INVESTIGATION ON CYBER-ATTACKS AGAINST IN-VEHICLE NETWORK

S.Vishnu Kumar,
Department of ECE,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai-India
mail2jitvishnu@gmail.com

G. Aloy Anuja Mary
Department of ECE,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai-India
aloyanujamary@gmail.com

P. Suresh
Department of ECE,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai-India
suresh3982@yahoo.co.in

R. Uthirasamy
Department of EEE,
KPR Institute of Engineering and Technology,
Coimbatore-India
uthirasamy.r@kpriet.ac.in

2021 7th International Conference on Electrical Energy Systems (ICEES) | 978-1-7281-7612-3/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICEES51510.2021.9383720

Abstract— **The adaptation of modern technologies in vehicles has revolutionized the way we commute both in private and commercial vehicles. The new era of connected vehicle eco-system is likely to improve the ease of driving and to reduce accidents. This is possible only with a complex network connectivity, which has caused a massive rise of cyber-attacks in the past decade. The nature of wired and wireless communication makes connected vehicles vulnerable to cyber threats, a serious security problem for both peoples on-board and on-road. Controlled Area Network (CAN), the de-facto protocol used for in-vehicle communication, suffers from security flaws such as message encryption and sender authentication, which are important to protect the network from cyber-attacks. This paper makes an investigation on different real time cyber-attacks took place in the past ten years to study and understand vulnerabilities that can make a vehicle network fragile. Suggestions are proposed to secure the in-vehicle communication bus and to develop suitable countermeasures. Future forecast has been discussed to highlight the seriousness of the cyber-attack towards vehicle ecosystem.**

Keywords— ***Cyber Security, Cyber Attacks, Connected Vehicles, Cyber-attacks on In-Vehicle Network***

I. INTRODUCTION

In the fast-paced world of urbanization, transportation plays an important role towards increasing the standards and life style, resulting in increased numbers of vehicles on-road. This increased number of vehicles has made some serious alarm towards road safety and environment leading to vehicle manufactures to equip their vehicles with smart technologies to prevent accidents, give post-accident collision warnings [1] and to improve passenger comfort. The adaptation of Advanced Driver Assistance Systems (ADAS), Drive by Wire and Internet Services are growing gradually, making possible to improve the Intelligent Transportation System (ITS) environment[2].

Modern vehicles are equipped with more of automation modules, where the operations of a vehicle is made autonomous and less controlled by a driver. While the drivers' safety is paramount in all aspects, a computer failure can lead to a turmoil. All the sub-modules of transmission system, steering systems, and electrical systems are controlled through Electronic Control Unit (ECUs), which in-turn are connected together through a common bus called CAN that empowers ECUs to work at high speeds.

The connected vehicle has multiple channels to get connected, like Wi-Fi, Bluetooth, Universal Serial Bus (USB) tethering etc. They also have a 16-pin port called On-Board Diagnostic (OBD) port which provides an additional connectivity channel. The OBD port provides open access to a vehicle's in-vehicle network bus; CAN bus. Through which an adversary can manipulate a CAN data packet, as the bus protocol doesn't have any security ascept. The research results by Carnegie Mellon's Computer Emergency Response Team (CERT) Coordination Centre showed significant gaps in connected vehicles. [3]

Thus, anytime a cyber-attack is possible on in-vehicle network of a connected vehicle. There are various studies and research focused to build an extremely secure system that is resilient to these kinds of attacks. This paper tries to document the various real time attacks that occurred previously, thus the readers of this paper will be educated to formulate new algorithms and protocols to defend the connected vehicles from future attacks.

In section II, the past attacks that took place are discussed with respect to attacks on vehicle and vehicle used for attacks over infrastructure. The importance of the vehicle network security and the adverse impact they could bring in the event of compromised network are discussed in section III. The research forecast is discussed in section IV. The authors suggestions and conclusions are recited in Section V and VI respectively.

II. LITERATURE SURVEY

The point of using embedded electronics in automobiles began with the introduction of United States' Clean Air Act in 1990, that forced manufactures to install on-board diagnostics to monitor exhaust air quality[4]. Today, electronics is at the core of the modern vehicles and with the power of technology, a lot of information about the vehicle and the people are tracked and processed automatically. Many new features are included into the vehicle to make ease of driving. However, all these features come at a price of security and privacy breach.

According to Gartner Incorporation; a well known research firm, Internet of Things will have a greater impact in the worldwide vehicle industry, such that by the end of 2020 we can observe, some form of wireless connectivity in 1/5th of vehicles on-road[5].

In an article released by Morris Garage; an automotive company based in India, the appeal for connected vehicles is projected to have an exponential growth with a market value of $3 Billion USD by 2020 in India[6]. Thus, as the market for connected vehicles grow, the cyber attacks over them is also expected to grow.

The cyber-attacks are increasing because of the consumer's need for convenience. The market competition forces manufacture to deploy vehicles without proper real-time testing; leading to security loopholes in vehicle. With every new technology being added some risks get added[7]. To understand cyber-attacks in details, the attacks happened year wise so far are descripted below.

A. Stolen Password-2010

Texas Auto Center, a car dealership based in Austin; started to receive complaints from vehicle owners, stating the vehicles they purchased suddenly started to horn or the engines won't start when ignition key is pressed. Initially the dealership considered it to be a mechanical fault, only later to know it was an act of their own disgruntled employee, Omar Ramos-Lopez who was laid-off. The dealership used a web-based application and an On-board device to collect their dues as an alternate to repossess the vehicle, called WebTech Plus. The hardware device is directly wired with engine immobilizer and horn unit. Even though the system doesn't affect a running vehicle, but followed the commands it received from a webpage to disable car's ignition system or starts honking as a remainder to pay the dues when the vehicle is parked. If payment is late the device activates the engine immobilizer, rendering the vehicle useless. Any employee of dealership had rights to disable the vehicle at any time needed. Even though intruder's credentials were disabled, he allegedly got in through another employee's account and pulled out the entire customers details, which helped him to deactivate the cars or set-out the horns[8]. This incident gives an insight as how a connected vehicle environment can be potentially exploited by someone with invasive intent.

B. Wired Experimental Analysis-2010

Cyber security investigators from University of Washington and University of California formed a joint venture; Center for Automotive Embedded Systems Security (CAESS), to investigate security issues in vehicles. In the year 2010, they published their findings entitled "Experimental Security Analysis of a Modern Automobile"[9]. The results published were based on the number of lab and road test conducted to inject malicious packets into vehicles CAN bus, to manipulate a vehicle's functions. The research demonstrated that if an attack occurs, the intruder has the ability to disable vehicle's brakes, immobilise the engine and fabricate speedometer details. During the time of demonstration, the researchers used wired technology to hack and were criticized by vehicle manufactures, stating it's impossible for an intruder to get wired access to a moving car. This demonstration highlighted the potential risk involved in a vehicle using electronics for controlling its functions.

C. CAESS Experimental Analysis-2011

In the year 2011, the CAESS team acknowledged that, it's possible for an intruder to gain access into a vehicle through available ports. They listed out all possible channels through which an intruder can get access to, in-vehicle communication network namely; Vehicle to Vehicle Communication port, OBD port, Infotainment port, and Telematics units such as Wi-Fi, Bluetooth, and Cellular.

D. The Physical Hack -2013

In 2013, Defence Advanced Research Projects Agency (DARPA) granted 80,000 USD grant to two white-hat security researchers Miller and Valasek. They demonstrated how a vehicle's OBD port; used for vehicle diagnostic, can be used to control the vehicle. They both showed a series of real-time demonstration to both media and network security professionals. The works of Miller and Valasek were published in Def Con conference. It was revealed, they used a custom-built communication cable, which was used to connect their laptop via USB to the OBD-II port of the targeted vehicles; 2010 Ford Escape and 2010 Toyota Prius. They observed the data packets generated by different sub-modules, which were communicated through CAN bus and the actions other sub-systems took as response. Later they reverse engineered to inject malicious packets to re-generate those actions like, jamming the steering wheel, bang the brakes. The main moto of this demonstration was to show what an adversary is capable of, once he gets access to a vehicle's CAN network.

E. Zero-Day Exploit-2015

In 2015, the researchers Miller and Valasek once again came up in headlines, but this time for hacking an unaltered passenger vehicle; a 2014 Jeep Cherokee. This event imitated a real-world problem

in which they were able to demonstrate both gaining remote access and ability to execute programming scripts. They created a software that sends command to the vehicle, through infotainment system. Once the file is opened, they were able to take control of vehicle. Miller and Valasek showcased what they can achieve once they got access to a vehicle like changing the air conditioning to its extreme cold level, turn the music system to full volume, and switch on wiper fluid. They also demonstrated controlling the throttle and disengage the transmission system. It was an example of the risk the network connection had between vehicles CAN bus and an infotainment system[10]. Later it was revealed by the researchers that the loophole was in Uconnect; a connected environment platform found in Chrysler, Dodge, Jeep, Ram and FIAT brand vehicles. The researchers also demonstrated the weakness in the cellular network that can be exploited by attackers; in this case the Sprint's Cellular Network, to which the vehicle Telematics units are connected. They highlighted any vehicles with Uconnect had an internal communication bus called D-Bus and in normal state not accessible for the users. But given anytime, if a device is connected to Sprint's 3G network, the device was able to communicate with D-Bus of any vehicle. This demonstration made Fiat Chrysler to recall all units with Uconnect to update with a patch, a costlier decision. [11]

F. Tesla Model S Hacked-2016

In 2016, a team of engineers; Samuel LV, Sen Nie, Ling Liu and Wen Lu from a Chinese research firm Keen Security Lab, demonstrated hacking into Tesla Model-S. The attacker was able to target the vehicle as far as 12 miles away from. It is to note that the researchers used unaltered Tesla Model S P85, the car with latest firmware at the time. The attack requires the vehicle is connected to Wi-Fi created by the attacker. Also, it requires Tesla's web-browser being used. The researchers used the weakness of the web-browser to get access to CAN network. This showed the weakness a web-browser based Application Programming Interface(API)s had over the functionalities of the vehicles[12]. The researchers showcased what can be done once a car is hijacked both in driving and parking mode; like automatic seat adjustment, activating windshield wipers, trigger the direction indicators, opening closing side mirrors, opening and closing of sunroof and boot. This was the first reported case with respect to successful attack on a Tesla model, still the company acted quickly to give an update patch over the air[13].

G. Cyber-attack using Mobile Phone-2016

Vehicle users like to have functions like doors unlocking, head lights on/off, trunk opening/closing to be controlled remotely. Now a days users started to enjoy keyless entry also. These limited functionalities bring risk along with the comfort. One way to avail these functions is to use dedicated mobile application running on the users' phone. This mobile application connects to a hidden network of the vehicle, to perform the required operations. Manufactures create such application using a software intermediary called API which communicates between mobile application and the software running in the vehicle. In 2016, Promon, a Norwegian security firm influenced a Tesla owner into downloading a malicious mobile application. It manipulated the Tesla's mobile application APIs, enabling the attackers to communicate with Tesla's server. They used this connection to issue remote commands to the vehicle[14].

H. Crowbars to Amplifiers -2017

The modern cars have started to roll-out a sophisticated system called keyless entry. A system which requires a wireless key fob to be in a range for the vehicle to open the doors or start the ignition. When the same key fob is kept in a distance; probably when the vehicle is parked. An attacker can reduce the distance between the key and the vehicle using an amplifier circuit, thus leading to opening of the car doors.[15]

I. Misconfigured Server-2017

A misconfigured cloud service could lead to a disaster. In 2017 a group of researchers from MacKeeper security centre, found a misconfigured Amazon Web Service (AWS) S3 Bucket, a publicly accessible cloud storage system. The SVR tracking company was using one of the AWS bucket services for their fleet tracking activities. It had information of more than half a million users which include drivers, owners and the companies using tracking services, without any protection. The details included logins and passwords, emails, International Mobile Equipment Identity (IMEI) numbers of Global Positing System (GPS) devices and Vehicle Identification Number (VIN). Fascinatingly details related to where exactly the tracking devices are fixed in the vehicle were also recorded. Since the tracking company tracks and updates the location details every two minutes, anyone with the login credentials can exactly pinpoint the location of a particular vehicle. This could be a serious threat as anyone with access to internet can track a vehicle and steal them just with publicly available credentials [16].

J. Vulnerabilities in The Onboard Units-2018

Researches from Keen Security Lab, over a yearlong audit found fourteen vulnerabilities in BMW cars. They focused their research towards three critical units of a vehicle namely Infotainment System, Central Gateway unit and Telematics unit. Out of fourteen faults, eight flaws impacted connected infotainment system, four flaws affected Telematics control unit and two flaws affected the Gateway unit. An attacker can send arbitrary

messages to the targeted vehicle's Engine Control Unit (ECU) exploiting these weaknesses. This would eventually allow troublemakers to take control over the functions of the affected vehicle. Four flaws required USB connections to take place, meaning a physical presence was required. Another four required indirect physical access to the car, while six flaws could be remotely exploited using Telematic devices[17].

K. Vulnerabilities in Lexus Vehicles-2020

Lexus, a well-known car model from car manufacturer Toyota. It is equipped with a new infotainment system since 2017, which had the capability to communicate with Internet. Researchers from Keen Security Lab discovered several security flaws with Bluetooth and vehicular diagnosis functions of the car. Through these flaws they were able to access infotainment system, through which they were able to inject malicious packets into CAN bus. This, resulted in serious physical actions[18].

Thus, having a deep understanding of previous attacks over the vehicle networks orchestrated will help in identifying the different threats a vehicle network has to face. This aids in developing new algorithms and protocols to defend the vehicle networks from future attacks.

III. The Fundamental Cyber Risks of Connected Cars

A modern vehicle can be termed as a computer on wheels, thus all security issue a computer faces can be expected in a vehicle. From the literature survey conducted we can understand cyber attacks in vehicle ecosystem can be categorized as active and passive attacks.

A. Passive Attacks

In passive attack, there is no physical contact required, it is very difficult to understand even if an attack occurred. Eavesdropping and traffic monitoring can be attributed as examples of passive attacks.

1) *Man-in-the-Middle Attack:* In this type of attack the attacker eavesdrop to communication between vehicle and infrastructure or vehicle to vehicle. This conversation which might include private conversation could be monitored by the adversary. Which may lead to information leak or misused against the driver or vehicle.

2) *Using Live Traffic Status:* Attackers could use road traffic analysis system to obtain the length and time of the messages trans-received between a vehicle and road-traffic server. With this detail they could gather information such as, the time the vehicle is used and the routine path the vehicle takes, which time a vehicle will be at a particular location. This is a serious data breach, which has to be addressed immediately.

B. Active Attack

From the previous case studies and a vast literature survey conducted, in general active attacks over connects vehicle can be categorized as Attacks targeting Vehicles and Attacks using Connected Vehicle.

1) Vehicle as Target

Attacks targeting a Vehicle can be classified as the cyber-attacks that focuses on one or more connected vehicles to snip privacy details or to create a destruction. They can further be classified as

- Attacks on Connected Units
- Attacks on Fleet of Vehicles
- Remote Hijacking

a) Attacks on Connected Units: Today's vehicle has more electronics than mechanical parts in a vehicle. These electronic equipment are controlled through ECU. Each ECU is responsible for one sub-task in a vehicle and are interconnected through a common bus called CAN Bus. The intruder could get access to this CAN bus through wired medium like OBD port USB port; wireless channel like Global System for Mobile Communications (GSM), Wi-Fi; and through APIs like Short Message Service (SMS) APIs, Web-interface APIs and Mobile APIs. Once the intruder gets access to these channels, they can make a targeted attack over connect units like the engine system, powertrain system, transmission system, safety system and brakes system. Connect vehicles are prone to security threads, once the manufacturer finds this, they release a patch update using Over-the-Air (OTA). They have equal benefits and security concern. Until the source of the updates is verified, they represent threats and risks.

b) Attacks on Fleet of Vehicles: Attacks on individual vehicles are gone, now attacks over an entire fleet of vehicle is the current trend. In a fleet operation, the dealership monitors the vehicles, through collecting different parameters; which are collected both from internal and external environment using different sensors. These sensors are interconnected through the same CAN bus to which vehicle's different ECU are connected; as ECUs also need to take actions based on these sensor values. Ransomware is a type of malware from crypto-virology that threatens to perpetually block access, unless a ransom is paid. Attacks on fleets of vehicle for a ransomware is an external attack carried over using the connected platform. The attackers plug an end-device to the connected platform to gain access to CAN bus, which would enable them to obtain access to the vehicle's internal systems to inject false sensors

values and force the vehicle into taking unwanted actions. The attacker would demand a ransom to release the system.

c) Remote Hijacking: Use of modern technologies to take automatic decision making is getting increased day-by-day and the controllers or processors embedded in the vehicles for the same differ company to company. Mostly importantly they differ between Original Equipment Manufacturer (OEMs) and supplier to OEM's. Thus, they form a strong weakness point to get explored. One example is manipulating a GPS device to falsify the destination co-ordinates, leading the vehicle to deviate from the original travel path. Backdoor attacks relating to vehicle can happen due to malicious firmware upgrades. For example, a weakness in the firmware can lead criminals and terrorists to use a vehicles dash camera to get a real time visuals of the place they are parked. If the vehicles are equipped with a Light Detection and Ranging (LIDAR) system, it can give a better high-resolution insights into the surroundings as well.

2) *Vehicles as Source*

Connected vehicles are computer in wheels with less computational power. A connected environment gets completed when an enterprises level infrastructure gets connected. Thus, connected vehicles can be used in reverse to access the infrastructures itself. The attacks of these type can be further classified as

- Attacks on Cloud Infrastructure
- DDoS

a) Attacks on Cloud Infrastructure: In a connect eco-system the cloud plays a vital role for a faster computation and decision making and handling a huge chunk of data. It's a repository of users data. It is also a central hub of communication to a pool of other connected vehicles. If one vehicle can be compromised it can open the gateway to this cloud infrastructure. Cyber-attacks over cloud services has the potential to target a mass at same time. Leakage of user data can be a serious privacy concern.

b) Distributed Denial-of-Service Attack: In Internet of Things era the connected vehicles are the end device in a network and has a huge potential to become a botnet. A botnet is a combination of two words "robot" and "network". In botnet attack the hacker requires a physical computational powered entity and as vehicles are a part of connected network and has a limited computational power, they can be hacked to be a botnet. Generating a large amount of request and deny resource for the other users, an attack termed as distributed denial-of-service attack (DDoS). They can also send remote commands to control other connected vehicles at the same time to control them remotely.

IV. Research Forecast.

The best way to deal with attacks is to have a vision; the visualization of attacks and the magnitude of damage they will create. The research data from the year 2010 to 2018 were sourced from Upstream Securities[19] to get an insight into the future related to attacks on connected vehicles.

A. Channels Used for attack

From the findings of survey conducted by Upstream Security, different channels used by the hackers to tamper the connected vehicles is compared and plotted. The study was to assess the type of attacks occurred at different times, using different mediums like cloud infrastructure, OBD ports, mobile applications etc. Rating the highest to lowest ordered medium based on number of times the medium being used to exploit the vehicle network system. The findings are figured in Fig. 1. An exponential projection study suggests that the trend is to grow in similar rate whereas moving average study suggests a change in trend; the attacks using infotainment and mobile applications are to increase. This gives an insight as, which are the devices we have to secure in future.

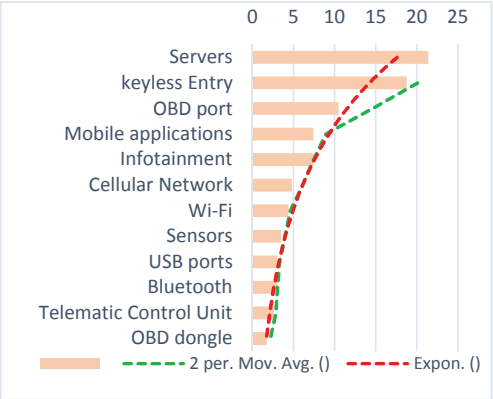

Fig. 1. Comparison between different channels used for hacking.

B. Remote vs Physical Attack Model

From the survey report submitted by Upstream Security, it is evident that the nature of attacks has changed trends over the year of evolution. Tracking from first event; stolen password[8] to hooking a Windows-XP machine to the vehicle's OBD port[9] to the recent remote controlling of Toyota Lexus[18] using connected infotainment system has given an understanding related to the evolution of hacking practices the adversary are following. A moving average study projects as in Fig.2, that the trend will continue, as a result we can expect to have more wireless hacks compared to any physical hacks in future.

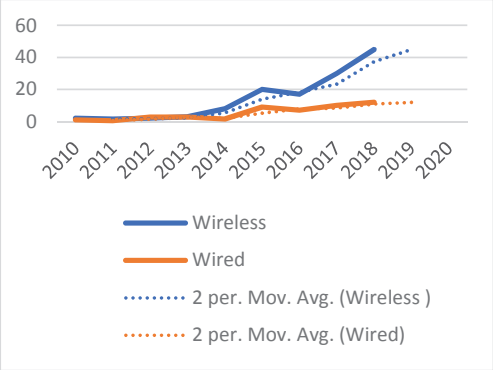

Fig. 2. Comparison between Wired and wireless attack over connected vehicle.

C. *Long Range versus Short Range*

Understanding the types of attacks is essential for protecting the eco-system, the distance from which the attack is launched is one way of difference we can see from the literature survey conducted. Thus, we can categorise the attack based on the distance as short-range and long-range attacks. Short range attacks uses mediums like Wi-Fi, Bluetooth and key-fob signals etc… The attacks carried out using Internet and cellular network accounts for long range distance attack. The comparison between long-range and short-range gives an overview as receipted in Fig. 3. Also, an exponential growth forecast, suggests the number of long-range attacks are to grow more compared to short range attacks in future.

Fig. 3. Comparison between Long-Range versus Short-Range attack over connected vehicles

D. *Top impacts of Cyber-attacks on automotive*

This study shows the effect of car hacks. The most important impact is the control over whole vehicle. At present the effect of hacking that controls actual components of the vehicle accounts as such 27.62% of occurrences. The trend projected using moving average states, that the trend is to stay, which forecasts, more incidents related to remote controlling of whole vehicle is to be expected in future as descripted in Fig.4.

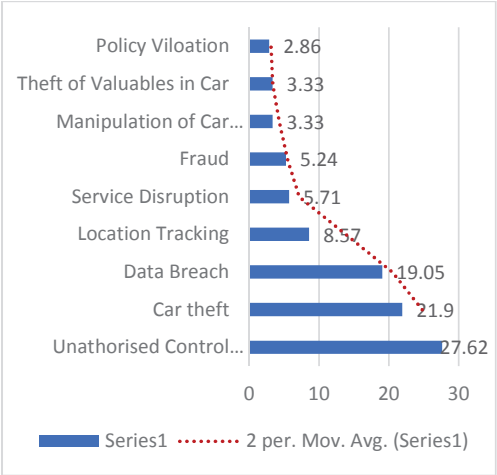

Fig. 4. Top impacts of Cyber-attacks on automotive eco

V. Suggested Solutions

From the survey conducted it is evident that, through different channels like Telematic units, Infotainment systems, weakly designed mobile application, insecurely configured cloud service, paves way for attacks. Securing these channels and infrastructure is one possible way to avoid future attacks. Edge device encoding, adding cryptographic verification in internode transport is another resistance against cyber-attacks. Creating, handling and updating cryptographic keys over a vast network is a complex effort but if implemented will help in reducing the rate of attack.

A. *Redundancy*

In cyber security, redundancy is the idea of connecting critical sub-system to more than one sub-system and thus eliminating single point of failure. It is a costly arrangement, given the extra weight and cost of the additional parts. In the event that one framework is seized by an intruder, different frameworks are still able to support the function the seized system was responsible for.

B. *Digital and Analog Co-design*

Introducing some fundamental analog control in an ever-advancing digital environment is another security arrangement. One role might be supported, for instance, by three repetitive electronic control frameworks and a mechanical one. This non-hackable, last-recuperation approach is starting to be presented in vehicles for safety-critical frameworks.

C. *Anomaly-based intrusion detection*

As in power distribution network system, a framework to find abnormal data patterns, can be used to monitor the data trans-received over the communication channel. This anomaly detection system if implement for safety critical sub-systems of a vehicle; will be able to predict the abnormal

activities of a unit and prevent it from further commanding other ECUs.

D. Air-Gap

As in aviation industry, separating the traveler's entertainment framework from the remaining systems of the flight is measured as a key element of a secured architecture in aviation. Adapting the same in automotive ecosystem can benefit by safeguarding the safety critical sub-systems of a vehicle.

VI. Conclusion

From the literature survey conducted it can be concluded that manufactures and researchers need to work together to defend against the cyber-attacks and no car models are 100% safe. The network and devices must be secured from both internal and external threats. Periodic vulnerabilities check in different levels of interface must be analyzed and any risk found must be fixed.

Three key characteristics to overcome a cyber-attack are; keep-updating, positive attitude and skilled administration. Using some standard security practices and getting updated with latest attacks will help the research team to come up with a solution in short. Getting help from white hackers to identify the loopholes will assist in developing a patch and the network could be saved in advance from a security breach. No security protocols are tamper proof and the discussed events have witnessed the same, thus in the event of an adverse situation occurred the respective manufactures have to address the issue in fast and well-defined manner.

Firmware must be kept updated periodically. While updating the firmware using patches from manufacturer, verifying the source before updating could be an added advantage. Isolation of in-vehicle bus and safety critical system from external network can be considered as one solution using intrusion detection systems. Incorporating Artificial Intelligence algorithms to monitor the network for abnormal data traffics can result in better attack defending system.

Reference

[1] S. Mathi, E. Joseph, S. Dharini, V. Mohan Karthik, and S. Harishkiran, "Design and Implementation of Message Communication to Control Traffic Flow in Vehicular Networks," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1, pp. 848–853, Oct. 2019.

[2] E. H. Dwi Shakti M, "Performance Analysis of Ad-Hoc Routing Protocol for Vehicular Ad-Hoc Network (VANET)," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1, pp. 1098–1104, Oct. 2019.

[3] "Vulnerability Analysis at the CERT/CC.", [Online]. Available: https://insights.sei.cmu.edu/cert/2008/04/vulnerability-analysis-at-the-certcc.html. [Accessed: 28-Nov-2019].

[4] "Clean Air Act (United States) - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Clean_Air_Act_(United_States). [Accessed: 28-Nov-2019].

[5] "Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities." [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2015-01-26-gartner-says-by-2020-a-quarter-billion-connected-vehicles-will-enable-new-in-vehicle-services-and-automated-driving-capabilities. [Accessed: 28-Nov-2019].

[6] "MG Motor partners with Cisco and Unlimit for connected mobility." [Online]. Available: https://www.mgmotor.co.in/media-center/newsroom/mg-motor-india-partners-with-cisco-and-unlimit-for-connected-mobility. [Accessed: 28-Nov-2019].

[7] "Automotive companies and cyber attacks: PwC." [Online]. Available: https://www.pwc.com/us/en/industries/industrial-products/library/automotive-cyber-readiness.html. [Accessed: 28-Nov-2019].

[8] "Hacker Disables More Than 100 Cars Remotely | WIRED." [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/. [Accessed: 24-Nov-2020].

[9] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," *Proc. - IEEE Symp. Secur. Priv.*, pp. 447–462, 2010.

[10] "Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED." [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 29-Nov-2019].

[11] "Fiat-Chrysler Software Recall: What You Need to Know - CarsDirect." [Online]. Available: https://www.carsdirect.com/automotive-news/fiat-chrysler-software-recall-what-you-need-to-know. [Accessed: 24-Nov-2020].

[12] "Car Hacking Research: Remote Attack Tesla Motors | Keen Security Lab Blog." [Online]. Available: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/. [Accessed: 24-Nov-2020].

[13] "Team of hackers take remote control of Tesla Model S from 12 miles away | Technology | The Guardian." [Online]. Available: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes. [Accessed: 29-Nov-2019].

[14] "Tesla-Stealing Hack is about Much More than Tesla | Fortune." [Online]. Available: https://fortune.com/2016/11/26/tesla-stealing-hack/. [Accessed: 30-Nov-2019].

[15] "Car hacking: Thieves armed with laptops are stealing cars | CSO Online." [Online]. Available: https://www.csoonline.com/article/3092871/car-hacking-thieves-armed-with-laptops-are-stealing-cars.html. [Accessed: 24-Nov-2020].

[16] "Auto Tracking Company Leaks Thousands of Records Online." [Online]. Available: https://mackeeper.com/blog/post/auto-tracking-company-leaks-hundreds-of-thousands-of-records-online/. [Accessed: 24-Nov-2020].

[17] "Experimental Security Assessment of BMW Cars: A Summary Report."

[18] "Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars | Keen Security Lab Blog." [Online]. Available: https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/. [Accessed: 24-Nov-2020].

[19] Upstream Security, "Global Automotive Cybersecurity Report 2019," p. 28, 2018.