A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs)

Mubashir Masood
Department of Electronic Engineering
University of Engineering and Technology (UET)
Taxila, Pakistan
mubashir.masod@students.uettaxila.edu.pk

Zubair Saeed
Department of Computer Engineering
University of Engineering and Technology (UET)
Taxila, Pakistan
zubair.saeed@students.uettaxila.edu.pk

Misha Urooj Khan
Department of Electronics Engineering
University of Engineering and Technology (UET)
Taxila, Pakistan
mishauroojkhan@gmail.com

Abstract— Connected and Autonomous Vehicles (CAVs) are a crucial breakthrough in the automotive industry and a magnificent step toward a safe, secure, and intelligent transportation system (ITS). CAVs offer tremendous benefits to our society and environment, such as mitigation of traffic accidents, reduction in traffic congestion, fewer emissions of harmful gases, etc. However, emerging automotive technology also has some serious safety concerns. One of them is cyber security. Conventional vehicles are less prone to cyber-attacks, but CAVs are more susceptible to such events as they communicate with the surrounding infrastructure and other vehicles. To gather data for a better perception of their surroundings, CAVs are outfitted with state-of-the-art sensors and modules like LiDAR, GPS, RADAR, onboard computers, cameras, etc. Hackers, terrorist organizations, and vandals can manipulate this sensor data or may access the primary control by cyber-attack, which may result in enormous fatalities. The automotive industry must put up a rigid framework against cyber invasions to make CAVs a more reliable and secure means of transportation. This paper provides an overview of cybersecurity challenges in CAVs at the module and software levels. The sources of active and passive threats are analyzed. Finally, a feasible solution is recommended to cope with such threats.

Keywords— Automotive security, connected vehicles, cyber security, V2X communication, Denial-of-Service (DoS) attacks

I. INTRODUCTION

Over the past few decades, technological advancements have been made to make travel more luxurious, pollution-free, reliable, and safe. The Cruise Control system, Advanced Driver Assistance System, Lane Departure Warning (LDW) system, and Anti-lock Braking system are some examples of these developments. Such technological advancements have transformed the automobile sector. Connected and Autonomous Vehicles (CAV), or Driverless Cars, are a new and emerging technology for the intelligent transportation system (ITS). An autonomous vehicle is a vehicle that perceives its surroundings through different sensors and drives safely without human intervention [1]. CAVs offer numerous benefits to our society, e.g., reduction in road crashes; mitigation of traffic congestion; the downgrading of CO2 emissions due to electric vehicles; etc. According to the World Health Organization (WHO), approximately 1.35 million people die in road crashes annually. The National Highway Traffic Safety Administration (NHTSA) investigated that 94% of accidents occur due to human errors [2]. Thus, CAVs are the most feasible solution to mitigate these casualties. The paramount force behind the development of autonomous vehicles (AV) is the safe, secure, and reliable transportation system. Technological giants like Google, Apple, and famous automobile companies such as Tesla, Ford, and General Motors are huge investors in the research and development of AVs [3]. Some automobile companies have already incorporated some features of driver assistance systems such as the Lane Departure Warning (LDW) system, Adaptive Cruise Control (ACC), Auto-Parking, etc. These features show the autonomy level of AV. The Society of Automotive Engineers (SAE) ranks the vehicle from Level 0 to Level 5 [4] as depicted in *Figure 1*, where Level 0 indicates no automation and Level 5 shows full automation. The US Department of Transportation (DOT) utilizes this SAE classification to evaluate the vehicle's autonomy level. Companies are doing their best to achieve a higher level of autonomy, and road testing is being carried out in limited circumstances. Numerous hi-tech companies, automobile manufacturers, and ride-hailing services (Uber) are gearing up their efforts to unleash fully autonomous vehicles on the roads by 2021. Big automakers depend on partnerships with chipmakers (Nvidia, Intel, etc.) and telecom giants to develop AVs. For instance, Ford partnered with Verizon to introduce 4G connectivity in their automobiles. Due to such joint ventures, investment in the connected car market has increased. *Figure 2* shows the investment from the private sector in the automobile field. Although autonomous vehicles offer a lot of benefits to our lives and society, they are also eminently vulnerable to security threats. CAVs are not isolated vehicles; they share information with other vehicles (V2V communication) and with infrastructure (V2I communication). Different computational units, i.e., LIDAR, GPS, and Inertial Measurement Unit (IMU), are embedded in AVs which control the different parameters of the vehicle. These units are primarily embedded systems that are highly prone to cybersecurity attacks [5]. In 2015, two researchers from the USA wirelessly hacked the Jeep Cherokee and disrupted its multimedia system and accelerator [6]. This incident shows serious threats to autonomous vehicles. This paper highlights the vulnerabilities of cyber-attacks to inter-vehicle (inside the vehicle) and intra-vehicle (with infrastructure and other vehicles) communication. This paper aims to review the major sources of cyber-security threats and propose feasible solutions.

II. RELATED WORK

Cybersecurity analysis Cybersecurity analysis is a well-researched and hot topic in the modern automotive industry. Conventional vehicles can be considered closed systems as they do not communicate with their surroundings. So, their core security concepts are limited to protecting against unauthorized access to vehicle anti-theft systems (immobilizers) and keyless locking systems.

How to cite: Masood, M., Saeed, Z., & Khan, M. U. (2023). A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs). *JAREE (Journal on Advanced Research in Electrical Engineering), 7(1).*

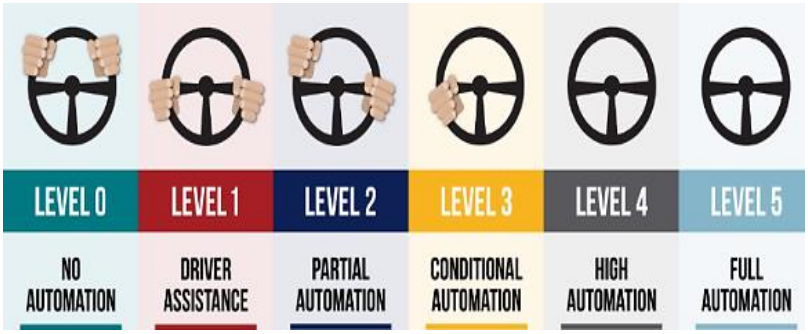

Fig. 1. Five levels of vehicle autonomy [6].

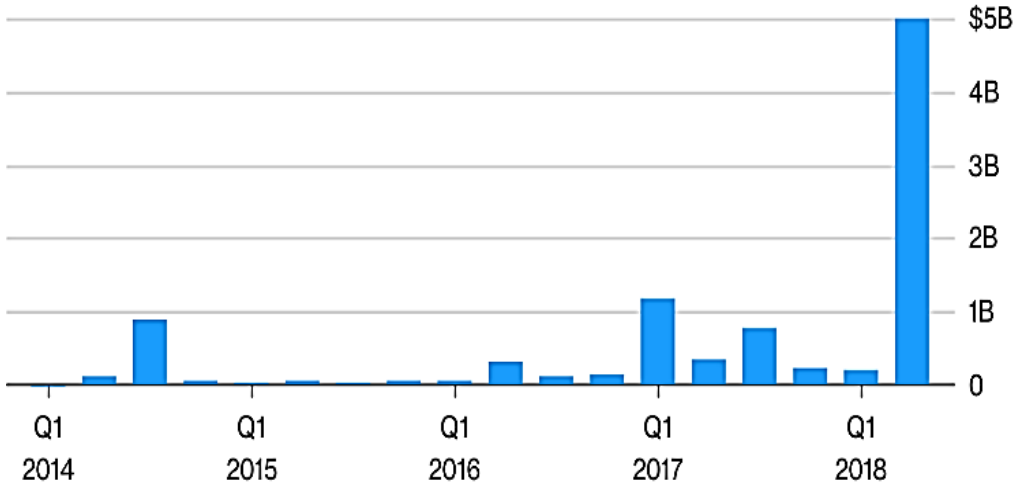

Fig. 2. Private investment in AVs startups [7].

Possible attack scenarios on such a system have been discussed in various publications [7-10]. A comprehensive literature review related to autonomous vehicle technology and cybersecurity threats is provided in this section. A report titled "Securing the Connected Car: A Study of Automotive Industry Cybersecurity Practices" published by Ponemon Institute, based on 593 surveys from automotive professionals, reveals that connected cars will have substantial safety features, i.e., airbags, seatbelts, and anti-lock braking, but not enough cybersecurity countermeasures.

Knowledge gap 1: *In case of a CAV accident, it is imperative to forensically analyze the vehicle's onboard system to find out what happened. This might be helpful to prosecute criminals. Currently, no literature is available to deal with how vehicle software might be developed that can provide a legal basis for criminal prosecution.*

Safety and security are indispensable features of a modern vehicular system. Although fully autonomous vehicles (Level-5) have not hit the road yet, However, extensive efforts are being made by all stakeholders. Hardware capabilities such as GPU/CPU computational power, resolution and Field of View (FOV) of cameras, LiDAR range, and other vital requirements have met the criteria for a fully autonomous functional vehicle. The major impediment is the development of CAV software, which manages all the crucial functions of the vehicle. The complexity of such software has now increased exponentially as a large number of critical tasks are being controlled by the software rather than hardware. Connected and Autonomous Vehicles (CAVs) gather data through various sensors mounted on the vehicles and share this valuable information with other vehicles for a greater and safer driving experience. These sensors are attached to the central control unit known as the Electronic Control Unit (ECU) via wired (i.e. CAN bus, Flexray, etc.) or wireless link (i.e. Bluetooth, Zigbee, Radio frequency identification (RFID), etc.). In [7], Lu et al. presented different wireless and wired connectivity methods to connect onboard sensors to the ECU. However, the authors did not consider the security issues related to these methods. Another survey conducted by He et al. [8] suggests the isolation of CAVs from the environment. The authors addressed only intra-vehicle communication. CAVs cannot be isolated from external infrastructure and vehicles. Because shared information among all the vehicles on the road will improve safety and reliability. CAVs are equipped with onboard sensors and modules, which are the targets of interest for many attackers. Hackers may alter the output of these sensors or maybe get full control over ECUs via these modules. In [9], the authors described the possible target of interest to hackers. Cameras, GPS, and LiDAR are the prime targets of hackers. For example, a wrong traffic sign shown by the attackers can input a false image to the camera, or hackers can modify the route of an autonomous vehicle by attacking GPS, which will ultimately result in destruction and violation [10]. In [11], Parkinson et al. categorized the vehicle components as vehicle and control units and discussed the possible attack scenarios for each. The authors elaborated on the GPS spoofing concept with illustrations. Similarly, they

showed an attack on the Inertial Measurement Unit (IMU), LiDAR, vehicle vision system, and network protocol attacks. They also illustrated vehicle-to-everything communication (V2X). In [12], Jawhar et al. described the network architecture and numerous ongoing projects related to Inter-Vehicular Communication (IVC) systems, i.e., FleetNet, CarTalk 2000, and INVENT. They divided the network architecture of CAVs into three categories: Wireless LAN architecture, which is a purely cellular network, Infrastructure-less architecture, which is an ad hoc network; and a hybrid architecture, which has the features of both WLAN and ad hoc networks.

The authors concluded the benefits offered by the Inter-Vehicular Communication (IVC) system and provided the future work direction. Literature [13] provides an overview of threats to various discrete systems, i.e., vehicles, infrastructure, ecosystems, surroundings, etc., and highlights the numerous initiatives taken by the Government Accountability Office (GAO). In [14-17], Hodge et al. elaborated on inter-vehicle communication. The author divides the surroundings of the vehicle into three categories: (a) In-vehicle category in which the author briefly describes the protocols used among different parts of the vehicle, like the Controller Area Network (CAN), FlexRay, and Local Interconnect Network (LIN). (b)The vehicle's second communication network category connects the vehicle with the back-end system. (c) The back-end system category consists of servers, and it is controlled by the service provider. The author concluded that the first and second categories are more vulnerable to nefarious hackers and vandals.

III. Environment Surrounding Connected Vehicle

This section describes the environment around connected vehicles and discusses the associated systems and protocols. Modern connected cars comprise tens of hundreds of well-connected ECUs (primarily via CAN buses) which run millions of lines of code to control the different automotive features, i.e., steering control, airbags, brakes, and engine control.

Knowledge gap 2: *Based on gathered data through various sensors, ECUs control the vehicle's decisions. In false conditions (i.e., poor or corrupted sensor data), the ECU may initiate emergency brakes. Very little literature is available related to mitigation strategies in such a scenario.*

ECUs and Controller Area Networks (CAN) manage an unsecured inter-vehicular network. To enable potential safety and reliability, CAVs communicate with other vehicles through Vehicle Ad Hoc Networks (VANET) or with infrastructure via 5G or Dedicated Short Range Communication (DSRC), which exposes the CAN and ECUs as more vulnerable to cybersecurity attacks. Furthermore, the infotainment system, navigation system, or even the Tire Pressure Monitoring System (TPMS) could be an entry point for attackers [17,18]. Figure 3 depicts the surroundings of connected vehicles.

A. In-vehicle Category

The in-vehicle network, which comprises a CAN bus with a large number of ECUs, significantly reduces the design issues of connected vehicles. It also helps to connect the vehicle with the outside world and rich interfaces, including a telematics system and an On-Board Diagnostic (OBD) port. For instance, vehicle performance can be improved by reprogramming the vehicle's firmware using the OBD port. Figure 4 depicts the ECUs communicating with each other through the CAN bus. Concisely, the embedding of connectivity features in CAV is much the same as exposing them to the outside world. Communication between vehicles and the outside world has become a trend in modern automobiles as it offers a lot of benefits, but adversaries can use this channel to take control of the vehicles. Attackers can access the ECU, which controls the functionality of the car from every aspect, with dire consequences [18]. In this category, we described the standard intra-vehicle network architecture along with existing protocols (Flexray, CAN, and LIN). Furthermore, vehicle sensors (LIDAR, RADAR, and visual sensors) are discussed from a cybersecurity perspective [19].

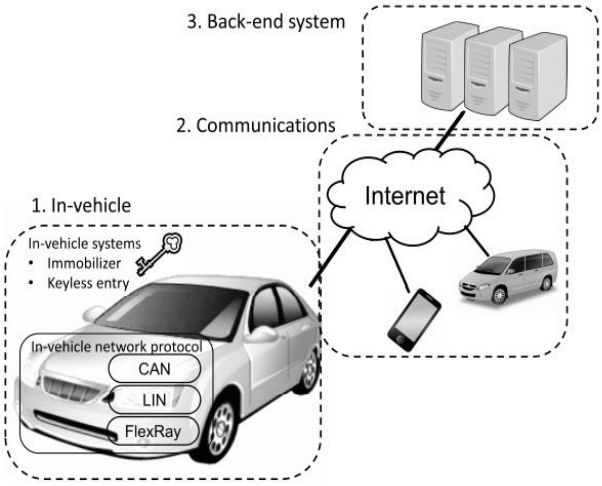

Fig. 3. Environment surrounding connected vehicles [20].

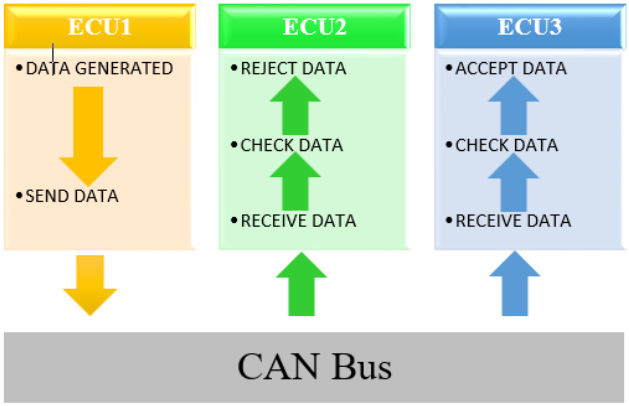

Fig. 4. ECUs communicating through CAN Bus [21].

1) In-Vehicle Communication Protocols: Modern vehicles consist of plenty of Electronic Control Units (ECUs), which are responsible for controlling and monitoring vehicles [28]. Due to the exponential growth of ECUs in modern vehicles, it is inefficient to connect all ECUs for point-to-point communication. A large number of wires, cost, space, and fault detection are the main factors that lead to the development of a common bus system with standard

protocols through which all ECUs are connected and communicate with each other [22]. In this section, we explored the standard protocols used in modern vehicles to connect different ECUs.

a) Controller Area Network (CAN): CAN is a simple and robust serial communication protocol that is primarily designed for the automotive industry. CAN has been the most successful and widely used in-vehicle communication protocol since its publication in 1986. can be successfully implemented in real-time systems [23]. From an autonomous vehicle perspective, it allows communication between different sensors and actuators. The Standard CAN protocol is used by different famous car manufacturers, i.e., Honda, Ford, General Motors, and Volkswagen [24]. In modern connected vehicles, hundreds of ECUs are embedded to control the different functions of the car. These ECUs are linked and communicate through the CAN bus. Thus, the CAN bus plays a vital role in autonomous driving as controlling, diagnosing, and different signals among various ECUs pass through the CAN bus. CAN is a plug-and-play system, which means without further modification, a new ECU can be added to the existing in-vehicular network [25-27]. CAN packets also contain no information about sender and receiver nodes, so it is easy for hackers to temper packet bits of the CAN bus system. Being a central bus in-vehicle system, the CAN bus is often the main target of hackers. All the ECUs are linked with each other through the CAN bus system, so if attackers gain access to this bus, it will be a major safety threat to the vehicle itself as well as its passengers. Attackers may stop the engine, disable door locks, temp sensor data, etc. In short, hackers may access the CAN bus via smartphone applications, USB, or through the OBD-II (On-board Diagnostics) port, which is harmful to vehicles, infrastructure, and passengers [21-27].

b) FlexRay: FlexRay is an advanced serial communication protocol in the automotive industry that addresses the security challenges faced by CAN and LIN bus protocols. Due to high-speed data transfer (up to 10 Mbps) and other safety-critical features such as fault tolerance, FlexRay is now being considered as a promising de facto standard protocol in the automotive industry, particularly in connected cars. It is a faster, safer, and more reliable protocol compared to CAN and TCP (Transmission Control Protocol), but it is costly. The Flexray protocol supports star, mesh, and hybrid topologies (a combination of bus and star) through which all the ECUs are connected [26]. The FlexRay protocol can be used in synchronous and asynchronous modes, which makes it an ideal choice for real-time in-vehicle systems such as engine RPM control, door lock systems, Anti-Lock braking systems (ABS), etc.

2) Local Interconnect Network (LIN): LIN is a low-cost, serial interface (between vehicle sensors and actuators) and is currently a de-facto standard in all modern vehicles to control vehicle seats, wipers, sunroofs, etc. with data rates up to 20kbps [34]. LIN is a master-slave architecture and provides collision-free communication for up to 16 slaves [35]. Typically, LIN nodes are grouped into clusters. Each cluster has a master node that communicates with the backbone high-speed CAN bus [36]. Vulnerabilities are associated with the LIN master-slave communication architecture, which can cause a spoofing attack on the LIN bus. For example, a message from a master node can cause a slave to go into sleep mode. Attackers can take the edge of the master to shut down the LIN network by turning slaves into sleep mode [27]. A comparison of FlexRay, CAN, and LIN is provided in Table 1.

TABLE I. COMPARISON OF CAN, FLEXRAY, AND LIN BUS SYSTEM

Features	Bus System		
	CAN	***FlexRay***	***LIN***
Message Transmission Mode	Asynchronous	Synchronous and Asynchronous	Synchronous
Data Rate	1Mbps	10Mbps	20Kbps
Complexity	Low	High	Low
Network Architecture	Bus	Bus, Star, Hybrid	Bus
Application	Airbag, Engine Control, Anti-lock braking	X-by-Wire systems (Throttle, steering, clutch)	Door locking, side mirrors, Wipers, Sunroof

3) Remote Attack Surfaces in Connected Cars: Connected cars are equipped with numerous sensors (LiDAR, cameras, radar, etc.) through which the car navigates itself from source to destination. The reliability and safety of the journey heavily depend on the performance of these sensors. Remote attacks from cyber criminals may lower the performance of sensors, which ultimately disrupts vehicle safety, so the robustness of sensors is imperative. For instance, if LiDAR is confused by a fake object, it may cause emergency brakes, which are adverse at a large scale level. This section briefly describes the various attacks on-vehicle sensors.

a) Cyber-attacks on Camera: The camera plays a vital role in an autonomous car as it is used for road lane detection, traffic light detection, pedestrian detection, road sign detection, and some other feature extraction. For sign detection, the camera can be fooled by placing ambiguous shapes on road signs. Similarly, for lane detection, the camera can be misled by drawing multiple lanes or by using unusual lane colors. Object detection is another prominent feature offered by a camera sensor. For object detection, the camera can be hacked by a Denial of Service attack (i.e., showing too many objects to detect, thus slowing down the processing time).

b) Cyber-attacks on LiDAR: Light Detection and Ranging (LiDAR) is an integral part of modern autonomous vehicles. For safe and secure transportation, awareness of the surrounding object's geometry is very important. The camera is not a robust sensor as lighting conditions and weather affect the camera's performance. LiDAR provides accurate geometrical information of road objects by which the number of objects can be detected and correspondent decisions (i.e., accelerate, brake, blinker, etc.) can be initiated. Adaptive Cruise Control (ACC) and Collision Avoidance Systems (CAS) are the two prominent features of modern vehicles, which are based on fixed-positioned LiDAR. To acquire a three-dimensional view of the environment, LiDAR is mounted on a rotatable fixture. The spatial resolution of

LiDAR offers accurate scanning, which helps to distinguish cars and pedestrians.

c) Cyber-attacks on GPS: To obtain the absolute location and navigation of vehicles with great accuracy, CAVs are equipped with a Global Positioning System (GPS). The transparent architecture of GPS offers hackers the opportunity to temper GPS data, which leads to the wrong direction of the vehicle. Such attacks, known as GPS spoofing attacks, are serious security threats to passengers. A recent study conducted by Regulus Cyber (a company that deals with smart sensor security) found that the navigation systems of the Tesla Model S and Model 3 are vulnerable to cyberattacks. Regulus researchers disclosed that spoofing attacks on Tesla GPS could easily be executed wirelessly [28-39]. GPS receivers are programmed to process the strongest signal. To mislead the vehicle, attackers must strengthen the spurious signal over an authentic GPS signal, as depicted in Figure 5. Research for the countermeasure of spoofing attacks has been taking place [40], [41], and [42]. Jamming is another simplistic attack associated with GPS. In such attacks, only substantial noise is transmitted on the GPS frequency (1575.42 MHz) to prevent the receiver from picking up the authentic signal.

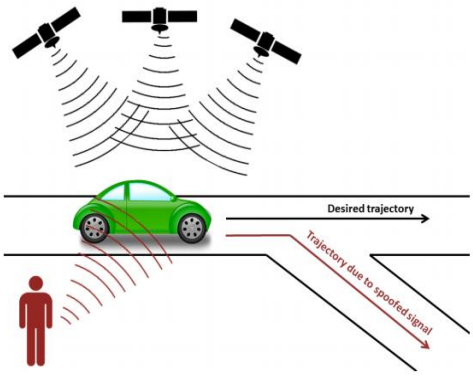

Figure 5: Illustration of a GPS spoofing attack [44].

Knowledge gap 3: *The modern automotive industry depends on chip makers and other vendors. Usually, a contract is signed to ensure the supply chain. Due to time limitations, manufacturers focus on the number of their products, and no extra effort is taken to assure strict security for the vehicle.*

4) Other Attack Surfaces

The other prominent attack surfaces are: An anti-theft system is designed to obstruct the vehicle engine from being started until a programmed key is not used. A Tyre-pressure monitoring system (tpms) is a small device mounted on the valve of each tire. It sends real-time information about tire pressure to an ECU. Cyber-attack on TPMS might result to send a false message (tire pressure) to the onboard system. A remote Keyless System (RKS) is a short-range radio transmitter that communicates with the vehicle ECU to check the validity of the lock/unlock and ignite key for the vehicle. RKS may be active or passive. In active RKS, a button is used while in passive RKS, a key is used to remotely lock/unlock the car [45-46]. Bluetooth is used in modern vehicles to sync a device with the car and media connectivity. The researcher shows that paired Bluetooth devices in the vehicle could start to communicate with ECUs. Cellular / Wi-Fi module is used in CAVs for long-range communication to obtain traffic or weather information by using 3G/LTE or GSM technology. On-Board Diagnostic (OBD) port is used for vehicle maintenance, finding system failure, and firmware upgradation. It can access all CAN buses in the vehicular network and can modify ECUs functionality. For instance, the mileage count may be reduced to enhance vehicle value. Therefore, the OBD port put the vehicle at a high threat level.

IV. Types of Cyber-Attacks

CAV connectivity with the outside world is imperative, but this exposes the vehicle to experiencing hazardous cyber-attacks. If we fail to provide a shield against such attacks, hackers may initiate commands to ECUs to misguide the vehicle, track its location, and steal passengers' private data from a remote location [53]. This section explores the active and passive attacks on CAVs.

Knowledge gap 4: *Modern vehicles have a lot of connectivity features such as Bluetooth, Email, and web browsing. Some literature describes how attackers may use the infotainment system to hack vehicles. But very few pieces of literature focus on mitigation strategies to deal with such attacks.*

A. Passive attacks

Identifying passive attacks is a challenging task as attackers cannot alter the contents of transmitted data. Both sender and receiver are unacquainted with the man in the middle of their activities. Such attacks monitor the traffic flow and do not interact with a third party [8]. The following passive attacks may be faced by CAVs:

1) Eavesdropping: In such attacks, attackers passively steal the communication messages on the Vehicle to Everything (V2X) communication channel. The CAN bus' potential vulnerability to cyber threats offers attackers the opportunity to gain access to the in-vehicle network and eavesdrop on the CAN transmission. The connectivity of CAVs with pedestrians, infrastructure, and vehicles gives more significance to eavesdropping attacks, as more private information may be listened to or monitored by hackers without permission.

2) Traffic Analysis: Eavesdropping attacks may be prevented by using cryptography. However, attackers may use traffic analysis techniques to deduce information by observing traffic flow, i.e., the length and time of the message, how many times (frequency) the vehicle communicated with X person, the amount of data, and the presence or absence of the peculiar driver. Based on these properties, attackers may infer the user's working time and daily habits [8-30].

B. Active attacks

In active attacks, the attackers intrude on the communication network, alter the contents of data, or generate new packets to damage the messages [8-32]. Active attacks are much more dangerous than passive attacks, especially in a CAV environment, because alteration of messages can cause physical damage to drivers as well as the vehicle itself. The following active attacks may be faced by CAVs:

1) Spoofing: In spoofing attacks, an unauthorized person intrudes into the network and poses as an authorized person. Based on false messages transmitted by the attacker, CAV may take the wrong decision. For instance, a serious accident could be caused if the vehicle believes that there is no obstacle in front. Similarly, attackers may direct all cars toward the wrong path, which ultimately causes traffic jams.

2) Replay Attacks: Replay attacks happen when a malicious user "sniffs" out data on the communication channel, captures it, and rebroadcasts it. In a replay attack, both the sender and receiver are verified, but they are unaware of the node in the middle intercepting the messages. Upon rebroadcasting the message, the malicious user arouses the receiver to perform an activity (e.g. a system reset) while the receiver thinks that the original sender is requesting this action.

3) Masquerade: In a masquerade attack, an unauthorized person impersonates a legitimate node and an authorized entity to gain access to information resources. The unavailability of encryption and lack of message authentication in CAN frames are two factors that facilitate the masquerade attacks. In the CAV environment, the malicious vehicle may pretend to be another vehicle to gain an advantage, i.e., pose as an ambulance to slow down the traffic or bypass traffic rules.

*4) Message modification:*In this kind of attack, false messages are inserted by attackers into the in-vehicle network through the OBD-II port or telematics system. The CAN protocol used in connected cars does not have a message authentication feature (i.e., no information about the validity of the source), so false frame injection is possible. Furthermore, message modification involves message delaying, inserting new frames, reordering, and deleting some bits or frames in a packet. For example, a delay in the emergency braking message may cause serious road accidents.

5) Denial-of-service (DoS): A denial of service (DoS) attack is a high-level security threat extensively used for many years to interrupt network operations by sending a vast number of high-priority messages toward hosts to overload them, and so, the host fails to provide service to legitimate users. In short, dummy messages are introduced to jam the network. Thus, the efficiency and performance of the host will be reduced. The prime objective of a DoS attack is to prevent a legitimate user from accessing the network services. Attackers could change the CAN segment identifier (which defines the priority of the message) to take control of the vehicle. Some DoS attacks may affect the infotainment system, while others target the CAN bus to disturb the critical parts such as the steering, throttle, and brakes. The ECUs responsible for these parts may be overloaded with DoS attacks, so they fail to initiate commands in real-time to control the vehicle [59-62].

V. Countermeasures for Cyber-attacks in-vehicle network

Cyber-attacks hit not only connected cars but also the backend servers and the entire network. Since 2016, automotive cybersecurity attacks have increased by 605%. In 2019, 57% of incidents were performed by cybercriminals while only 38% were carried out by researchers to expose the vulnerabilities in in-vehicle systems. A wide variety of cyber-attacks are remote attacks that do not require a physical connection with a vehicle. For example, in 2019, 82% of incidents were carried out remotely. Due to the limited computational power of electronic devices, conventional defense mechanisms cannot be deployed inside the vehicular network [28]. This section describes the various defensive schemes that are being used in connected cars to prevent unauthorized access to the vehicle.

Knowledge gap 5: *Insufficient research is available about the reaction of a vehicle or driver to a cyber-attack. Is there any safe mode in the vehicle that will be activated to ensure the safety of the vehicle, driver, and passengers? Does the vehicle have the level of sensibility to pass control to the driver in such circumstances?*

A. Authentication:

The CAV, users, and back-end servers should be authorized to use the vehicle network. Especially in the V2X channel (when the vehicle communicates with everything), there should be a hard-and-fast authentication procedure to verify all parties. From the military aspect, this procedure becomes more prominent.

B. Encryption

Messages broadcast to all vehicles and surrounding infrastructure should be encrypted so that only legitimate users can get access to the message contents. A strong encryption-decryption system improves the overall security of message transmission [8]. The availability of CAN buses makes the in-vehicle network more vulnerable to cyber threats. Encryption is a technique used to protect the message from the agent and make communication more secure by using various codes so that only the sender and intended receiver can read and acknowledge the communication. Encryption is an integral part of modern vehicular communication that ensures the safety and integrity of data. Therefore, communication between vehicles and backend servers should be properly encrypted. Moreover, the IP address of the telematic unit should not be revealed to any external device.

C. Gateway Installation

A gateway is an indispensable part of connected vehicle communication networks, as different ECUs communicate with each other through a gateway. The gateway acts as a translator among various nodes with different protocols and data frame formats. For example, a low-speed ECU wants to send a signal to another ECU that has a high speed, so gateways adjust the baud rate to ensure compatibility between the sender and receiver ECUs. Installation of gateways in the vehicular network is not a new idea, but modern gateways are more complex as the number of ECUs has been increased to fulfill the requirements of different features in connected cars.

D. Isolating potential attacking surfaces from vehicular Network

The interfacing of in-vehicular networks with the outside world served as an entry point for attackers to inject a false message into a vehicular network. The On-Board Diagnostic (OBD) port and telematics system are the most common interfaces which connect the CAV with outside devices. The OBD port is used for diagnostic purposes while the telematics system gathers important information related to the vehicle's location, activity, and driver behaviors and sends it to the secure servers via cellular networks. The OBD port is difficult to isolate from the in-vehicle network as it diagnoses the vehicle's fault and can be used to improve vehicle performance by reprogramming the firmware. However, installing a detector on the OBD port which identifies false frame injection when the vehicle is linked with the OBD tool to pull vehicle information for diagnostic purposes.

E. Intrusion Detection System

An intrusion detection system (IDS) is designed for the CAN network, which follows the misuse detection system. This system uses the features of already known attacks to recognize specific attacks such as Denial of Service (DoS) attacks. However, with this system, the complexity of the system has increased. Numerous authors proposed different techniques, i.e., deep learning, anomaly detection systems, etc., to implement IDS in a vehicular network. CAV designers should add intrusion protection systems to in-vehicle networks that detect unauthorized intrusion and report it.

TABLE 2: SUMMARY OF COUNTERMEASURES

Type of attack	Proposed Countermeasure
Eavesdropping	Authentication, Encryption, Cryptography
Traffic Analysis	Intrusion Detection System (IDS), Encryption
Spoofing	Authentication, IDS
Replay Attacks	Gateway installation, Encryption
Masquerades	Authentication, Gateways, Encryption
Message Modification	Authentications, Encryption
Denial-of-Service Attack	Gateways installation, IDS, Encryption, Authentication

VI. CONCLUSION

The exploding number of ECUs, exceeding lines of code, and a higher level of connectivity and integration make the CAV a more complex system and create unique challenges for automakers. This review paper highlights the vulnerabilities of vehicle communication protocols and sensors. This paper aimed to provide an overview of the in-vehicle network structure and threats associated with the vehicle. Various in-vehicle communication protocols (e.g. CAN, FlexRay) are elaborated on with their pros and cons in this paper. Similarly, numerous sensors with their possible attacks are presented. Active and passive attacks could be prevented with substantial safety measures like Message authentication, Encryption, intrusion detection system (IDS), etc. Consistently implementing effective secure design at the hardware and software level may guarantee product security. This requires a sound and well-managed collaboration among automakers, IT security companies, and chip makers. There are considerable knowledge gaps presented in this paper which require substantial efforts from CAV researchers. These knowledge gaps should be addressed promptly to ensure rigorous cyber security defense in CAVs. In conclusion, this paper provides a better understanding of connected vehicles' cyber-security threats and their mitigation strategies.

REFERENCES

[1] "Self-driving car", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Self-driving_car. [Accessed: 26- Mar- 2020].

[2] Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibáñez, J. (2019). Autonomous Cars: Challenges and Opportunities. *IT Professional*, *21*(6), 6-13

[3] "Autonomous Vehicles & Car Companies l CB Insights", *CB Insights Research*, 2020. [Online]. Available: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/. [Accessed: 26- Mar- 2020].

[4] "Levels of Driving Automation" Standard for Self-Driving Vehicles", *Sae.org*, 2020. [Online]. Available: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its- "levels-of-driving-automation"-standard-for-self-driving-vehicles. [Accessed: 26- Mar- 2020].

[5] Morimoto, S., Wang, F., Zhang, R., & Zhu, J. Cybersecurity in Autonomous Vehicles.

[6] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, *2015*, 91

[7] Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. *IEEE internet of things journal*, *1*(4), 289-299.

[8] He, Q., Meng, X., & Qu, R. (2017, May). Survey on cyber security of CAV. In *2017 Forum on Cooperative Positioning and Service (CPGPS)* (pp. 351-354). IEEE.

[9] Raiyn, J. (2018). Data and cyber security in autonomous vehicle networks. *Transport and Telecommunication Journal*, *19*(4), 325-334.

[10] "Self-driving car technology: When will the robots hit the road?", McKinsey & Company, 2020. [Online]. Available: *https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/self-driving-car-technology-when-will-the-robots-hit-the-road*. [Accessed: 28- Mar- 2020].

[11] Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, *18*(11), 2898-2915.

[12] Jawhar, I., Mohamed, N., & Zhang, L. (2010, July). Inter-vehicular communication systems, protocols and middleware. In *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage* (pp. 282-287). IEEE.

[13] Axelrod, C. W. (2017, May). Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE.

[14] "Uber has resumed testing its self-driving cars in San Francisco", The Verge, 2020. [Online]. Available: *https://www.theverge.com/2020/3/10/21172213/uber-self-driving-car-resume-testing-san-francisco-crash*. [Accessed: 29- Mar- 2020].

[15] "Waymo", En.wikipedia.org, 2020. [Online]. Available: *https://en.wikipedia.org/wiki/Waymo*. [Accessed: 29- Mar- 2020].

[16] H. Pyeongchang!, "Hyundai self-driving cars: initial testing is successful! | Car News | Auto123", auto123.com, 2020. [Online]. Available: *https://www.auto123.com/en/news/hyundai-autonomous-vehicles-successful-first-tests/64371/*. [Accessed: 29- Mar- 2020].

[17] Hodge, C., Hauck, K., Gupta, S., & Bennett, J. C. (2019). *Vehicle Cybersecurity Threats and Mitigation Approaches* (No. NREL/TP-5400-74247). National Renewable Energy Lab.(NREL), Golden, CO (United States).

[18] Tout, S., Abualkibash, M., & Patil, P. (2018, May). Emerging Research in the Security of Modern and Autonomous Vehicles. In *2018 IEEE International Conference on Electro/Information Technology (EIT)* (pp. 0543-0547). IEEE.

[19] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium* (Vol. 4, pp. 447-462).

[20] Takahashi, J. (2018). An overview of cyber security for connected vehicles. *IEICE TRANSACTIONS on Information and Systems*, *101*(11), 2561-2575.

[21] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010, May). Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy* (pp. 447-462). IEEE.

[22] Jayabala, Pradeep & Sebasteen, S & Dineshkrishna, R. (2018). COMPARISON OF CAN AND FLEXRAY PROTOCOL FOR AUTOMOTIVE APPLICATION. *International Journal of Pure and Applied Mathematics. 119.* 1739-1745.

[23] Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. *Journal of information security and applications*, *36*, 90-100.

[24] Lin, C. W., & Sangiovanni-Vincentelli, A. (2012, December). Cyber-security for the controller area network (CAN) communication protocol. In *2012 International Conference on Cyber Security* (pp. 1-7). IEEE.

[25] Rishvanth, D. V., & Ganesan, K. (2011). Design of an In-Vehicle Network (Using LIN CAN and FlexRay) Gateway and its Diagnostics Using Vector CANoe. *American Journal of Signal Processing*, *1*(2), 40-45.

[26] Hafeez, A., Malik, H., Avatefipour, O., Rongali, P. R., & Zehra, S. (2017). *Comparative study of can-bus and flexray protocols for in-vehicle communication* (No. 2017-01-0017). SAE Technical Paper.

[27] Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., ... & Xiang, Y. (2019). An overview of attacks and defences on intelligent connected vehicles. *arXiv preprint arXiv:1907.07455*.

[28] Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, *31*(5), 50-58.

[29] Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015). Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, *11*, 2015.

[30] Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, *12*(4), 369-381.

[31] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2019). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 100214.

[32] Al-Kahtani, M. S. (2012, December). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In *2012 6th International Conference on Signal Processing and Communication Systems* (pp. 1-9). IEEE.

[33] La, V. H., & Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey.

[34] Amirtahmasebi, K., & Jalalinia, S. R. (2010). Vehicular networks–security, vulnerabilities and countermeasures.

[35] Hu, Q., & Luo, F. (2018). Review of secure communication approaches for in-vehicle network. *International Journal of Automotive Technology*, *19*(5), 879-894.

[36] A. Thomas, "What's Happening with Automated Vehicles?", *Self Driving Cars 360*, 2020. [Online]. Available: https://www.selfdrivingcars360.com/whats-happening-with-automated-vehicles/. [Accessed: 15- May- 2020].

[37] C. Electronics, "LIN Bus Explained - A Simple Intro", *CSS Electronics*, 2020. [Online]. Available: https://www.csselectronics.com/screen/page/lin-bus-protocol-intro-basics/language/en. [Accessed: 15- May- 2020].

[38] Kumar, A. D., Chebrolu, K. N. R., & KP, S. (2018). A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities. *arXiv preprint arXiv:1810.04144*.

[39] R. Cyber, "Tesla Model S and Model 3 Prove Vulnerable to GPS Spoofing Attacks as Autopilot Navigation Steers Car off Road, Research from Regulus Cyber Shows", *Prnewswire.com*, 2020. [Online]. Available: https://www.prnewswire.com/il/news-releases/tesla-model-s-and-model-3-prove-vulnerable-to-gps-spoofing-attacks-as-autopilot-navigation-steers-car-off-road-research-from-regulus-cyber-shows-300871146.html. [Accessed: 17- May- 2020].

[40] Warner, J. S., & Johnston, R. G. (2003). GPS spoofing countermeasures. *Homeland Security Journal*, *25*(2), 19-27.

[41] Wen, H., Huang, P. Y. R., Dyer, J., Archinal, A., & Fagan, J. (2005, September). Countermeasures for GPS signal spoofing. In *ION GNSS* (Vol. 5, pp. 13-16).

[42] Haider, Z., & Khalid, S. (2016, August). Survey on effective GPS spoofing countermeasures. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 573-577). IEEE.

[43] C. Recommendations, "Connected Car Security Threat Analysis And Recommendations", *Sites.google.com*, 2020. [Online]. Available: https://sites.google.com/view/bifazpqpdf/connected-car-security-threat-analysis-and-recommendations. [Accessed: 30- Jun- 2020].

[44] "Bloomberg - Are you a robot?", *Bloomberg.com*, 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2018-08-01/autonomous-car-tech-investment-skyrockets-on-softbank-deals. [Accessed: 01- Jul- 2020].

[45] "Automotive cybersecurity incidents doubled in 2019, up 605% since 2016 - Help Net Security", *Help Net Security*, 2020. [Online]. Available: https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/. [Accessed: 02- Jul- 2020].

[46] Gülsever, M. (2019). A Study on Vulnerabilities in Connected Cars.

[47] Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

[48] Verdult, R., Garcia, F. D., & Ege, B. (2015). Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *Supplement to the Proceedings of 22nd {USENIX} Security Symposium (Supplement to {USENIX} Security 15)* (pp. 703-718).

[49] Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). Lock it and still lose it—on the (in) security of automotive remote keyless entry systems. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*.

[50] Wyglinski, A. M., Huang, X., Padir, T., Lai, L., Eisenbarth, T. R., & Venkatasubramanian, K. (2013). Security of autonomous systems employing embedded computing and sensors. *IEEE micro*, *33*(1), 80-86.

[51] King, J. D. (2001). *U.S. Patent No. 6,236,333*. Washington, DC: U.S. Patent and Trademark Office.

[52] Miller, C., & Valasek, C. (2014). A survey of remote automotive attack surfaces. *black hat USA*, *2014*, 94.

[53] "Vehicle Hacking", *Argus Cyber Security*, 2020. [Online]. Available: https://argus-sec.com/car-hacking. [Accessed: 07- Jul- 2020].

[54] Vahidi, A., & Eskandarian, A. (2003). Research advances in intelligent collision avoidance and adaptive cruise control. *IEEE transactions on intelligent transportation systems*, *4*(3), 143-153.

[55] Shaout, A., Colella, D., & Awad, S. S. (2011, December). Advanced driver assistance systems-past, present and future. In *2011 Seventh International Computer Engineering Conference (ICENCO'2011)* (pp. 72-82). IEEE.

[56] Clanton, J. M., Bevly, D. M., & Hodel, A. S. (2009). A low-cost solution for an integrated multisensor lane departure warning system. *IEEE Transactions on Intelligent Transportation Systems*, *10*(1), 47-59.

[57] Bera, T. K., Bhattacharya, K., & Samantaray, A. K. (2011). Evaluation of antilock braking system with an integrated model of full vehicle system dynamics. *Simulation Modelling Practice and Theory*, *19*(10), 2131-2150.

[58] Hu, J., & Xiong, C. (2012, March). Study on the embedded CAN bus control system in the vehicle. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 2, pp. 440-442). IEEE.

[59] Rizvi, S., Willet, J., Perino, D., Marasco, S., & Condo, C. (2017). A threat to vehicular cyber security and the urgency for correction. *Procedia computer science*, *114*, 100-105.

[60] He, L., Li, W., Guo, C., & Niu, R. (2014, December). Civilian unmanned aerial vehicle vulnerability to gps spoofing attacks. In *2014 Seventh International Symposium on Computational Intelligence and Design* (Vol. 2, pp. 212-215). IEEE.

[61] Seo, S. H., Lee, B. H., Im, S. H., & Jee, G. I. (2015). Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. *Journal of Positioning, Navigation, and Timing*, *4*(2), 57-65.

[62] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011, October). On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 75-86).