be broadcasted over channel.

Device Name	Fix ID	Channel ID	Message	Reserve

Fig.2 Packet Format

The description of the field names shown in Fig 2 is given below:

Device Name: - Indicates the logical name of the device that will be used to identify the vehicle.

Fix ID: - It is a manufacturer ID that will be used to authenticate the communication.
Channel ID: - This field gives the frequency ranges over which the communication will take place.
Reserve: - This field is reserved for future additional needs.

Step 4:- Assembling a model that will help to demonstrate the functionality. Fig. 3 shows the proposed architecture of the system.

It contains micro-controller board connected with input unit, control unit, LCD module and transceiver.

Input unit takes the input from the external devices like clutch, accelerator, etc. This indicates the types of message which will be generated, so that the control unit will react accordingly.

Control unit will be connected to the control devices of the vehicle to control the vehicular activity like speed, break, etc.

LCD device will be connected to the micro-controller to show the indication related to the received message type.

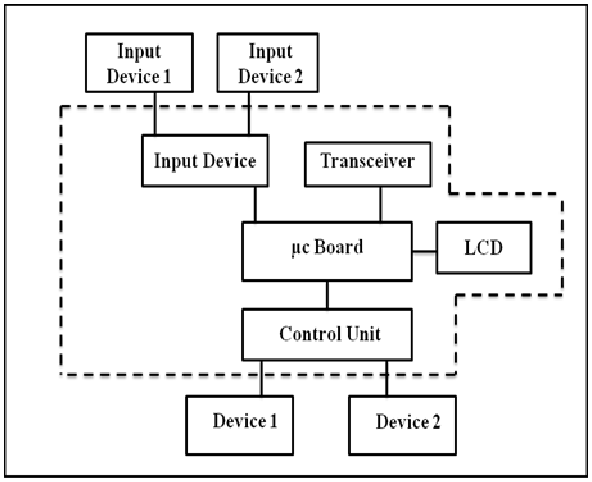

Fig.3 Proposed System Architecture

This methodology leads to the following points of consideration.

1. Communication,
2. Versatile Messages,
3. Data Security.

For communication, we have used a transceiver for wireless data transfer of versatile messages which carry control or warning packets used to inform driver about the road side conditions.

To identify the sender we will need a micro-controller based hardware and software module which will identify the sender by a unique ID.

4. Communication Module

As the idea behind the proposed system is to create wireless nodes for V-2-V communication, so we created experimental test bed using Atmega family development board. Here a node consist of LCD unit for showing communication messages; Atmega16 microcontroller for controlling logic, CC2500 based RF module and UART port for connecting RF module with Atmega16.

Advantage of using CC2500 is, it is having multiple channels to let the nodes communicate in different channels for preventing it from frequency conflict. It also provide a logical addressing scheme to give unique ID to every node and the module will internally check for the message with matching ID while receiving the messages and this will let the system unicast, multicast and broadcast messages between nodes.

Atmel Studio 6 is used for writing the 'C' code for communication module. For successful and connection oriented communication we implemented the message acknowledgment scheme. By the time starting the nodes it waits for connection request from any other node. Like in mobile service any node can initiate connection and act like guest and other node will act as a host.

Now consider the condition there are two nodes A & B. First A will send connection request to B by sending predefined symbol and if B accepts it, then it will give acceptance acknowledgement to A and both are ready for transferring the data by creating logical connection between both. For testing purpose node can send two predefined messages to other node and receiving node will display it on LCD. At any time of instance any node can close the connection and send the connection closing acknowledgement to other node so that other node can stop data transfer. This complete connection is logical and not in one to one mode rather broadcast mode.

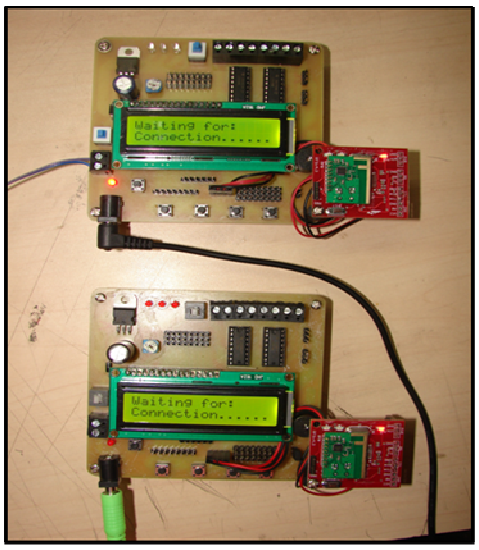

Fig.4 Communicating Devices

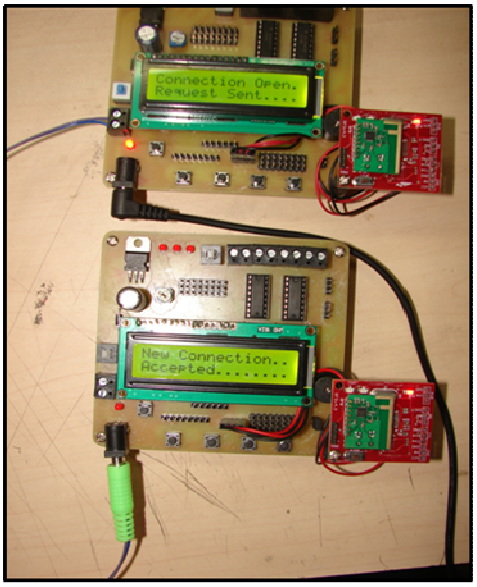

Fig. 5 Establishing Connection between Devices

5. Identification of Fake Packet/Message

In the communication module shown here, two wireless nodes communicate with each other for exchange of information. In VANET any node is an active participant in the communication through the broadcast of messages which is received and reacted upon by other nodes. Therefore it is important to identify the fake broadcast packets for secure communication in VANET.

In this module we are using CC2500 based RF module which has a logical addressing scheme that provides a unique ID to every node. Our proposed module is shown in Fig.6. In the developed test bed Node A and Node B are authorized nodes and the Node Att. is an Attacker/Hacker Node. In this scenario when the Node A wants to connect with the other node (i.e. Node B), it sends a request for connection which includes Node A's unique ID. The node which responds with the received Id and his unique ID becomes an authorized node for communication (here we are considering only one-to-one communication).

Now, let us assume that in the current session, the Node Att. become an attacker node whose ID is not in the memory of either Node A or Node B. When the Node Att. sends message to Node A and Node B during current session it is detected as a fake packet and rejected, thus rejecting the attacker/hacker Node Att. in the current session.

Nodes broadcast the message M according to the format shown in Fig.2.

General scenario for every sender node in VANET:

Step 1:- Sender (Node A) generates the unique ID (FID) for the current session.

Step 2:- Identifying channel for transmission (CID) in the current session.

Step 3:- Generating message (say, M) - either control or warning or infotainment message according to given situation.

Step 4:- Wireless node broadcast {DN||FID||CID||M||X} to neighboring wireless node.

General scenario for every receiver node in VANET:

Step 1:- If received message's FID is not identical (after comparing from memory) then check for message type.

Step 2:- If message type = "Request for Connection" then respond it by following same steps as sender node i.e. {DN||FID||CID||M||X} + (Node A) SFID.

Where,
SFID is sender's FID (in this session FID of Node A)
M is the acknowledgement for sender (Node A).

Step 3:- If message type = any string (control or warning message) and connection is open then

If SFID = FID (current sender of message) then message will be received successfully.

Else
If SFID! = FID (current sender of message) then message will be discarded and identified as a "Fake Packet".

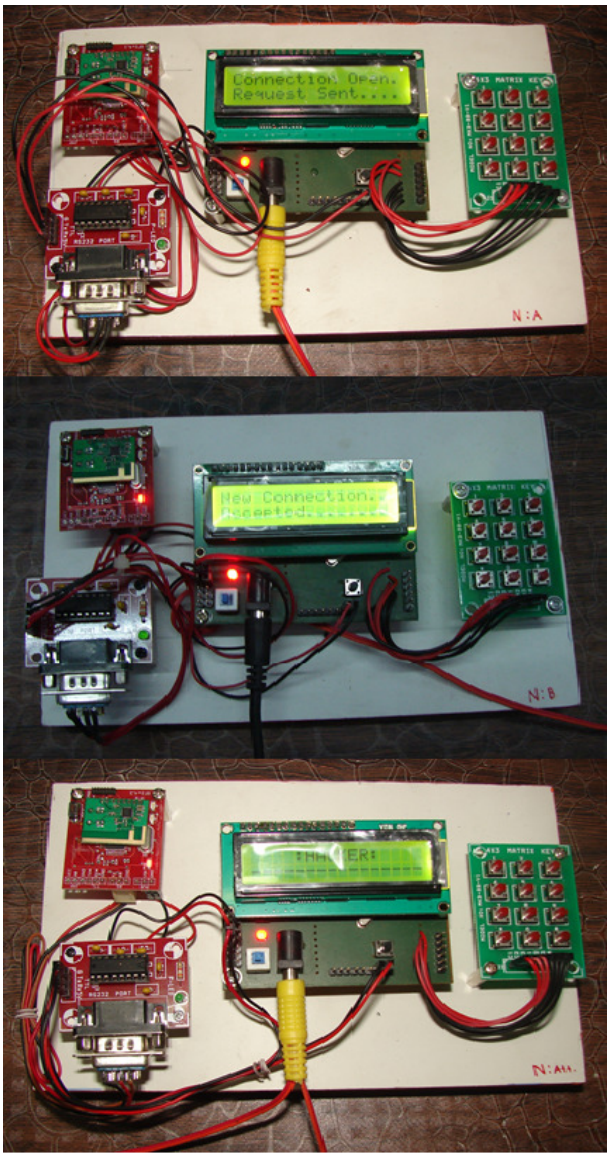

Fig.6 Identifying Fake Packet

6. Conclusion

In VANET the driver must be reported every time there is a sudden change in the condition on road side. If the diver is not aware about the changing condition then it will affect emergency message transmission leading to many problems such as traffic dead ends, blind spots, etc.

The exchange of messages helps to update the neighboring vehicles' records and raises the awareness of other nodes through requests and replies. The developed test bed helps to identify fake packet so that the trusted third party can reveal misbehaving users. Our solution thus demonstrates the secure transmission of messages between two devices in a VANET network.

References

[1] Ambuj Kumar and Rajendra Prasad Nayak,"An Efficient Group-Based Safety Message Transmission Protocol for VANET", *International Conference on Communication And Signal Processing, April 3-5, 2013.*

[2] Kanitsorn Suriyapaiboonwattana, Chotipat Pornavalai, Member IEEE, and Goutam Chakraborty, IEEE SM," An Adaptive Alert Message Dissemination Protocol for VANET to Improve Road Safety", *FUZZ-IEEE 2009, Korea, August 20-24, 2009.*

[3] N. Wisitpongphan,o. K. Tonguz,j. S. Parikh,p. Mudalige, f. Bai,v. Sadekar, "Broadcast Storm Mitigation Techniques In Vehicular Ad Hoc Networks", *Communications Magazine, IEEE, December 2007.*

[4] Liqi Wei, Xiaoqiang Xiao, Yingwen Chen, Ming Xu, Haikuan Fan, "Power-control-based Broadcast Scheme for Emergency Messages in VANETs", *IEEE 2011.*

[5] Ching-Yi Yang and Shou-Chih Lo,"Street Broadcast with Smart Relay for Emergency Messages in VANET", *IEEE 24th International Conference on Advanced Information Networking and Application Workshops, 2010.*

[6] Sok-Ian Sou, "Modeling Emergency Messaging for Car Accident over Dichotomized Headway Model in Vehicular Ad-hoc Networks," *IEEE Transactions On Communications, Vol. 61, No. 2, February 2013.*

[7] Gustavo Marfia, Marco Roccetti, Alessandro Amoroso, and Giovanni Pau, "Safe Driving in LA: Report from the Greatest Intervehicular Accident Detection Test Ever," *IEEE Transactions On Vehicular Technology, Vol. 62, No. 2, February 2013.*

[8] Osama Abumansoor, Azzedine Boukerche. "A Secure Cooperative Approach for Nonline-of-sight Location Verification in Vanet", *IEEE Transactions On Vehicular Technology, Vol. 61, No. 1, January 2012.*

[9] Vaishali D. Khairnar and Dr. Ketan Kotecha,"Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment", *International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.2, March 2013.*

[10] Mehdi Khabazian, Sonia Aïssa, and Mustafa Mehmet-Ali, "Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks", *IEEE Transactions On Intelligent Transportation Systems, Vol. 14, No. 1, March 2013.*

[11] Irshad Ahmed Sumra, Iftikhar Ahmad Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of Attacks in VANET", *Electronics, Communications and Photonics Conference (SIECPC), Saudi International, April 24-26 2011.*

Miss. Pooja Kothe holds a Bachelor of Engineering degree in Computer Science and is currently pursuing Master of Engineering in Wireless Communication and Computing.

Ms. V. N. Katkar holds a Bachelor of Engineering degree in Computer Technology, Master of Engineering in Wireless Communication and Computing and is currently an Assistant Professor in G. H. Raisoni Institute of Engineering and Technology for Women, Nagpur University.