A Survey on Security in Vehicular Ad-Hoc Network

Under the guidance of Dr. Arjan Durresi
By Debraj Dey
Indiana University Purdue University, Indianapolis

***Abstract*—A vehicular ad-hoc network is a special type of network for the vehicle to vehicle (V2V) communication system. As the amount of vehicle is increasing in the roads drastically, the concern about the safety and security is alarming our doors. The issue is not only about security but also about the safety of mankind. The paper gives you an idea to understand and analyze the vehicular routing process and different security features in Ad Hoc network. It also discusses the challenges regarding automotive security and gives you several probable solutions to counter the problem. This paper also includes a brief discussion about different legacy routing protocols and the misuse that can happen if we keep on using these protocols.**

***Keywords*—Vehicular ad hoc network (VANET), vehicle to vehicle (V2V), medium access control (MAC), Dedicated Short Range Communication (DSRC), time driven multiple access (TDMA).**

I. Introduction

Different types of vehicular communications are increasing day by day. Unfortunately, vehicle hacking has already made the headlines, cyber britches are going to be catastrophic with respect to the safety of the vehicle or its occupant and a concern for the reputation or financial liabilities of many automotive companies. Not only that, but the concern regarding road accidents is also responsible for modicum deaths not only in the United States but also throughout the world. According to the survey in 2017 by Medical News Today [4], road accidents are the fourth leading cause of death in the US. Nearly 136,053 deaths were recorded alone in the year 2016. Statistics [6] shows 90% of these road accidents is caused by human error, and 60% of these accidents could be avoided if the driver could have given 0.5 seconds beforehand. So, to avoid all these difficulties, in this survey paper we will discuss different communication process include communication of Engine Control Unit or ECU, within a vehicle and vehicle to environment communication or V2E. But our main focus will be on the security in the vehicle to vehicle or V2V communication, where new evolving protocols like Medium Access Control protocol or MAC based on TDMA, commonly known as Time-division multiple access and a Delay Tolerance MAC protocol or DTMAC will be discussed and explore possible vulnerabilities of these protocols. Also, we will try to find out a probabilistic solution in terms of security and safety of the passenger as well as the vehicle altogether and look for various case studies related to vehicular vulnerabilities.

The rest of the research paper is divided into eight sections. In section II the protocols of VANET is discussed. Then in section III common automotive communication protocols are shown, and followed by safety requirements and attack detection or challenges in section IV and V. Further in section VI probable solution for security is shown. Finally, in section VII and VIII future work and conclusion is discussed followed by the references in section IX.

II. Protocols for VANET

VANET is not only used to provide onboard infotainment in the form of internet access, the location of free parking spaces in the road, video streaming, sharing music and much more but also it provides improved road security using different onboard technology as well as improved traffic management. The safety-related application [2] mainly relates to inter and intravehicular communications. For example, if an accident is detected on the road, a vehicle can continuously broadcast information about this critical situation to the vehicle which is approaching the accident

site. In this paper, I have discussed the three most important protocols that can improve the V2V communication for future VANET technology.

A. Medium Access Protocol (MAC)

Medium Access Protocol or commonly known as MAC is one of the most popular protocols that is used in data communication between two computers, known as point to point communication and between multiple computers, known as a broadcast network. Medium Access Protocol can be divided into four types of fixed assignments, random assignments, demand assignments, and mixed assignments. Implementing this concept in the Vehicular Adhoc network can work well. It can provide a broadcast service with bounded access delays, which can solve the sole purpose of communication between two or more vehicles even though the delay in Adhoc should be very less or negligible due to the nature of the network also it provides a minimum transmission collision which can give us effective and reliable communication.

B. MAC Based TDMA

MAC protocols distinctly with TDMA [12] technology allows multiple vehicles to use the same frequency channel. This process works without even interfering with each other's transmission range. It also helps to avoid reservation collision between two or more vehicle. But the real issues with TDMA is it uses distributed scheme which means it allocates different timeslots to vehicles, but here two different types of collision can occur. One, access collision where two or more vehicle trying to access the same available timeslots provided by TDMA [9] and the other one is emerging timeslots where two or more vehicle is already using an existing timeslot. To avoid both issues the Time-division multiple access (TDMA) principle consists of allocating the bandwidth to the vehicles by dividing the time into several different frames, these frames works independently, and each frame is divided into several timeslots. Each and every vehicle can access these channels during its dedicated timeslots to send or receive data. However, many issues arrive due to the greater number of vehicles in the road which can severely affect the performance of TDMA. Figure 1.1 shows two different frames are used for to different vehicles, where both are using different timeslots to avoid a collision.

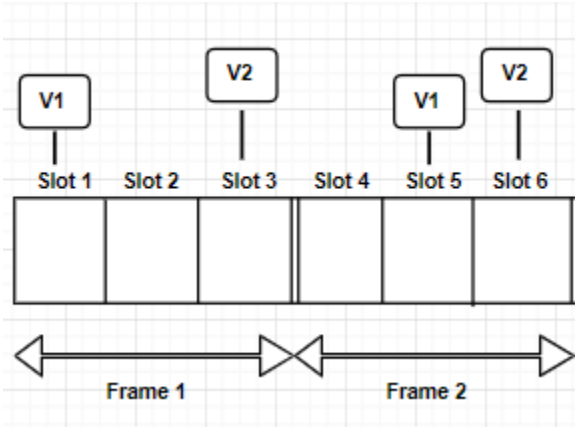

Figure 1.1: Vehicles using multiple frames in TDMA

C. DTMAC

In order to improve the efficiency of VANET [9] proposed a fully distributed TDM based MAC protocol which does not rely on an expensive infrastructure. The DTMAC [12] uses vehicles locations and a slot reuse concept to ensure vehicles and the adjacent have a collision-free schedule.

D. TRPM

In order to ensure event-driven safety messages can be sent long distance [10] proposed TRPM a TDMA aware routing protocol for multi-hop communication. This routing scheme is based on a cross-layer approach between the MAC and a routing layers in which the intermediate vehicles are selected using TDMA scheduling information. It gives better performance in terms of collision rate, average end to end delay and an average number of hops.

E. Dedicated Short Range Communication Channel (DSRC)

Commonly known as Dedicated Short-Range Communication channel is a short or mid-range communication protocol used especially in

a vehicular system. According to the Federal Communications Commission (FCC) a DSRC can allocate 75 MHz of spectrum in the 5.9 GHz band [11] for use by ITS vehicle safety and mobility applications. Applications like Blind Spot Warning or BSW, Lane Change Warning or LCW, Emergency Electronic Brake Lights or EEBL etc. are commonly used. The DSRC uses the OBD port to communicate, which is also a security concern for this issue.

III. Automotive Communication Protocols

These communications involve different protocols such as Controller Area Network or CAN, Local Interconnect Network or LIN, FlexRay. Such protocols are very vulnerable to various attacks which have been witnessed in past as well. My focus in this survey paper will be to explore those vulnerabilities along with proposing probable solutions for such issues.

A. Controller Area Network (CAN)

Invented by Robert Bosch in the year 1983, CAN is the widely used serial protocol in the automotive industry. Each automotive unit consists of at least three CAN Busses embedded in them. CAN operate in various speed stating from 128kbps up to 1024 kbps. All the major engine control units inside a car communicate with the help of CAN. This protocol can be classified into two sections. The first section is the low speed CAN, which had a speed of 200 kbps, the later one is the high speed can which consist a speed in between 200 kbps and 1 Mbps. CAN uses differential signals which means it has two wires for its data transmission. CAN doesn't involve node addressing while transmission of data in the bus, which makes it vulnerable to different types of attack. The paper [7], discusses various CAN vulnerabilities such as accessing the bus using the onboard diagnostic port. This proves tampering the bus is an easy accomplishment to achieve. In the paper [5] authors have performed various experiments to exploit the vulnerabilities present in CAN communication. Just like the tool Wireshark, there exists a tool called Carshark, which sniffs serial data packets. Moreover, using Carshark, we can penetrate malicious packets which can malfunction the onboard car computer system to kill the breaks, blasts music, disable the engine etc. CAN is easily accessible through onboard diagnostic ports or OBD, which is usually present beneath the steering wheel. The paper [6] which is about the infamous jeep hacking describes using the OBD 2 port to hack Jeep cars and make them function in a way in which they are not supposed to. Here a group of researches sent a random bit of code through the port and then they managed to open the trunk, blow horns even the breaks stopped functioning. Figure 1 typically describes the data frame of CAN, where the entire data frame is about 128 bits, but 120 bits are generally used. Of course, the data field contains the modicum bits between 0 to 64. The base identifier is of 11 bits, but the extended identifier is usually 18 bits in size. In the later section, I will discuss the probable solutions, which can be implemented to mitigate such vulnerabilities.

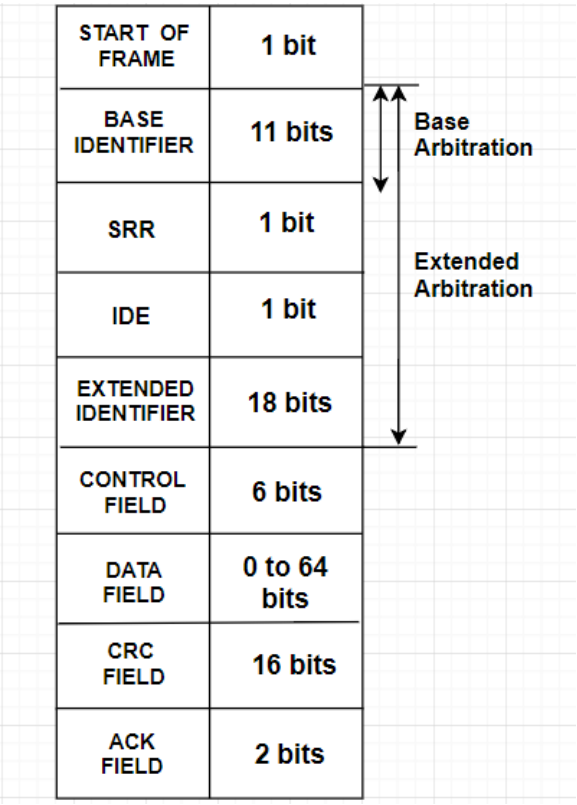

Fig. 1.2 Data frame of CAN

B. FLEXRAY

Modern vehicles and their complex driver assistance, safety functions are made possible,

thanks to the comprehensive integration of electronic control modules. These implementations require very high data transfer rates to transmit the increasing number of control and status signals. The signals not only need to be transmitted extremely quickly the transmission also needs to be time critical. The popular design of steering and braking system requires a fault tolerance network architecture and associated hardware. This is the reason for the growing importance of communication systems guarantee fast and time-critical data transmission. The Control Area Network or CAN cannot meet the needs of these new communication systems due to its limited bandwidth and event-driven bus signals. This is the reason why FlexRay has been introduced. Which is much faster and more reliable than CAN and TTP. Of course, installation of FlexRay can be only possible in the high-end vehicle due to the cost associated with it.

IV. Security Requirements

Every new application comes with some serious security concerns. Security requirements in a vehicle to vehicle (V2V) system include message authentication and integrity, where the content of the message must be protected from any alteration before and after the transmission. Security requirements also includes message non-repudiation [13], where the sender of a message cannot deny the fact that he or she sent a message. For example, in case of VANET if a vehicle gives right turn signal and goes left side, he or she cannot deny the integrity of the message.

In case of Entity Authentication, [8] the receiver is ensured by the fact that the sender generated a particular message and the receiver has evidence of the liveness of the sender including the Ip address or other packet information. Access Control Authorization, where authorization established what each node can do in the network. Security requirement also includes privacy and anonymity where vehicular communication (VC) systems should not disclose any personal and private information of their users. Any observes should not know any future actions of the nodes. [13] But sometimes the anonymity of vehicular information may not be a reasonable requirement for all entities of the vehicular communications system. According to the paper [13] published by P. Papadimitratos, V. Gligor and JP Hubaux “Liability Identification is when protocols and services should remain operational even in the presence of faults, malicious or benign”. And finally, availability, where users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes. [8] In case of confidentiality of the message, where the content of a message is kept secret from those nodes that are not authorized to access it. Which means a particular node in a network is not supposed to access the information which is sent by a private node. The next section of the paper describes the challenges regarding attack detection.

V. Attack Detection or challenges

Detecting an attack and securing your own data and personal information is a key aspect right now. The following points below gives us an idea of how attack detection can work out.

A. Increasing attack surface

These days modern vehicles are increasing technical interfaces, which are reaching the outside world and interconnects the car with services which are external to it. Here, attack surfaces in a car include [1] wireless connection or Wi-Fi, Bluetooth, aux cables, USBs, ethernet. Also, things like charging stations, ports or other backend devices etc. It means the car is more and more becoming a part of the internet of things, which makes it more vulnerable.

B. Need to protect features and Business

This is one of the most important challenges in the automotive industry, where every day new features in the car or new business models are coming up. But, the downside of this is that the things are getting more critical, which means the attack surface’s connectivity involves the potential of attacking the cars itself from the potential interfaces or attack surfaces. We must understand that it is not just protecting the individual cars but protecting the business model

as well. So, that in the future the company doesn't have to suffer from potential loss of customers.

C. Legacy Technologies

Bringing new technologies in the automotive security field is important. Protocols like CAN and automotive Ethernet will still be around. But more features are coming along includes more threats towards the security if the car. Also, these old protocols are not designed with security mind which is a great concern right now. Introduction of different firewalls can also come handy, but the implementation of it in an automotive environment is difficult and time-consuming. Also, meaningful transfer of IT security technologies required.

D. Lack of automotive specific standards

Now the subject of security in automotive requires a lot of consultation due to Limited resources for security mechanisms or performance constraints, that makes it a little difficult to implement. Also, security includes a number of processes and functions. In upcoming days more testing and implementation can be introduced in the industry including brand new tools and software.

VI. Probable Solutions

A. Authenticating user with digital signature

The concepts of cryptography and using digital signature is nothing new, it is getting developed each day. This concept can be implemented in terms of automotive security as well. Where once a vehicle receives a packet from another vehicle, some sort of public and private key should be used to decode and encode the packet or the request. This will help to get at least one layer of security during the communication process.

B. Layered Security Concept

Security is nothing alike one action can prevent the entire service or function. So, breaking into different layers are difficult that breaking one vault at a go. The concept of layered security concepts is nothing new but requires more precision to implement. Figure 2 shows a basic concept of layered security where the core is a secure platform, which includes key storage, a library of crypto functions, encoding-decoding computation and calculation, secure boot hardware and security updates are the part and parcel of it.

The next layer of the layered security is the Secured In-Vehicle communication, where we know the information regarding the messages which is sent or received. Means, the authentication of the message, the integrity of the message so that the messages are not being modified or been changed, and freshness which is to check the messages are not outdated. Also, the confidentiality of the message comes into play.

So, the layer above the Secured In-Vehicle Communication is Secure Gateway, which includes firewalls, access control, key infrastructure throughout the processes which are updateable and distributed. This layer also includes synchronized secure time, different intrusion detection mechanisms and functions etc.

The outermost layer is called the Secure External Communication, through which the security threats are often reduced from a charging device or a backend service.

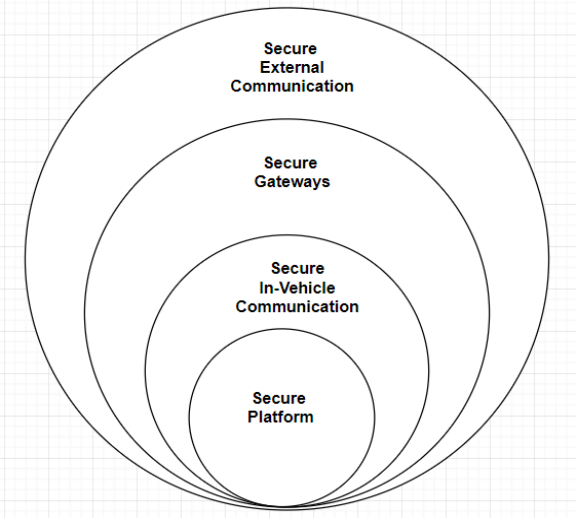

Fig 2: Layered Security Concept

C. Trustworthy system using machine learning

This can be achieved by implementing different algorithms and analyzing mathematical

models. [4] The process of creating a true mathematical model requires a lot of computation resources and manpower. The true system will be able to detect the malicious packets using machine learning and the model which can perform a particular task which is assigned to it.

D. Building up good and bad profiles for different network traffics

Creating a profile after analyzing the packets can be helpful in this process. Like Wireshark, in case of vehicle we use Carshark, this tool can help us to detect packets which are being sent and received from the vehicle. So, in this process we first need to collect all the packets and then analyze them, once the analyzation is done, we can start to create different profiles. The profiles will be generated in terms of the trust. This will be achieved by normalizing the number of packets which are being dropped or received. For example, if an Ip address drops a lot of packets then it has a less score than an Ip which doesn't. Also, by using this process we can detect malicious packets and stop them from in coming.

VII. Future Work

From the future point of view, we can suggest that the vehicle to vehicle (V2V) will gain much more popularity in upcoming years. This survey paper allows you to find different aspects of VANET and security associated with it. In terms of future work, a lot of implementation and development is required before this technology comes into the public. Also, the concept of the smart city can only come to reality if we create smart vehicle not only in terms of safety but also the security of that vehicle from hackers must be considered. Also, as 5G LTE network is coming along with the V2V communication, the future of security is bright.

VIII. Conclusion

This survey paper represents a brief history of legacy protocols in automotive communication especially in V2V system. Also, discusses about the probable security concerns and type of attacks that can occur regarding a vehicle to vehicle communication process. This paper also portrays several solution techniques and ideas that can come handy in the future security aspects. Further, the goal of this paper is quite achieved in terms of discussing all the protocols regarding vehicle to vehicle communication system.

IX. References

[1]. Network security and surveillance system by MV Trcka, KT Fallon, MR Jones, RW Walker - US Patent 6,453,345, 2002

[2]. Vehicle tracking and security system by John P. Mansell, William M. Riley. Publisher number US5223844B1

[3]. Intrusion detection system using deep neural network for in-vehicle network security by MJ Kang, JW Kang - PloS one, 2016 - journals.plos.org

[4]. Medical News Today by Hannah Nichols 23th February 2017

[5]. Vehicle network security testing by Jihas Khan, IEEE Explore. INSPEC Accession Number: 17263298

[6]. Human error as a cause of vehicle crashes by Bryant Walker Smith on December 18, 2013.

[7]. Experimental security analysis of a modern automobile by Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno. Department of Computer Science and Engineering.

[8]. Cyber security attacks to modern vehicular systems by L. Pan, Hongxu Chen, Xi Zheng, Lynn Batten, Journal of Information Security and applications. 29th August 2017.

[9]. Game-based TDMA MAC Protocol for Vehicular Network by Zhang Tianjiao and Zhu Qi, Journal of communications and networks, vol. 19, No. 3, June 2017.

[10]. PTMAC: A Prediction-Based TDMA MAC Protocol for Reducing Packet Collisions in VANET by Xiaoxiao Jiang; David H. C. Du.

[11].DSRC v. 5G: Which Will It Be for Connected Vehicles? by Wassom, Brian, June 19, 2018.

[12]. Design and optimization of access control protocols in Vehicular Ad Hoc Networks (VANETs) by Mohamed Hadded 30th November 2016.

[13]. Securing Vehicular Communications - Assumptions, Requirements, and Principles by P. Papadimitratos, V. Gligor, JP Hubaux