A Empirical Study on Connected Vehicles

Kirti Gupta[1], Nitish Kaushik[1]

[1]MCA Student, Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India

---***---

Abstract - Connected vehicles are the future of Transportation. Though autonomous vehicles have been there in the scene for quite a time now and are being implemented and used in the modern vehicles by the Vehicle Companies, there is still a lot of challenges in attaining fully driver less vehicles that can run in dynamic scenarios. Connected vehicles is the way by which we can have infrastructure and vehicles communicating among themselves and take smart decisions based on their communication. In this paper we will discuss few techniques/protocols which can be used by Connected Vehicles to increase the performance, reliability and data rates and also the potential threat vectors that could be potential source of vulnerabilities for the system.

Keywords—component, formatting, style, styling, insert (**keywords**)

1. INTRODUCTION

The most crucial problems that are present in most of developed and developing countries are traffic congestion, cost of extra fuel and road accidents. Despite of all the hi-tech transport management systems and other advanced technologies. With increasing number of vehicles on road the above problems are also increasing which suggests us to come up with certain paradigm which could reduce these problems and save millions of lives of the people who lose their life in Road accidents every year. One such techniques that are in trend is Connected Vehicles. However like every new technology there are lot of challenges inside and outside that are still waiting for their answers as of now. Discussing further on Connected Vehicles a study[1] led by the U.S. Department of Transportation (U.S. D.O.T.), connected vehicles can save 74% of car crashes. Hence making this field more promising.

In this paper, we will discuss few techniques that promise to be the solution for the problems that are inherent in the connected vehicles scenario and also we will discuss that what are the potential vulnerabilities and threat vectors that are present so that we can optimize our solutions to make it less vulnerable security wise.

2. TECHNIQUES

- There are few techniques used by the vehicles to make the communication among them possible. Few of the techniques are Dedicated Short-Range Communications (DSRC), **On**line **C**ontrol **A**pproach for **P**ower and **R**ates (OnCAR) which promises consistent performance in highly dynamic environments[2].

Dedicated Short-Range Communications (DSRC): DSRC or Dedicated Short-Range Communications can be explained as a communication that takes place between the various components that together consist of the environment of the connected vehicles i.e. the infrastructure and the vehicle itself. The DSRC consists of two types of the communication vehicle to vehicle a.k.a V2V and Vehicle to Infrastructure a.k.a V2I communication. Both these communication constitutes the Connected vehicles environment. The DSRC technology enables variety of applications such as adaptive cruise control, forward collision warning, lane change assist and etc [2].

According to U.S. Department of Transportation (U.S. D.O.T.)[3], DSRC enables the most reliable, high speed vehicle-based technology for crash prevention safety applications, provides for a broad cross-section of dedicated connectivity options for surface transportation safety and DSRC based communications serves as the basis for connected vehicle safety and mobility application integration.

There are two types of communications that take place in DSRC:

a. Vehicle to vehicle communication (V2V): According to wikipedia, [4] “Vehicle-to-vehicle (V2V) is an automobile technology designed to allow automobiles to "talk" to each other”. As the name suggests, vehicle to vehicle communication takes place between vehicles to share vital information like positions so as to avoid collisions when changing lanes or taking blind turns via. Notifications/warnings. This all communication takes place over short-waves. The US V2V standard is commonly known as WAVE (Wireless Access for Vehicular Environments) and based on the standard IEEE 802.11p.

b. Vehicle to infrastructure communication (V2I): Just like V2V, V2I is the technology by which the vehicle communicates with the surrounding infrastructure. The infrastructure may vary from a traffic signal to a smart band wore by a person to make his trajectory and position visible to the surrounding vehicles to ensure safety. Vehicle to infrastructure works similar to the vehicle to vehicle communication. It's also known as V2X communication as X in the context can be any part of infrastructure. The vehicle to infrastructure makes possible the advance notifications to the system/driver about the potential concern about the possibility of a collision or some other sort of the

problem. The V2I communication comprises of mainly two equipment Vehicle on board unit and Road side unit or RSE.

Online **C**ontrol **A**pproach for **P**ower and **R**ates**(OnCAR):**

The above technique, DSRC have some shortcomings. As traffic during rush hours can create disturbances in the channel 172, that is used by DSRC for communication. This can compromise the driving safety. Moreover, during rush hours network topologies also could be very dynamic and can change faster than normal making the communication difficult due to the questionable reliability on the channel.

In order to optimize the performance of DSRC, we have **On**line **C**ontrol **A**pproach for **P**ower and **R**ates **(OnCAR),** that promises to enhance the overallreliability and efficiency of DSRC by 23.7% and 31%, respectively.[5]

The motivation to this approach is:

i. Real life traffic is dynamic, introducing rapid variations to the network structure/topology and wireless channels.

ii. The DSRC performance, especially the accuracy degrades when there is lack of responsiveness and coordination.

The OnCAR approach takes the effective Packet

Delivery Ratio (ePDR) as the metric of reliability and considers the effective throughput (eTPUT) as the metric of efficiency.

3. BASIC ECOSYSTEM

The typical connected ecosystem contains of different things like sentient vehicle, Road side unit, Trusted authority and sentient components. All these components collectively constitute the system.[2]

Here is a short description of the components that constitute a typical ecosystem:

Sentient car/vehicle: sentient car is an enabled carloaded with sensors, communication and actuators that make it capable of communicating with other vehicles and infrastructure.

Fig 1: s-car [2]

Communication bridges between the sentient car and the other communication channels the duty of the RSUs is to provide near real time image of surroundings for the s-car to make it easier for it to be aware of the surroundings.

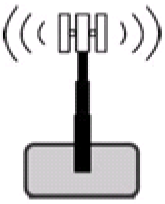

Fig 2. RSU [2]

Trusted Authority (TA): T.A. or Trusted authorityare the roots of certifications for the communication that takes place between the ecosystem let it be the vehicles or the components. The Trusted Authority can be private or public organization.

Fig 3. TA [2]

S-components: s-components or sentinel components arethe components that come under infrastructure like traffic signals and few other components such as a wrist band for human. These components are not in picture as of now. But as this ecosystem will advance lots of components will start to come under this category.

Fig 4. S-components [2]

Environment: Environment constitutes of all other physicalthings that surround this ecosystem.

Fig 4. Environment [2]

Road side unit (RSU): The road side units are the

As any other system, connected vehicles has got its own set of nightmares to deal with. As just before this section we discussed the ecosystem of a typical connected system we will now discuss potential spaces where attacker can attack our connected vehicle system.

The attacks could be global or inter-vehicular However this is the broad classification of the type of attacks :

i. On global communication: The first and most dangerous attack can be global attack that could bring whole system to halt. The attacks can be DDOS or similar attacks compromising the speed of the system making it less responsive and ultimately not working.

ii. On local V2V communication: Other possibility might be attacking the local V2V communication. This attacks are believed to be less destructing as we have RSUs that make the V2V communication a solitary source of information and signals.

iii. On in-vehicle communication: Other possible attack can be on the in-vehicle communication. The in vehicle communication needs to be very efficient and reliable as it will be similar to response to stimuli in human. Any alteration in response time of the in-vehicle communication can lead to serious damages. A focus is made on machines as machines cannot be understood by verbal communication it forms abstractions and concepts[6].

iv. On exposed vehicle software: The communications in the vehicle usually takes place via single or multicore processors but increasing need of other multimedia, it needs to be PC like. Hence have to run an OS on it. The problem with that is it introduces the vulnerabilities inherent in the OS as well. Once anyone compromises the OS, they can very well fake sensor data and provide that in loop to make system behave unexpectedly.

v. On exposed road side unit software: RSU are very critical components in the whole setup as they serve as the interface and communication points for all the V2I communications. They act similar to mobile phone base stations inheriting all the vulnerabilities the former are related to. These vulnerabilities can compromise whole V2I communication and lead to serious consequences.

vi. On sensors and control sensitive data: The sensors are the eyes and ears of the system, as most of the detection and responses are done with the help of sensors. Any change or compromise of the control sensitive data can lead to severe consequences. Though we have no idea right now how this might occur but a skilled and motivated hacker can attack along this threat vector.

vii. On authentication mechanism: The authentication mechanism checks the integrity of the data and signals making it very delicate part of the chain. Trusted Authorities should use secret key access mechanism to avoid the addition of any fake hardware/RSU in the system.

viii. Physical level attacks: Physical level attacks are the attacks directly to the hardware. These attacks can be avoided by making the build of hardware more robust and reliable.

4. CONCLUSIONS

The future is being risen by the new 5G technology for autonomous vehicles with minimum fractional sec. quiescence, high-bandwidth and network slicing capabilities. The advent of 5G presents scarcely credible (in a positive aspect) new gaining window for many stockholders in the automotive ecosystem, from the automakers themselves to new entrants creating innovative services. It truly is an exciting time.

5G also enables automakers and OEMs to greatly speed up innovation. Faster ingression of data and computer work tendency can be shifted while balancing dynamically, what analysis gets done in the car, and what gets done in the cloud. By moving computing significantly closer to the vehicle, 5G and the edge will be able to support roads full of self-driving vehicles, and the data computing needed to provide innovative safety and infotainment services. From the last few years we have noticed many cyber security attacks in all over the world and in almost all sectors like telecom, banking, e-commerce etc with make cyber security as biggest challenges for world [7].

5G is where car connectivity is driving, but automakers need to plan and strategize the best way to reach the goal. In addition to knowing how 5G is becoming the future of autonomous vehicles, automakers will get advantageous information about how.

Although 5G networks are still a work in progressfor mobile operators, the pace of deployment and launches is picking up. By the end of 2019, according to the GSAGlobal mobile Suppliers Association), 61 operators in 34 countries had launched one or more3GPP-compliant 5G services. Of those, 49 operators had launched 5G mobile services, while 34 had launched FWA (Fixed Wireless Access) or home broadband services. Furthermore, the GSA said, 77 operators had deployed 3GPP-compliant technology in their networks and 348 operators in 119 countries were investing in 5G.

REFERENCES

[1] W. G. Najm, J. Koopmann, J. D. Smith, and J. Brewer, "Frequency of target crashes for intellidrive safety systems," DOT HS 811381, 2010.

[2] António Lima, Francisco Rocha, Marcus Völp, and Paulo Esteves-Verissimo - Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems, October 28, 2016

[3] United States Department of Transportation http://www.its.dot.gov/factsheets/dsrc_factsheet.htm

[4] Wikipedia - Article on vehicle to vehicle communication https://en.wikipedia.org/wiki/Vehicle-to-vehicle

[5] Xi Chen, Linghe Kong, Xue Liu, Lei Rao, Fan Bai and Qiao Xiang - How Cars Talk Louder, Clearer and Fairer: Optimizing the Communication Performance of Connected Vehicles via Online Synchronous Control, November 2015.

[6] L. Kharb et al (2019) "Brain Emulation Machine Model for Communication" in International Journal of Scientific & Technology Research (IJSTR). pp 1410-1418.

[7] Shubham. et al. Security for Digital Payments, Int. J. Sci. Res. in Network Security and Communication, Volume-6, Issue-5, October 2018.