Shielding the Drive: A Survey of Cybersecurity Challenges and Solutions in Automotive Control Networks

Md Abdul Muntaqim Qureshi
ID 40191640

Mehran Mujib
ID 40276697

Aporajita Dutta Purkayastha
ID 40233325

Akash Saha
ID 40233587

Nadia Ferdous
ID 40263272

Md Anisuzzaman Rumon
ID 40222093

Md Hafizul Islam
ID 40225761

Pritom Samanta Picklu ID 40255233

Fatema Ahsan Meem
ID 40235119

Mohammad Tawsif Ul Hye Chowdhury
ID 40261062

Mehrab Helal Shuvo
ID 40241199

***Abstract*— Modern vehicles rely on a core digital framework, primarily the Controller Area Network (CAN) and its variations, which manage numerous essential operations. As vehicles become more interconnected and autonomous, ensuring the security of these in-vehicle control networks becomes crucial. Cyberattacks targeting these systems could lead to significant risks, affecting everything from user privacy to overall vehicle safety. This review delves into a thorough investigation of recent cyberattacks on automotive networks, including CAN, Local Interconnect Network (LIN), and , aiming to pinpoint persistent security flaws and assess the necessary computational and communicative efforts for such breaches. The findings from this study will contribute to crafting more robust security strategies, thereby safeguarding the functionality and dependability of in-vehicle control systems in contemporary cars.**

Keywords*— *Automotive Control Networks, Controller Area Network (CAN), Subsystem Communication, ECU Communication Standard, ocal Interconnect Network (LIN), FlexRay, Digital Protection, Protective Strategies, Risk Overview, Cybersecurity, Vehicle ECUs Network, Attack Vectors, Vulnerabilities, Threat Landscape, Security Measures, In Vehicle Control Networks, High-Speed Communication, Exploitation Methods, System Weaknesses, Internal ECU Interconnectivity.

I. INTRODUCTION

The automotive sector's rapid adoption of advanced electronic systems has ushered in a new era of vehicle functionality while simultaneously exposing vehicles to unprecedented cybersecurity risks. The integration of sophisticated electronic components, such as sensors, actuators, and communication systems, has transformed vehicles from closed to open systems, significantly expanding the potential for cyber threats. This evolution has introduced complexities in vehicle communication and broadened the scope for cyber-attacks, which can now be executed remotely without physical access to the vehicle.

One critical concern is the Controller Area Network (CAN) protocol, where vulnerabilities can be exploited, compromising the principle of availability by allowing messages of the highest priority to dominate the network. This manipulation can render the network inaccessible to lower-priority nodes, violating the principle of availability. Automotive cyber-attacks are categorized into physical access attacks and remote access attacks. Physical access attacks involve direct interaction with the vehicle's network systems through methods like On-Board Diagnostic (OBD) port attacks or installing unauthorized devices within the network. Remote access attacks exploit wireless communication interfaces like Bluetooth, Wi-Fi, and cellular networks.

Notable examples include physical access attacks through the OBD port, where attackers can manipulate critical vehicle modules such as brakes and engine control. Selective Denial-of-Service (DoS) attacks disrupt networks without full message transmission by overwriting specific bits in transmitted data, exploiting vulnerabilities in the CAN standard. Research in this area has focused on exploiting these vulnerabilities, leading to government alerts and increased awareness of vehicles' susceptibility to such attacks. Indirect physical access attacks do not require direct access to the vehicle's network but can be executed through methods

like attacking via multimedia devices or hacking car service IT systems.

Remote access attacks pose a significant threat due to the integration of various wireless interfaces necessary for communication with systems like anti-theft devices, tire pressure monitoring systems (TPMS), Bluetooth, and telematics units. Exploiting wireless interfaces connected to the CAN via a gateway ECU has been demonstrated as a vulnerable point for hacking. Successful compromises of these systems can lead to unauthorized control over the vehicle, including unlocking doors and manipulating vehicle functions remotely. Over-the-air (OTA) updates present another attack surface where hackers can potentially intercept these updates to infiltrate the vehicle's communication network, leading to ransomware attacks or other forms of cyber sabotage. The advent of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications introduces new vulnerabilities that can be compromised by spoofed messages, resulting in disruptions to in-vehicle communication networks.

Attacks on in-vehicle network systems target various entry points susceptible to security breaches, including OBD-II ports used for monitoring vehicle diagnostics, USB and charging ports that are susceptible to severe security threats like installing malicious codes, TPMS systems that are well-documented targets for exploitation lacking essential security safeguards, bus network ports vulnerable due to lack of communication protection in CAN protocols allowing attackers to send fake frames leading to unintended vehicle behaviour, and vehicular communication ports enabled with technologies like Bluetooth, Wi-Fi, DSRC, and cellular networks vulnerable to various attacks including jamming and eavesdropping potentially allowing attackers full access to vehicles.

II. Overview

Imagine this: your automobile, an intricate creature, vibrating with digital vitality across unobserved networks. The Controller Area Network (CAN) is a crucial communications hub that coordinates the various tasks of your vehicle. The Local Interconnect Network (LIN) and FlexRay are key components inside the vehicle's ecological framework.

Furthermore, as our vehicles progress into increasingly interconnected entities, equipped with advanced intelligence and autonomy, they also become very susceptible to cyber adversaries. Cybersecurity is not merely an additional attribute; it serves as a protective barrier, a protector that stands between security and disorder.

This investigation focuses on the fundamental aspects of automotive networks, specifically CAN, LIN, and FlexRay. We are currently investigating the intricacies of communication within these systems, the possible risks that exist in the digital realm, and the advanced measures being developed to mitigate these cyber attacks. It is not alone about protecting our automobiles, but also about guaranteeing the safety of individuals inside them.

Controller Area Network (CAN)

The Controller Area Network (CAN) is a resilient vehicle communication system that facilitates communication between different electronic control units (ECUs) within a vehicle, eliminating the need for a central computer. CAN, created by Bosch in the 1980s, was specifically built to cater to the requirements of intricate cars. It effectively handles the transmission of information among the various systems responsible for control, safety, efficiency, and comfort.

A. Notable characteristics and capabilities of CAN

The CAN system functions based on a multi-master principle, wherein any Electronic Control Unit (ECU) has the capability to initiate communication within the network. The instantaneous processing and action upon sensor input is of utmost importance in real-time systems.

The management of message priority in CAN is achieved by the utilisation of a non-destructive arbitration approach. In the event that two Electronic Control Units (ECUs) initiate message transmission concurrently, the message possessing a higher priority, as indicated by its lower identification value, is accorded precedence within the network. This prioritisation mechanism guarantees the prompt transmission of crucial information.

CAN networks provide resilient error detection and handling techniques, encompassing frame checks, acknowledgment checks, and error signalling for effective error management. These characteristics guarantee a high level of dependability and integrity in the transfer of data.

The basic CAN network functions at speeds of up to 1 Mbps. However, the more recent CAN FD (Flexible Data-Rate) technology enhances this capability by enabling larger data rates and optimising the utilisation of network bandwidth.

CAN greatly enhances vehicle economy by enabling numerous ECUs to communicate via a single or a few wires, resulting in reduced complexity and weight of car wiring harnesses.

B. Summary of Operations

Data in a CAN network is conveyed using messages. The priority and content type of each message are determined by an identifier, whereas the address of a specific receiver is not included. Every message is received by all nodes in the network, which then determine whether to handle it based on its identity. This methodology streamlines the structure of the network and improves its adaptability and expandability.

C. Elements comprising a CAN Network

The transceivers are responsible for the conversion of digital signals received from the ECUs into differential signals that are utilised on the CAN bus, and vice versa.

Connectors play a crucial role in enabling physical connections among participants within a network.

Terminators refer to resistors positioned at both ends of a bus in order to mitigate signal reflections.

D. Application Areas

The utilisation of CAN extends beyond automotive applications, encompassing industrial automation, medical equipment, and other domains where the establishment of dependable communication among diverse devices is of utmost importance.

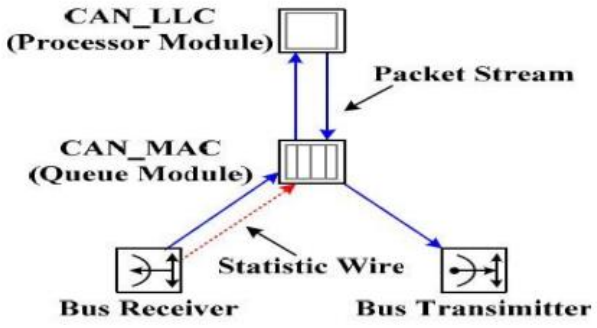

Figure: A CAN Network diagram {citadel}

A simplified diagram showing several ECUs (like the engine control unit, brake control unit, and airbag system) connected through a twisted pair of wires representing the CAN bus. Each ECU has a transceiver connecting it to the bus, with terminators placed at both ends of the network to ensure signal integrity. This configuration highlights how information flows seamlessly across different vehicle systems via the CAN network, enabling integrated vehicle control and diagnostics.

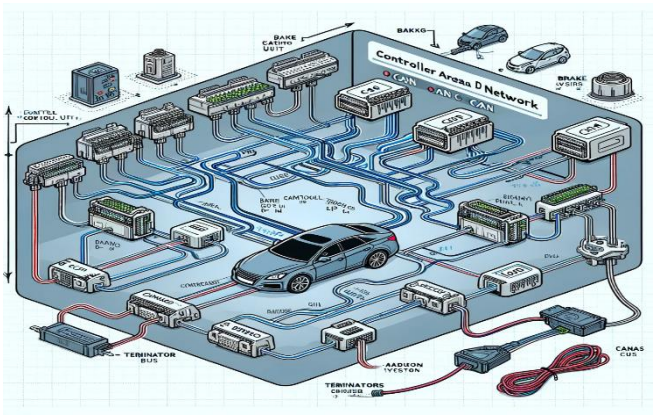

Figure: Controller Area Network (CAN) in a vehicle

Here's a diagram illustrating the Controller Area Network (CAN) in a vehicle. It shows multiple Electronic Control Units (ECUs) such as the engine control unit, brake control unit, and airbag system, all connected through a twisted pair of wires representing the CAN bus. Each ECU is linked to the bus with a transceiver, and terminators at both ends of the network ensure signal integrity. This visual representation helps to understand how information flows across different vehicle systems via the CAN network, enabling integrated vehicle control and diagnostics.

Local Interconnect Network (LIN)

The Local Interconnect Network (LIN) is a serial network protocol that is employed in automobiles to

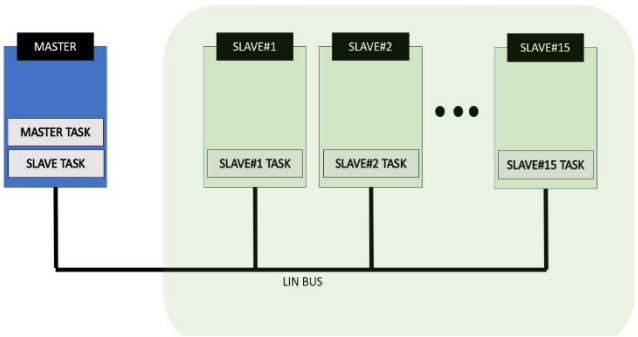

Figure: A LIN Network {Mitadel}

facilitate communication between various components within the vehicles, offering a cost-effective solution. The Linear Interval Network (LIN) was created as a supplementary component to the more intricate Control Area Network (CAN) network. Its primary purpose is to provide lower data rates and less crucial applications, rendering it well-suited for the control of uncomplicated functions such as mirrors, window controls, and seat adjusters.

A. Main Characteristics and Purposes of LIN

The LIN system functions based on a master-slave architecture, wherein a solitary master control unit establishes communication with a maximum of 16 slave nodes. This configuration streamlines network administration and diminishes the intricacy of wiring.

Economical: The LIN protocol use low-cost silicon and necessitates a reduced number of cables, rendering it a cost-effective option for interconnecting non-essential vehicle operations.

The communication in a LIN network is characterised by determinism, wherein the timing of message transmission is predetermined and scheduled by the master node. This characteristic ensures that communication intervals are predictable.

Interoperability is a key feature of LIN, as it is specifically engineered to facilitate seamless integration with other automotive communication systems such as CAN, hence enabling seamless communication inside the electrical architecture of the car.

B. Summary of Operations

The primary node in a Local Area Network (LIN) is accountable for coordinating communication and transmitting header frames that indicate the appropriate slave node to reply. Upon identifying its address in the header, every slave node promptly answers at the specified time. The use of this regulated system effectively mitigates data collision and guarantees uninterrupted data transmission, even in the presence of network constraints.

C. Elements comprising a LIN Network

The Master Node is responsible for managing the network, coordinating communication schedules, and initiating data frames. Slave nodes are responsible for executing certain operations or sensors in response to master commands. The LIN Bus is a solitary cable that links all nodes and transmits data signals across the whole network.

D. Application Areas

The utilisation of LIN is widespread in several domains such as body electronics, comfort functions, and sensor networks inside automotive configurations. The cost-effectiveness and straightforward deployment of this technology render it an appealing choice for manufacturers seeking to incorporate advanced control mechanisms at a minimal cost.

The diagram depicts a basic LIN network configuration, where the master node is linked to multiple slave nodes by a single cable (the LIN bus). Each slave node is assigned certain vehicle functions, such as window control and mirror adjustment. The communication paradigm employed by LIN is characterised by a simplistic yet effective approach, wherein the master node plays a crucial role in scheduling communication and facilitating the directional flow of data from the master to the slaves and vice versa.

LIN provides an efficient and economical solution for the management of less essential communications within automotive vehicles. The design of this protocol addresses the requirements of the automotive industry, which seeks a lightweight solution that can effectively handle the growing intricacy of vehicle electronics while minimising resource use.

FlexRay

FlexRay is a communication protocol that has been specifically developed to provide a greater bandwidth and enhanced reliability compared to conventional communication mechanisms such as CAN or LIN. FlexRay has been designed to address the growing requirements of contemporary vehicles' sophisticated control systems. It offers support for both time-triggered and event-triggered communication, rendering it highly adaptable for a range of automotive applications, particularly those that necessitate accurate timing and determinism, such as brake-by-wire or steer-by-wire systems.

A. Main Characteristics and Purposes of FlexRay

The Dual-Channel Configuration offered by FlexRay enables the utilisation of two distinct communication channels, which can be employed to achieve redundancy or enhance bandwidth capacity. This guarantees

exceptional dependability and resilience, which is crucial for safety applications.

FlexRay has data transmission rates of up to 10 Mbps, which is considerably higher than those of CAN or LIN. This allows for the transfer of a greater volume of data in a shorter duration.

FlexRay facilitates a hybrid communication mechanism that integrates time-triggered communication for jobs that require prompt response and time-sensitive information, alongside event-triggered communication for the transfer of less critical data.

FlexRay's network architecture provides the capability to be set in diverse topologies, such as bus, star, or a hybrid configuration, hence granting flexibility in the design and implementation of networks.

Deterministic data transmission refers to the process of transmitting messages at certain and specified time intervals. This type of communication is essential for synchronising control operations in sophisticated automotive systems.

B. Summary of Operations

Within the FlexRay network, every individual node functions in accordance with a standardised global schedule that governs the precise timing of data transmission. The implementation of this schedule guarantees the timely transmission of time-triggered messages, hence preventing collisions and promoting determinism within the network. Predefined dynamic segments can be utilised to transmit event-triggered messages, hence enabling adaptability in communication.

C. The constituents of a FlexRay network

In accordance with the FlexRay protocol, the Communication Controller is responsible for managing the transmission and receiving of data. The Bus Guardian is responsible for monitoring network communication in order to prevent any node from breaching the established communication schedule, hence improving the overall resilience of the network. A physical layer refers to the collection of cables and connectors that constitute the physical network, facilitating the connection between nodes.

D. Application Areas

FlexRay finds predominant utilisation in domains necessitating elevated data rates and deterministic communication, such as advanced driver-assistance systems (ADAS), active suspension systems, and other pivotal vehicle control systems.

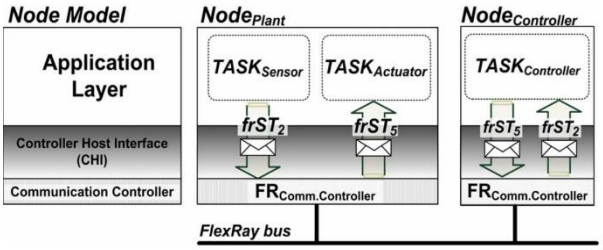

Figure A FlexRay network diagram {Kitadel}

A FlexRay network diagram, envision a structure where many control units (referred to as nodes) are interconnected along two parallel lines, symbolising the dual-channel arrangement. In order to ensure redundancy, certain nodes may be connected to both lines, but others may utilise only one channel. The diagram may incorporate a central control unit that assumes the responsibility of organizing the communication schedule of the network. Every node, which includes sensors and actuators, is illustrated as being connected to this network, emphasizing the transmission of communications that are triggered by time and events.

FlexRay is a significant technological advancement in the progression of automotive communication protocols, providing the necessary attributes of rapidity, dependability, and predictability essential for the forthcoming era of vehicle control systems. Its versatility and effectiveness meet the intricate requirements of contemporary vehicles, facilitating safer and more efficient transportation.

III. METHODOLOGY

A. The CAN Protocol Vulnerability Assessment

The Controller Area Network (CAN) protocol, while widely used for its efficiency and reliability, presents significant security challenges. The analysis of vulnerabilities of the CAN protocol are across three key security aspects: confidentiality, integrity, and availability. The analysis will examine how the lack of inherent cryptographic mechanisms, message

authentication, and robust error management contributes to these vulnerabilities.

1) Confidentiality Concerns

The CAN protocol lacks cryptographic methods to ensure confidentiality, allowing intruders to access sensitive user data and invade privacy [31]. Each message transmitted on the CAN bus is sent to every node, making it easy for a malicious node to listen and read message content, consequently leading to a lack of confidentiality [32]. Furthermore, the absence of suitable security support within the CAN protocol renders it vulnerable to attacks such as CAN bus Denial of Service (DoS) and bus injection attacks, which pose significant threats to confidentiality [33]. The broadcast nature of CAN messages combined with the lack of encryption further worsens the vulnerability, making the protocol susceptible to traffic analysis. This vulnerability enables attackers to passively monitor and collect detailed metrics about CAN traffic, thereby compromising confidentiality [34].

2) Integrity Concerns

The CAN protocol's lack of built-in authentication mechanisms creates significant integrity concerns. This vulnerability opens the door to message injection and tampering attacks by unauthorized actors. Furthermore, the absence of secure key management allows these malicious entities to manipulate or forge messages entirely. Replay attacks pose an additional threat, where intercepted valid messages can be retransmitted, leading to unauthorized actions or data corruption. Compounding these issues, the lack of message source authentication makes the CAN protocol susceptible to impersonation attacks. In such scenarios, attackers can masquerade as legitimate nodes and inject malicious messages. Finally, the CAN protocol's limited error management capabilities can also impact integrity. Errors caused by external disturbances or hardware faults can lead to the transmission of erroneous messages, further compromising data integrity [35], [36].

3) Availability Concerns

The CAN protocol's reliance on a priority-based messaging system has availability concerns. When a high-priority message is transmitted, it can effectively block lower-priority nodes from accessing the network, hindering their ability to send critical messages. This directly violates the principle of availability. Furthermore, the lack of comprehensive integrity checks within the CAN protocol exacerbates availability issues. The protocol's current Cyclic Redundancy Check (CRC) is insufficient to prevent malicious data injection. When attackers exploit this weakness, the accuracy and validity of data are compromised, potentially leading to disruptions in system operation and reduced availability [31].

Attacks such as CAN bus Denial of Service (DoS) can disrupt the availability of the CAN bus by overwhelming it with high priority messages, preventing the transmission of messages from other Electronic Control Units (ECUs).

Finally, the absence of fault-tolerant mechanisms in the CAN protocol can lead to availability issues in safety-critical applications. System failures caused by external factors or hardware malfunctions can disrupt communication and lead to potentially severe consequences [33].

B. Automotive Attack Surface Expansion

The expanding complexity of modern vehicles opens the door to a wider range of security threats. There are two primary attack categories: physical and remote. Physical attacks focus on exploiting the Controller Area Network (CAN bus), the vehicle's internal network, often through the On-Board Diagnostic (OBD) port. The analysis will explore how attackers can manipulate brakes, engines, and even disrupt the network entirely. Remote attacks target the vehicle's wireless interfaces like Bluetooth and cellular networks. This section will investigate how attackers can exploit these interfaces for unauthorized access, including compromising in-vehicle systems and manipulating software updates [31].

1) Physical Access Attacks

Physical access attacks on automobile systems need direct communication with the network systems of the car, frequently by installing unauthorized devices within the car's network architecture or by using exposed ports. Among these assaults are:

On-Board Diagnostics (OBD) Ports Attack: The OBD port is a main target for attackers since it

provides a direct path to the vehicle's network. Attackers have the ability to manipulate a number of vehicle modules, including crucial ones like engine and brake control, by taking advantage of the OBD port. They have the ability to alter engine parameters, release brakes, stop brake activation, manipulate instrument clusters, and even turn off the engine while the car is moving.

Selective Denial-of-Service (DoS) Attacks: These attacks attempt to interrupt the network without transmitting whole messages. They can be executed by overwriting specific bits of transmitted data, causing transmission problems and abusing the CAN standard's vulnerabilities. Research in this arena has been essential in exploiting these vulnerabilities, which led to government alerts and raised awareness of the susceptibility of cars to such attacks.

Indirect Physical Access Attacks: In contrast to direct attacks, these do not require access to the vehicle's network. For example, hacking a car service's IT system can provide them indirect access to the CAN network. Furthermore, attacking via multimedia devices like as CDs, USBs, or MP3 players, while not directly breaching the CAN, can cause the driver to display warnings on the screen or play alarm signals.

The interpretation of these attacks underscores the critical need for robust cybersecurity measures within automotive systems to safeguard against unauthorized access and manipulation of vehicle networks [37].

2) *Remote Access Attacks*

The integration of numerous wireless interfaces into modern vehicle systems, such as anti-theft measures, Tire Pressure Monitoring Systems (TPMS), Bluetooth, and telematics units, has increased the vulnerability to remote access cyber-attacks. The vulnerabilities highlighted are:

Wireless Interface Exploitation: These interfaces, which connect to the Controller Area Network (CAN) via gateway Electronic Control Units (ECUs), present substantial security threats. Hackers have exploited such weaknesses to gain unauthorized access and remotely modify numerous vehicle functions, including door unlocking.

OTA Update Vulnerabilities: The ease and cost-effectiveness of Over-the-Air (OTA) software upgrades adds another layer of susceptibility. Malicious actors may intercept these updates, corrupting the vehicle's communication network and resulting in ransomware attacks or other cyber-sabotage activities.

V2V and V2I Communication Risks: The rise of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, which are critical for vehicular ad hoc networks (VANETs), has revealed new vulnerabilities. These systems, which are intended to optimize traffic and prevent collisions, could be endangered by faked communications, causing in-vehicle communication networks to malfunction.

This thorough investigation emphasizes the increasing risk posed by the incorporation of wireless connections into current automobiles, identifying potential channels for illegal access and control by malevolent actors. The referenced journal paper provides an in-depth assessment of these vulnerabilities as well as ideas for strengthening cybersecurity in automobile systems using cutting-edge approaches [38].

C. *Automotive Attack Surface Expansion*

In-vehicle network system attacks can be categorized based on their entry points: sensor-initiated, infotainment-initiated, telematics-initiated, and direct interface-initiated [33].

- Sensor-initiated attacks exploit vulnerabilities in vehicle sensors, manipulating data to cause malfunctions or false readings.
- Infotainment-initiated attacks target the infotainment system, aiming for unauthorized access and control of its functionalities.
- Telematics-initiated attacks focus on exploiting vulnerabilities in the telematics system

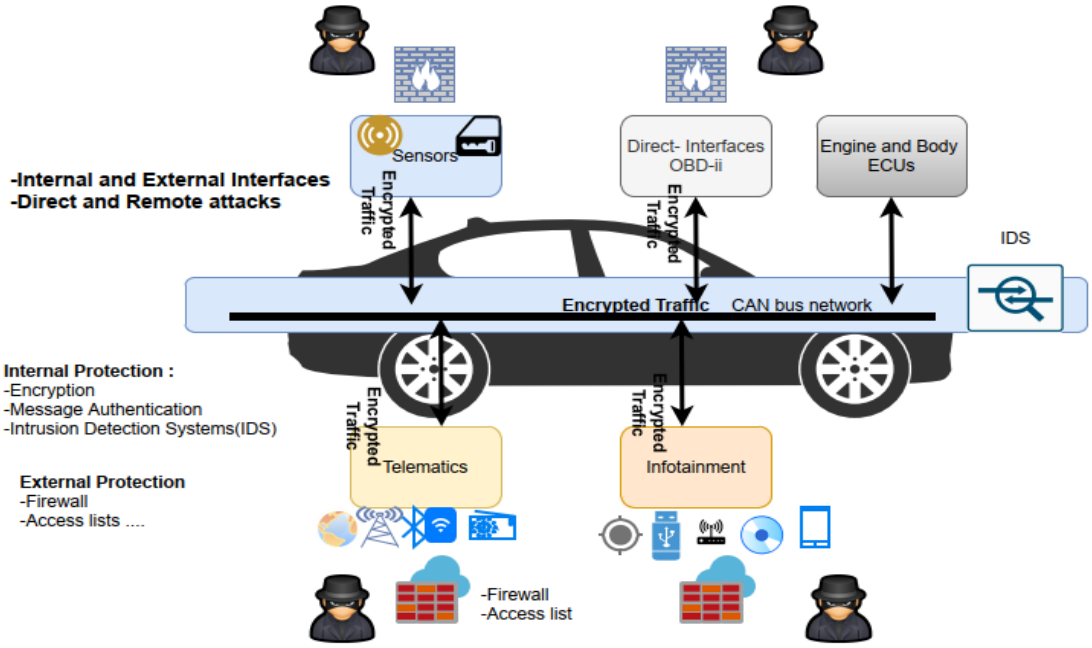

Figure: Four attack vectors for data manipulation in connected cars: Telematics, Infotainment, Direct Interfaces, Sensors. [33]

(communication and navigation) to gain unauthorized access or manipulate data.

- Direct interface-initiated attacks exploit vulnerabilities in communication interfaces (e.g., OBD-II port) to access internal networks and compromise Electronic Control Units (ECUs) [35].

Attackers leverage various methods to gain access, including wireless and physical access, exploiting software bugs, remote keys, and other vulnerabilities in ECUs [33].

These vulnerabilities in communication protocols like CAN bus and Automotive Ethernet (AE) create openings for a range of attacks. The CAN bus is susceptible to bus-off, denial-of-service (DoS), masquerading, injection, eavesdropping, and replay attacks [35]. Similarly, attackers can launch traffic integrity, confidentiality, access, and DoS attacks against Automotive Ethernet [33].

IV. Attacks in a In-Vehicle Network

A. *Eavesdropping Attacks*

Eavesdropping attacks happen when people who aren't supposed to, can listen in on car messages.[1] Since the car network sends out messages for anyone on the network to see, once these attackers get into the car's network, they can secretly listen to these messages. They can even start to notice regular patterns in the messages that are supposed to be private.

Data that do not match the rest of the dataset's data are known as outliers [2]. Anomalous data concealed within a typical data collection is identified by outlier detection. Anomaly detection is comparable to a classification challenge in certain ways. There are two types of network flow: normal and aberrant. Finding the most suitable type for the observed data stream is our aim. The conclusion that follows is that anomaly detection works better at identifying variants of known assaults than it does at identifying new malicious activities [3]. In this situation, the system can be taught using frequent background traffic and known attack samples to facilitate a more dependable decision-making process.

B. *TPMS Exploitation*

The Tire Pressure Monitoring System (TPMS), which lack of crucial security measures, is a well-documented target for attack. One can target the tire pressure monitoring system (TPMS) passively or actively. The TPMS interfaces with the vehicle's Electronic Control Unit (ECU) and continuously checks tire pressure. While active attacks use

wirelessly injected spoof signals to fool the ECU, passive attacks use captured TPMS signals to track the movement of the vehicle. False tire pressure readings may be displayed as a result of these attacks, putting the safety of the vehicle at serious risk. To overcome these vulnerabilities, countermeasures include using encrypted signal transmissions and hardware pairings.

Approximately three miles of wire are present in modern cars, and as we add more on-board electronic components, such as entertainment systems, navigation systems, and in-car sensors, to make our cars smarter, the amount of wire in them will only grow. Car weight and wiring complexity are directly impacted by an increase in wires, which reduces fuel efficiency and makes troubleshooting more difficult. Because of this, wireless technologies will be utilized more often inside and outside of cars to gather status and control information about their electronics.

The procedures will considerably reduce the security risks associated with TMPS and include recommendations for cryptographic protocols along with relatively simple design adjustments. The creation of additional new wireless in-car sensing systems can profit from the knowledge gained. [4] classification challenge in certain ways. There are two types of network flow: normal and aberrant. Finding the most suitable type for the observed data stream is our aim. The conclusion that follows is that anomaly detection works better at identifying variants of known assaults than it does at identifying new malicious activities.[3]. In this situation, the system can be taught using frequent background traffic and known attack samples to facilitate a more dependable decision-making process.

C. *Lockpicking Attack on Keyless Entry Systems*

The lock picking attack takes use of a weakness in keyless entry systems, which are commonly utilized for garage openers and automobile doors. Using a gadget that intercepts the key fob's sent signal and simultaneously transmits a jamming signal on the same frequency, the attack employs a man-in-the-middle technique. The attacker's device records the second code transmission when the key fob user attempts again, allowing it to open the door with the first code and store the second code for future illegal entry. Sales of these devices have increased despite their general availability and potential for misuse, raising worries and leading manufacturers to demand for stronger security measures.

One of the earliest methods is fixed-code RKE, in which a key fob transmits the instruction along with a predefined authentication code. While fixed-code RKE makes design and manufacturing simpler, replay assaults can easily exploit it. To put it another way, it would be quite simple for an attacker to intercept the broadcast signal, extract the predefined code, and then utilize it to get unauthorized access. In order to get around the fixed-code RKE's limitations, rolling code RKE was created [5]. Rolling-code RKE uses a synchronized counter that is kept in sync between the key fob and the receiver to determine the authentication code that the fob should broadcast at each connection attempt, or press. The fob communicates an encrypted version of the current counter value on each attempt, incrementing it once the transmission is complete. The value of the synchronized counter is retrieved by the receiver using code decryption, and it is then compared to the value of its own counter. The receiver's counter value is increased and the fob is verified to execute the desired action if both matches. It is important to remember that the secret key that is needed for both encryption and decryption is never shared. The receiver matches not only the current counter value but also a few more following ones in order to resolve this issue. To get back into in sync, the receiver changes the counter value in accordance with any matches it discovers. Lastly, the code will be rejected and the fob will not be verified if the recipient receives a counter value that is less than expected.

D. *Denial of Service(DoS)/Distributed Denial of Service(DDoS) Attacks*

DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are malicious attempts to disrupt the normal operation of a computer system, network, or service by overwhelming it with a flood of illegitimate traffic or requests. Autonomous vehicles (AVs) rely heavily on communication systems for real-time data exchange, therefore Avs

are connected to different communication routes. These include Vehicle-to-satellite, vehicle-to-vehicle (V2V), vehicle-to-internet, and other communication technologies. Furthermore, internal communication is facilitated by the controller area network (CAN). If any of these communication channels are disrupted, the vehicle may not be able to operate correctly and may become blind to its surroundings. DoS attacks allow attackers to prevent the camera from identifying objects, roads, and warning signs[19]. DoS assaults may harm the braking system, causing the car to stop suddenly or not at all[19].

A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet DDoS attacks are carried out with networks of Internet-connected machines. These networks consist of computers and other devices (such as IoT devices) that have been infected with malware, allowing them to be controlled remotely by an attacker.

E. ***Bus-off Attacks***

Using the CAN protocol's error-handling characteristics, a bus-off attack compels the target node to enter the bus-off state. In the bus-off state, a node cannot transmit/receive any messages[17]. A bus-off attack aims for the frame collisions.

Under CAN, every node can send a message while the bus is idle. CAN is unable to transmit multiple messages simultaneously. Thus, to prevent message collisions, the other nodes wait for transmission while one node starts transmission. When a bus-off attack is used to transition a target ECU identified by a specific CAN ID to a bus-off state, the authorized transmission ECU is unable to recognize the spoofing message[18]. At this point, spoofing messages are sent by the attacker within the same cycle as the regular message. The receiving ECU is unable to recognize the spoofing as a result. Identifying anomalies from the receiving frequency is impossible since the receiver ECU only gets the spoofing message[18].

A couple of requirements had to be satisfied for the attack to succeed: synchronization with the victim's message and message ID matching the victim. The attack is performed by detecting a unique message that precedes the victim [18]. However, if there is no unique pre-ID, it has been suggested to prepare and inject unique pre-IDs to disrupt the transfer of the victim.

F. ***ECU Impersonation Attacks***

Before we delve into the topic of impersonation/spoofing attacks on an ECU, we need first to understand the significance of an ECU in a CAN bus. As described by M. J and K. C (2021), an Electronic Control Unit or ECU is a component in every single vehicle [7]. Every vehicle comes with ECU nodes and each of them is designed to task one specific task, for example, to monitor the seat-belt status, or to check the temperature, humidity, or altitude of the vehicle. A single higher-powered controller computer then takes the data from the ECU nodes and runs an algorithm to verify the messages. On the other hand, in a CAN bus, in case of an error, an ECU sends an error frame to inform other ECUs in the network. Once the error is detected by the controller, it increases the bits of TEC and REC.

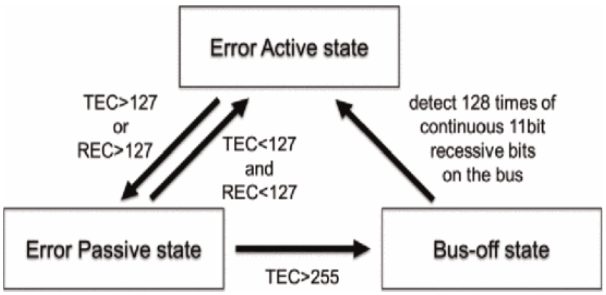

Figure: CAN bus state transition[7]

In the paper “Spoofing attack using bus-off attacks against a specific ECU of the CAN bus” by K. Iehira, H. Inoue, and K. Ishida (2018), they have described a spoofing attack method that cannot be detected by the controller [9]. The proposed attack forces a legitimate ECU into a bus-off state, where it is unable to transmit or receive any messages, thus preventing the controller from detecting spoofed messages injected by the attacker. This happens due to the attacker causing errors in the messages from the authorized ECU, thus transitioning it into an off-state, and injecting the spoofed messages onto the CAN bus.

Mimicking the cycle and the IDs of legitimate messages, the attacker’s spoofed messages go

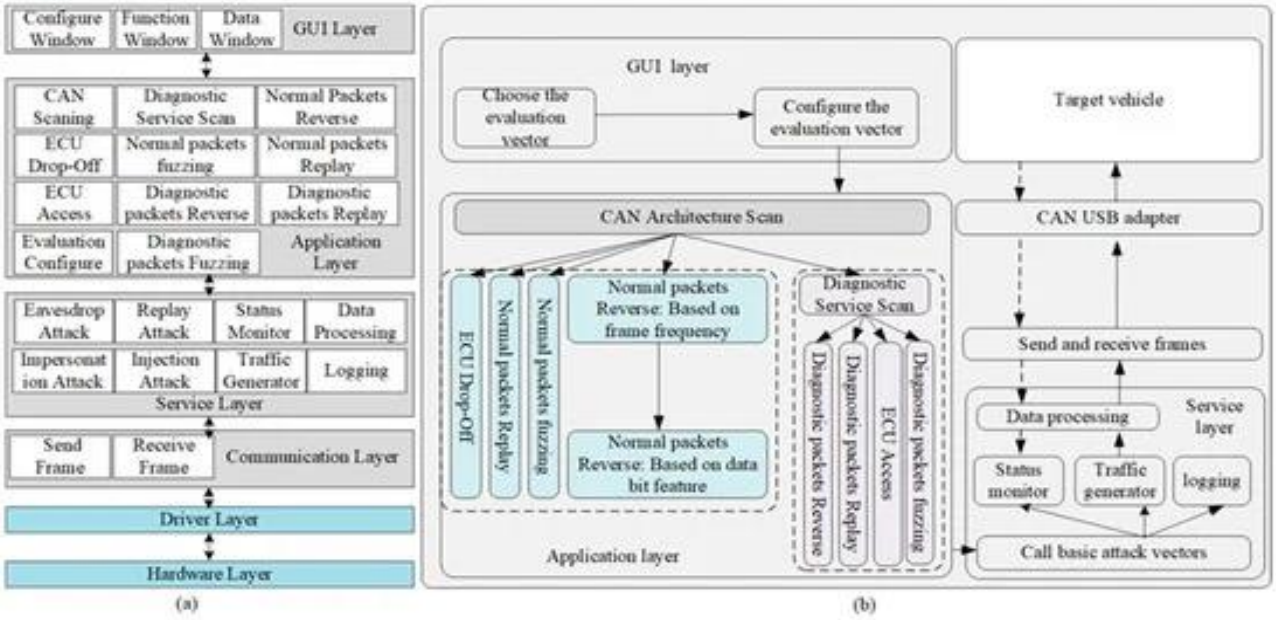

Figure: CANsec Architecture [12]

unnoticed, which in turn compromises the integrity and safety of the vehicle's network. This can result in false readings from the ECU nodes and result in fatal errors in extreme cases. The impersonation attack in this case is successful as there's no authentication process and doesn't have any way to identify the source of the message.

To mitigate these types of attacks, a study by Yang Y et. al (2020) proposes a deep learning model for detecting spoofing attacks in-vehicle CAN networks, thus utilizing a theoretical framework of the CAN physical layer to authenticate data frame IDs [8]. By using extensive simulated CAN signal data, they apply a recurrent neural network (RNN) with long short-term memory (LSTM) to identify deep features of CAN signals and pinpoint malicious ECU nodes. However, they also note that their work still has a long way to go to be implemented in a real-life scenario, as they would need the model to work in a real-time setting and need data from a diverse dataset of real CAN bus signals.

G. *The Jeep Cherokee Attack*

The Jeep Cherokee cyberattack by Charlie Miller and Chris Valasek truly bridged the gap between modern automotive technology and cybersecurity. This eye-opening event has revealed that the connectivity we enjoy in vehicles also opens doors to potential cyber intrusions [13].

Following this revelation, there's been a concerted effort within the automotive industry to fortify the digital defenses of vehicles [14]. As for safeguarding tactics, there's a growing focus on implementing multi-layered defense mechanisms. This includes segregating critical vehicle networks, ensuring the integrity and confidentiality of firmware updates, and adopting the principle of least privilege to minimize potential attack surfaces. These measures are non-trivial, given the complex and proprietary nature of automotive systems, which vary significantly across different manufacturers and models [15].

The computational prowess needed to mount such an attack is considerable but within reach of skilled hackers, given the advancements in technology [15]. More challenging, however, is the intricate knowledge required to navigate the proprietary systems of various vehicles, which adds a layer of complexity to the execution of widespread attacks.

This attack has started a broader awareness and action within the automotive sector, driving home the point that vehicle safety now transcends the physical into the digital realm. The combined efforts towards establishing industry-wide cybersecurity standards exemplify the proactive steps being taken to safeguard modern vehicles against cyber threats [14].

H. *Replay Attacks*

Replay attacks represent a significant security threat to the CAN in vehicles. In such attacks, attackers capture valid network communication and replay it to induce unauthorized actions or responses from the network. This type of attack exploits the CAN's lack of built-in security features like authentication and encryption, which were originally omitted to keep the network lightweight and efficient [12]. The CAN was designed in a time when in-vehicle networks were not exposed to external connections, making security less of a concern. However, with the increasing connectivity of vehicles, including the Internet of Things (IoT), vehicle-to-x communication, and over-the-air updates, the potential for cybersecurity threats, including replay attacks, has significantly increased.

One practical approach to evaluating and mitigating the risk of replay attacks on CAN is the use of a security evaluation tool like CANsec. This tool can monitor changes in vehicular status, log evaluation activities, and replay captured CAN frames to test the vulnerability of the network to replay attacks. Experiments conducted using CANsec on a vehicle revealed that the replay attack was indeed effective against the vehicle's instrument panel, demonstrating the capability of such attacks to manipulate vehicle functionalities like engine speed, turn signals, door status, and wipers. The success of these attacks highlights the inherent security vulnerabilities of the CAN bus broadcasting mechanism.

To mitigate the vulnerabilities exposed by replay attacks, a secure boot scheme has been proposed as a mitigation strategy. This scheme utilizes cryptographic data integrity algorithms to ensure that only authentic and untampered software can run on the vehicle's ECUs. The presence of malicious code in one or more ECUs is a common root cause of CAN bus attacks, and secure boot schemes can effectively prevent the execution of such codes. Testing and comparison of different data security algorithms implemented on a hardware security module (HSM) demonstrated that certain schemes, such as the secure boot with the cipher-based message authentication code (CMAC) and the secure boot with the elliptic curve digital signature algorithm (ECDSA), offer a favorable balance between security level and performance. A novel variation of the ECDSA algorithm based on the CMAC algorithm also showed a 19% performance improvement over the standard ECDSA-based secure boot scheme [12].

I. *Malicious Diagonstic Applications*

Another prominent way of attacks these days is gaining control of the vehicle by attacking the CAN bus through malicious apps. The apps are specifically designed for infiltrating the vehicle’s network, exploiting the vulnerabilities, and allow the hackers to gain control of the CAN bus to send unauthorized signals. Recently one of the most infamous examples was the Jeep Cherokee attack where the researchers took control of the vehicle via cellular network [13]. Another notable mention involves Tesla, where the security experts identified and exploited vulnerabilities to remotely execute unauthorized malicious attacks, showcasing the critical need for security measures in modern-day vehicles [16].

Simple tasks like sending false signals can be done pretty easily and need minimal resources like a smartphone or a laptop with an internet connection. Incidents like these remind vehicle owners to be more vigilant about the apps they install on their devices and ensure they come from reputable sources and are kept up-to-date with the latest security practices.

J. *CAN Bus Specific Attacks*

Cars can be vulnerable to attacks if someone gets access:

CAN Sniffing: This is when attackers quietly watch the data moving through the car's CAN system. They use special tools to understand this data and can then create fake messages that look real.

CAN Fuzzing: In this case, attackers send random data to the car's CAN system to see what happens. This can cause unexpected changes, like the car speeding up or slowing down, because the system gets confused by the strange messages.

There are various ways to defend against assaults on CAN bus systems in automobiles. Encrypting data transferred over the CAN bus is a crucial strategy to prevent attackers from understanding or replicating the messages. Strict access control

implementation can also restrict who is able to connect to the CAN system, lowering the possibility of unwanted access. Frequent monitoring and anomaly detection can aid in the early detection of aberrant behavior, enabling prompt intervention.[6] Lastly, increasing general security can be achieved by teaching car mechanics and users about these threats and countermeasures.

K. ***Road Infrastructure Attacks***

Road infrastructure components are now vulnerable to potential cyber-attacks due to the growing connection of automobiles. New attack vectors are presented by vehicle-to-infrastructure (V2I) connectivity, which includes components like smart traffic lights and road signs. In one famous case, networked traffic signals across several states were compromised and began to show messages indicating they had been hacked. Even though these attacks are first thought of as jokes, they have significant consequences, particularly in times of need. Tight password management and secure sensor design for V2V and V2I communications are necessary to mitigate these threats.

Implementing multiple approaches focused on at reducing potential threats is essential when solving road infrastructure security. This includes putting in place surveillance devices to keep an eye out for any odd activity. Additionally, the establishment and implementation of strict regulatory structures function as a barrier against intentional acts of damage. Campaigns for public education and awareness are essential because they give the public the skills necessary to identify and report such risks. Additionally, securing against and quickly recovering from attacks depends critically on the incorporation of technology into infrastructure design, including resilience-enhancing elements. To create a safe and responsive environment for road infrastructure, law enforcement, governmental organizations, and the community must work together.

L. ***Manipulating Vehicle Communications***

AD operations may be disrupted by hijacking and manipulating communication channels. Attackers can manipulate critical control systems within the vehicle, such as the engine, brakes, steering, sensors, or acceleration. As a result, a vehicle may act differently from what was planned or designed for it. Attackers can exploit manipulated communications to facilitate unauthorized access to vehicle electronic control units (ECUs) or the roadside unit (RSU)[19]. For instance, remotely unlocking doors, disabling alarm systems, or starting the engine can aid in stealing the vehicle or its contents.

For manipulation, it is required for the attacker to get access to the vehicle network. The attacker can use the TPMS for an eavesdropping attack to get access to the vehicle network and perform malicious activities [8]. The majority of smart vehicles are equipped with Wi-Fi, allowing them to connect to the internet via Wi-Fi hotspots located along roadsides. However, the low level of security at these hotspots poses a significant risk, as they may utilize outdated security protocols, making vehicles vulnerable to various threats. Hackers can exploit these weak access points to target vehicles effectively [24].

M. ***Manipulation via OBD-II Ports***

Attackers can gain entry to the in-vehicle network through OBD-II ports, compromised ECUs, or infotainment & telematics systems[20].

OBD-II ports are vulnerable to in-vehicle network access attacks and dongle exploitation attacks.

In-vehicle network access attack: In instances of in-vehicle network access attacks, attackers exploit vulnerabilities by inserting an external device into the OBD-II port, thereby gaining access to the in-vehicle network. OBD-II ports serve as significant weak points in vehicular security, facilitating the extraction of diagnostic data, access to the in-vehicle network, and installation of malware[21]. Valasek and Miller [22] demonstrated the ability to send and receive messages over the Controller Area Network (CAN) by utilizing an ECOM cable and self-made connectors to link with the OBD-II port.

Dongle exploitation attack: Dongles inserted into the OBD-II port can be remotely controlled and are susceptible to decryption [23]. An example of such a dongle is the Bosch Drive-log connector, designed to monitor vehicle maintenance and provide guidance for servicing by connecting to the vehicle's OBD-II port. This dongle was

compromised when the Argus Cybersecurity firm executed a brute-force attack, allowing them to establish a Bluetooth connection and send harmful messages through the Controller Area Network[20]. These transmissions ultimately caused the engine of a moving vehicle to fail[20].

To connect to ODB-II port, special hardware is required, that is often compact yet capable of powerful interfacing with the vehicle's internal systems. Additionally, some vehicles feature wireless connectivity to the OBD-II port, allowing remote access for diagnostic and software updates. However, this also opens up the possibility of remote cyberattacks if proper security measures are not in place. Another way to exploit ODB-II port is by malwares, these can be injected into the vehicle's onboard systems through the OBD-II port, either via physical connection or remote access.

V. COUNTERMEASURES & MITIGATION TECHNIQUES

A. ***Existing security measures and their effectiveness***

Over the past decade, scholars have delved into a broad spectrum of strategies aimed at safeguarding computer and mobile systems from malware. These strategies encompass signature-based, behavior-based, heuristic-based, cloud-based, and machine learning-based methodologies. In this segment, we offer an exhaustive examination of the key elements involved in implementing these protective measures to shield smart vehicles from malicious software. These elements encompass the chosen approach, data analysis techniques employed, targeted operating system, detection speed and response, data sources, as well as the primary merits and drawbacks associated with each defense mechanism. We divided the taxonomy dimensions into six categories. Furthermore, we provide concise descriptions of these categories below.

Methodologies: We categorize the prevailing methods for detecting malware into five distinct groups: signature-based, behavior-based, heuristic-based, cloud-based, and machine learning-based techniques. Each of these methodologies presents its own set of advantages and disadvantages, which we thoroughly examine to understand the strengths and limitations of each approach.

Analysis Approaches: The entirety of the detection procedure employs static, dynamic, and hybrid analysis methods. Below, we delineate each method:

Static Analysis: This methodology involves analyzing executable code without executing it. In static analysis, low-level information from codes is extracted through disassembly using disassembler tools. The primary advantage of this approach is its ability to unveil the code structure of the program without actual execution. Nonetheless, it may falter when confronted with analyzing unknown malware or detecting malware that employs obfuscation and evasion techniques within its code.

Dynamic Analysis: This malware analysis method involves executing the malware and observing its behavior, interactions with the host system, and effects on the host environment. The infected files are scrutinized within a simulated environment, such as an emulator, virtual machine, or sandbox, to render the environment imperceptible to malware. While this approach is effective in detecting malware, it may still fall short in identifying malware that utilizes obfuscated code and evasion techniques.

Hybrid Analysis: This malware analysis method integrates both dynamic and static analysis techniques. It comprehensively assesses the static attributes of malware code and augments them with behavioral characteristics to enhance the overall analysis process. While this method can effectively address the limitations of both static and dynamic analysis approaches, it may incur an increase in total execution time overhead.

Target Operating System (OS): This term denotes the operating system under scrutiny by the system. It may include LINUX, Windows, or Android, depending on the context of the analysis.

Detection Time: This term denotes the duration between the occurrence of the analyzed event and

the actual detection of the threat. Detection time can be categorized into real-time (online) detection, where automatic responses such as blocking the attacker and terminating the malware process are enabled immediately, or non-real-time (offline) detection, which occurs after the event has transpired.

Detection Response: This refers to the consequential action taken by the system upon detecting a threat. It can be passive, involving an event notification such as displaying an alert message, or active, involving an automatic reaction such as blocking the attacker or terminating the malware process.

Data Source: This indicates the origin of the input data analyzed by the system. It may include hosting logs, which comprise data from the operating system and system applications; application logs, which consist of data directly generated by applications; or network traffic, which encompasses data generated by the network layer.

B. *Existing Detection Techniques effectiveness*

Malware detection system taxonomy Signature-Based Malware Detection: The signature-based approach to malware detection, widely employed in commercial antivirus solutions, consists of two primary phases. Initially, a distinct signature is generated for each malware instance, obtained through a combination of manual and automated analysis of data sourced from networks and user devices. Subsequently, these signatures are stored on devices for identifying malware in files or data streams. This method involves dissecting and examining malware binary codes and is straightforward, rapid, and secure, particularly for smart vehicles. While it excels at detecting known malware, it falls short in identifying novel threats due to susceptibility to evasion. In contrast, novel malware detection methods focus on digital traces in various log files and utilize different analysis techniques, such as static analysis, function call graph similarity, and API call sequences. While accurate for known malware, these approaches are limited in detecting unknown threats and are unsuitable for real-time applications, such as those in intelligent cars.

Additionally, scientists have investigated several advanced methods for detecting malware, with a primary focus on the Windows operating system. These approaches involve examining program binary files without executing the code (static analysis) and utilizing distinct markers such as control flow graph signatures and byte sequences from executable files.

Behavior-Based Malware Detection: This approach examines a program's actions to determine whether or not it is malicious. It accomplishes this in a secure environment, such as a virtual computer, and doesn't rely on external frameworks for new, undiscovered malware. Many use this tactic to combat malware, observing typical behaviors and employing information indicators on various operating systems. Despite having a high locating rate, it is inappropriate for sophisticated vehicles due to its large costs and complexity. Although it is successful in identifying new malware, it struggles to accurately arrange all conceivable behaviors, which may lead to false positives or negatives. In contrast to recognition based on signatures, it is more difficult to implement and take seriously for in-vehicle gadgets, posing challenges for long-distance vehicles use.

Machine Learning Based Malware Detection: Artificial intelligence has long been a crucial tool in the fight against malware, utilizing algorithms with different specialties like logistic regression, Bayesian networks, and Naive Bayes. A number of variables, including feature relationships and data distribution, affect how effective these algorithms are. An increasingly powerful technique is Deep Learning, a subtype of artificial neural networks, particularly in image processing, speech recognition, and, more recently, malware detection. Its vulnerability to avoidance and evasion strategies, as well as the lengthy process of creating hidden layers, highlight the necessity for careful implementation.

Heuristic-Based Malware Detection: The heuristic-based method for discovering malware

involves examining program files for suspicious attributes or simulating program execution to identify potential malicious activities. This approach, renowned for its complexity, relies on past experiences and utilizes techniques such as data mining, rule-based systems, and AI to understand program characteristics. Widely used in antivirus software, it is capable of detecting various known and unknown malware, including zero-day threats. However, it struggles with identifying the most new and sophisticated malware and is susceptible to advanced techniques such as code obfuscation and evasion. Researchers have suggested static analysis techniques, such as control flow charts, and dynamic methods using DLLs or API call patterns. Although effective for known malware, these approaches are intricate, have high false positive rates, and are not suitable for continuous detection due to their time-consuming nature. Despite its strength in identifying unknown malware, the heuristic-based method is challenging and resource-intensive compared to signature-based and behavior-based strategies. It may not be suitable for resource-constrained in-vehicle devices due to their complexity and potential obsolescence over time.

Cloud-Based Malware Detection: Distributed computing has gained popularity due to its convenient accessibility, on-demand capacity, and cost-effectiveness. Recently, it has been employed in malware detection through the Cloud-based approach, utilizing agents located on cloud servers. This method enables users to submit files for analysis and receive reports on their malware status. While it enhances detection performance with extensive databases and computational resources, it encounters drawbacks such as reliance on a stable and fast internet connection, vulnerability to continuous file monitoring, and susceptibility to obfuscation and evasion techniques.

Researchers have explored cloud-based strategies for malware analysis, utilizing static analysis with features such as document content and relationships, as well as dynamic analysis through system call monitoring. However, these approaches incur significant costs and time delays, rendering them inadequate for continuous detection, particularly in smart vehicles. Despite the advantages of rapid access and updated installations, the cloud-based approach is hindered by the need for a reliable internet connection and vulnerability to advanced evasion techniques, raising concerns about its safety in smart vehicles. The emergence of high-speed 5G technology might enhance its feasibility in this specific context.

C. Attack Identification

Although a lot of work has gone into keeping malicious actors out of the automotive CAN, it is impossible to stop every kind of unidentified assault. Finding a new assault and a compromised ECU is therefore important, and this can be done via data logging CAN traffic. When an attack takes advantage of a stealth characteristic like Stuxnet, data recording by itself is insufficient to identify a compromised node completely; therefore, attestation could also be used to identify a compromised node.

I) Data Logging: For a data recording system, an information set consisting of CAN ID, packet arrival time, and domain ID (such as powertrain, comfort, and infotainment) should be well maintained. But because an attack attempt could readily taint this data set, it is insufficient to identify the source ECU from which a genuine automotive CAN assault was carried out. Stated differently, this set lacks unique data, such as digital fingerprints, such as electric CAN signal information. For instance, if a compromised ECU carried out message flooding assaults with the CAN ID of 0 × 00, details regarding the CAN ID and packet arrival time recorded in the logging system might be utilized to examine the characteristics (such as attack packet frequency) of the message flooding attacks. The logging system still has trouble figuring out which ECU has been used in message flooding attacks. One crucial and required step in a quick and effective response to an attack is identifying a hacked ECU. From there, a security patch or isolation technique can be applied to the affected ECU. A voltage-based ECU identification system that would use voltage measurements to fingerprint ECUs' CAN transceivers will be used, in order to satisfy this

testing on two actual cars that their logging system can detect a corrupted ECU with a mere 0.2% false positive rate. To guard against forgery attacks, a trusted execution environment (TEE)-based logging system was recently proposed.

II) Attestation: The verifier is tasked with attestation of all ECUs on automotive CAN. to a particular device or another ECU to verify the integrity of the firmware that is placed on every ECU. As a result, an attestation code and a distinct attestation key ought to be installed in each ECU of a vehicle at production, together with a specific ECU for verification. When the ignition is turned on, the ECU firmware attestation procedure can be initiated, or it can run automatically anytime the ECU firmware has to be verified.

D. ***Segmenting the network***

One of the main safety measures is to implement network division by dividing the CAN system into subnetworks. This allows for control over access and limits the potential for assaults to spread. The standard procedure in business cars involves an Electronic Control Unit (ECU) on the door that controls connections between subnetworks. However, vulnerabilities arise if the door ECU is breached, as demonstrated in certain hacking scenarios.

E. ***Encryption***

The implementation of a lightweight encryption system is essential since the CAN convention exposes its correspondence to potential enemy eavesdropping in the absence of implicit encryption. Although there are producer-only techniques and encryption strategies based on business programming, publications point to vulnerabilities in commercially available car encryption frameworks. Difficulties with security Could encryption ever include the field for restricted information. That would be problematic for organisations with huge traffic volumes, but it could be handled by providing different CAN outlines for a single message. Furthermore, dynamic key trading is necessary due to the computing requirements of ECUs to prevent static key splitting during the course of a vehicle's life. However, dynamic key trading is unsuitable for security-critical continuous frameworks due to its execution difficulties, computational expenses, and idleness problems for asset-compelled ECUs.

F. ***Secure Boot***

The concept of Secure Boot is not unique to the automobile sector; in fact, the majority of home PC BIOSes support it. It is a Unified Extensible Firmware Interface (UEFI) method that restricts the bootable software on the machine to only those with legitimate signatures. During the manufacturing process, the manufacturer inserts databases containing keys and signatures inside the device. Before booting, the firmware would next be signed and verified by signature. Although malicious firmware cannot be booted thanks to the incredibly powerful security technique known as safe booting, there have been instances in the past when certain implementations' flaws have allowed for bypasses, therefore secure booting is not a foolproof solution.

G. ***Safe Access Program***

As the scientists worked on a 2010 Toyota Prius and a 2010 Portage, they investigated the diagnostics validation component. Break, exposing an ISO 14229-1-characterized Security Access system implanted within the Bound together Diagnostics Administration (UDS). For Electronic Control Units (ECUs) in the automotive industry, UDS serves as a standard diagnostics correspondence convention. It provides many services to collect information on a vehicle's utility and condition. Using a Test Reaction protocol, the Security Access administration requires a "seed" from the ECU, which is then returned to it after it has reached adulthood. An ECU key and a cryptographically secure capability are shared by both the analyzer and the ECU. However, the free standard requires interesting points like the seed age, keys, or competence. Remarkably, vulnerabilities were identified, such as predictable seeds and short reaction times, which let attackers to use beast power or replay attacks. The specialists were able to separate keys efficiently by identifying and locating security flaws in these auto frameworks.

H. ***Secure Onboard Communications***

To address the authentication shortcomings in the Controller Area Network (CAN), the

AUTOSAR community introduced the Secure Onboard Communications (SecOC) module. This module enhances CAN message authentication by adding signatures to in-vehicle communications. SecOC supports both symmetric and asymmetric cryptography, assuming that key management and exchange are already established. The approach involves appending a signature, along with a freshness value for uniqueness, to the protected data unit (PDU) within the CAN frame.

In symmetric mode, for instance, the sender computes a Message Authentication Code (MAC) over the input data and freshness value using a shared key, attaching it to the message. The receiver verifies the freshness value and recalculates the MAC, accepting the message if correct. However, adapting this system to a standard CAN framework presents challenges, such as truncating the 128-bit MAC into a 27-bit value, potentially vulnerable to brute force attacks.

Additionally, SecOC introduces measures to safeguard against replay attacks by including freshness values in the data packets. These values help to ensure that each message is unique and has not been intercepted and replayed by an attacker.

An alternative approach, the Plug and Secure Key Establishment (PnS), offers a low-cost symmetric key establishment protocol for CAN. It utilizes a physical property in the bus to establish a key between two devices whenever they communicate a frame simultaneously, enhancing security within the network.

I. Firewall Gateway

Enhancing security in in-vehicle communication systems may involve implementing a firewall mechanism within network gateways. If Message Authentication Codes (MACs) or digital signatures are utilized for authentication and validation between Electronic Control Units (ECUs), firewall policies can be derived from the permissions specified in each ECU's certificate. In cases where MACs or digital signatures are absent, firewall rules can be individually defined based on vehicular subnet permissions, allowing only messages from legitimate and authenticated ECUs to pass through and be transmitted across the in-vehicle communication system.

Another approach is to restrict the access level of different network types to specific segments of the communication system, preventing less critical networks, such as LIN or MOST, from sending messages to higher safety-critical systems, such as CAN or FlexRay. This helps in segregating and protecting critical communication channels from potentially less secure ones, thereby enhancing overall system security.

J. Segmenting the network

Securing in-vehicle communication systems is crucial due to the vulnerability introduced by wireless communication gateways. Attackers can exploit remote access to launch cyber-attacks directly on the in-vehicle network, which controls essential vehicle functions. Understanding attackers' behavior is essential for developing effective security solutions. Honeypots, designed to appear as vulnerable targets, serve as tools for the prevention and early detection of malicious attacks. In the automotive sector, realistic honeypots can be deployed to attract genuine attackers without disrupting normal vehicle operations. These honeypots collect data as the vehicle travels through predetermined areas, capturing information affecting the in-vehicle network. Analysis of this data identifies attack patterns, scenarios, and commands, aiding in the development of robust security measures to protect in-vehicle communication systems in future designs and implementations.

VI. Conclusion

The increasing dependency on computer systems of cars requires the security machines against the cyber-attacks to be significantly revised. On the other hand, the electronic components inside a car are linked in this way by the networks, which have no fundamental difference in this respect from say the hydraulic system of an aircraft. The main issue here is the CAN protocol which might contain different vulnerabilities (attack vectors) that in their turn may result in serious risks.

For instance, eavesdropping on CAN messages , message forgery, service outage because of

excess traffic, assuming legitimate identity of driver/vehicle, and infamous Italian job hack through cellular connection demonstrate the pressing need to enhance security in automobiles. These hacks, especially, demonstrated that hackers can manage to access the critical vehicle functions without permission and the invasion of privacy. Also, it prioritizes that cybersecurity risks should not be ignored.

In order to enhance the safety of the car cyber security, the appropriate countermeasure and mitigation methodologies must be kept in mind. Besides adding new security solutions, further development already involves the recognition of threats according to well-known patterns, analyzing system behaviour for any suspicious activity, or making general rules to detect anomalies. It should also be noted that techniques such as cloud and machine learning are currently being studied. Such strategies look for anomalies in data by the keyword and block cyber-attacks. Greater security is required to connect devices like Bluetooth and Wi-Fi, on OBD-II, and defend vehicle sensors and actuators from physical attacks, senses prevention of signal blocking and jamming and relay attacks on systems such as LiDAR and keyless entry. Besides, the installation of security protocols is an undoubtedly unavoidable measure for the purpose of decreasing cyber risks that are aimed at vehicle communication networks.

REFERENCES

[1] J. Liu, W. Sun, Yongpeng Shi, In-vehicle network attacks and countermeasures: challenges and future directions, IEEE Netw. 31 (2017) 50–58.

[2] H. C. Mandhare and S. R. Idate, ‘‘A comparative study of cluster based outlier detection,distance based outlier detection and density based outlier detection techniques,’’ in Proc. Int. Conf. Intell. Comput. Control Syst. (ICICCS), Jun. 2017, pp. 931–935.

[3] Learning Based Adaptive Network Immune Mechanism to Defense Eavesdropping Attacks MINGYUAN LIU, DEYUN GAO, GANG LIU, (Student Member, IEEE), JINGCHAO HE, LU JIN, CHUNLIANG ZHOU, AND FUCONG YANG

[4] Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study Ishtiaq Roufa, Rob Millerb, Hossen Mustafaa, Travis Taylora, Sangho Ohb Wenyuan Xua, Marco Gruteserb, Wade Trappeb, Ivan Seskarb ∗ a Dept. of CSE, Univ. of South Carolina, Columbia, SC USA

[5] A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic. Kyle Greene, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, Vijay Devabhaktuni Purdue University Northwest. JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015

[6] Cybersecurity attacks on CAN bus-based vehicles: a review and open challenges. Faten Fakhfakh, Mohamed Tounsi, Mohamed Mosbah Library Hi Tech ISSN: 0737-8831 Article publication date: 12 August 2021

[7] M. J and K. C, "Smart vehicle monitoring for detecting anomalies on CAN bus," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 1-6, doi: 10.1109/CONECCT52877.2021.9622628

[8] Yang Y, Duan Z, Tehranipoor M. Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal. Smart Cities. 2020; 3(1):17-30. https://doi.org/10.3390/smartcities3010002

[9] K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319180.

[10] Adly, S., Moro, A., Hammad, S., & Maged, S. A. (2023). Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles. Applied Sciences, 13(16), 9374. https://doi.org/10.3390/app13169374

[11] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

[12] Zhang H, Meng X, Zhang X, Liu Z. CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. Sensors. 2020; 20(17):4900. https://doi.org/10.3390/s20174900

[13] Brookings. (2015, August 5). Jeep Cherokee hack offers important lessons on the “Security of Things”. Retrieved from https://www.brookings.edu

[14] Autoblog. (2019, September 21). How a hacked Jeep Cherokee led to increased security from cyber carjackers. Retrieved from https://www.autoblog.com

[15] Carnegie Mellon University - Software Engineering Institute. (n.d.). Vehicle Cybersecurity: The Jeep Hack and Beyond. Retrieved from https://insights.sei.cmu.edu

[16] Zhou, K., & Staggs, J. (2018). "A Survey of Remote Automotive Attack Surfaces." IEEE Security & Privacy, 16(3), 16-28. While not focused solely on Tesla, this paper reviews various remote automotive attack surfaces, including those relevant to the Tesla incidents discussed by Keen Security Lab.

[17] M. Takada, Y. Osada and M. Morii, "Counter Attack Against the Bus-Off Attack on CAN," 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), Kobe, Japan, 2019, pp. 96-102, doi: 10.1109/AsiaJCIS.2019.00004.

[18] K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319180.

[19] M. Girdhar, J. Hong and J. Moore, "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 417-437, 2023, doi: 10.1109/OJVT.2023.3265363

[20] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, “Cybersecurity challenges in vehicular communications”, Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2019.100214.

[21] Carsten, Paul, Todd R. Andel, Mark Yampolskiy, and Jeffrey T. McDonald. "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions." In Proceedings of the 10th Annual Cyber and Information Security Research Conference, pp. 1-8. 2015, https://doi.org/10.1145/2746266.2746267.

[22] Valasek, C., & Miller, C. (2014). Adventures in automotive networks and control units (Technical White Paper). IOActive.

[23] M. Hashem Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," in IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 45-51, June 2017, doi: 10.1109/MVT.2017.2669348.

[24] Rathore RS, Hewage C, Kaiwartya O, Lloret J. “In-Vehicle Communication Cyber Security: Challenges and Solutions”. Sensors

(Basel). 2022 Sep 3;22(17):6679. doi: 10.3390/s22176679. PMID: 36081138; PMCID: PMC9460802.

[25] DDoS Attacks - Imperva. https://www.imperva.com/learn/ddos/ddos-attacks. [Accessed on 22-0-2024]

[26] What is a DDoS attack? Cloudflare https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack . [Accessed on 22-03-2024]

[27] V. Tanksale, "Controller Area Network Security Requirements," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2020, pp. 157-162, doi: 10.1109/CSCI51800.2020.00034. **{citadel}**

[28] F. Oberti, E. Sanchez, A. Savino, F. Parisi, M. Brero, and S. Di Carlo, "LIN-MM: Multiplexed Message Authentication Code for Local Interconnect Network message authentication in road vehicles," in *IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2022, pp. 1-7, doi: 10.1109/IOLTS56730.2022.9897819. **{Mitadel**

[29] I. Park and M. Sunwoo, "FlexRay Network Parameter Optimization Method for Automotive Applications," in *IEEE Transactions on Industrial Electronics*, vol. 58, no. 4, April 2011, pp. 1449-1459, doi: 10.1109/TIE.2010.2049713. **{Kitadel**

[30] W. Jeong, E. Choi, H. Song, M. Cho, and J.-W. Choi, "Adaptive Controller Area Network Intrusion Detection System Considering Temperature Variations," in *IEEE Transactions on Information Forensics and Security*, vol. 17, 2022, pp. 3925-3933, doi: 10.1109/TIFS.2022.3217389. **{Ajadel}**

[31] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, "Evaluation of CAN Bus Security Challenges," *Sensors*, vol. 20, no. 8, Art. no. 8, Jan. 2020, doi: 10.3390/s20082364.

[32] F. Fakhfakh, M. Tounsi, and M. Mosbah, "Cybersecurity attacks on CAN bus based vehicles: a review and open challenges," *Libr. Hi Tech*, vol. 40, no. 5, pp. 1179–1203, Jan. 2021, doi: 10.1108/LHT-01-2021-0013.

[33] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and Countermeasures for In-Vehicle Networks," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, Jan. 2022, doi: 10.1145/3431233.

[34] V. Tanksale, "Controller Area Network Security Requirements," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2020, pp. 157–162. doi: 10.1109/CSCI51800.2020.00034.

[35] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," *Sensors*, vol. 22, no. 17, Art. no. 17, Jan. 2022, doi: 10.3390/s22176679.

[36] S. Hounsinou, M. Stidd, U. Ezeobi, H. Olufowobi, M. Nasri, and G. Bloom, "Vulnerability of Controller Area Network to Schedule-Based Attacks," in *2021 IEEE Real-Time Systems Symposium (RTSS)*, Dortmund, DE: IEEE, Dec. 2021, pp. 495–507. doi: 10.1109/RTSS52674.2021.00051.

[37] V. Renganathan, E. Yurtsever, Q. Ahmed, and A. Yener, "Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems," *Cybersecurity*, vol. 5, no. 1, p. 30, Oct. 2022, doi: 10.1186/s42400-022-00132-x.

[38] S. H. Oh, J. Kim, J. H. Nah, and J. Park, "Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity," *Electronics*, vol. 13, no. 3, Art. no. 3, Jan. 2024, doi: 10.3390/electronics13030555.

[39] Jo, Hyo Jin, and Wonsuk Choi. "A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures." *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, July 2022, pp. 6123–41. *IEEE Xplore*, https://doi.org/10.1109/TITS.2021.3078740.

[40] Alkhateeb, Omar. Controller Area Network Attacks and Defense Mechanisms: Survey Created By. 2020. DOI.org (Datacite), https://doi.org/10.13140/RG.2.2.25052.82561.

[41] Sedar, Roshan, et al. "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths." *IEEE Open Journal of the Communications Society*, vol. 4, 2023, pp. 325–91. *IEEE Xplore*, https://doi.org/10.1109/OJCOMS.2023.3239115.

[42] A Survey and Comparative Analysis of Security Properties of CAN Authentication Protocols. https://arxiv.org/html/2401.10736v1. Accessed 22 Mar. 2024.

[43] "Cybersecurity Best Practices for the Safety of Modern Vehicles." *Federal Register*, 9 Sept. 2022, https://www.federalregister.gov/documents/2022/09/09/2022-19507/cybersecurity-best-practices-for-the-safety-of-modern-vehicles.

[44] Zhang, Haichun, et al. "A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units." *IEEE Access*, vol. 9, 2021, pp. 49690–706. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2021.3124565.

[45] Adly, Salah, et al. "Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles." *Applied Sciences*, vol. 13, no. 16, Jan. 2023, p. 9374. *www.mdpi.com*, https://doi.org/10.3390/app13169374.

[46] Dibaei, Mahdi, et al. "An Overview of Attacks and Defences on Intelligent Connected Vehicles." *arXiv.Org*, 17 July 2019, https://arxiv.org/abs/1907.07455v1.

[47] Lin, Chung-Wei, and Alberto Sangiovanni-Vincentelli. "Cyber-Security for the Controller Area Network (CAN) Communication Protocol." *2012 International Conference on Cyber Security*, 2012, pp. 1–7. *IEEE Xplore*, https://doi.org/10.1109/CyberSecurity.2012.7.

Roles and Responsibilities

Team Members	Roles and Responsibilities
Mehrab Helal Shuvo (40241199)	-Overview of Automotive Networks -Brief discussion on the significance of security in automotive networks and Introduction to CAN -Conclusion of the survey paper and key takeaways from the literatures
Aporajita Dutta Purkayastha (40233325) Pritom Samanta Picklu (40255233)	- Overview of CAN, LIN, and FlexRay networks - Comparison of functionalities and use cases - Security concerns and challenges in each network type
Mehran Mujib (40276697) Nadia Ferdous, (40263272)	-Methodologies of the attacks (e.g., DoS attacks, spoofing, message manipulation) -Detailed discussion of notable attacks with examples
Akash Saha (40233587) Fatema Ahsan Meem (40235119) Mohammad Tawsif Ul Hye Chowdhury (40261062)	-Summary of recent attacks on CAN -Affects of attacks on these networks - Resources needed by attackers to complete the attacks

Md Abdul Muntaqim Qureshi (40191640) Md Anisuzzaman Rumon (40222093) Md Hafizul Islam (40225761)	-Existing security measures and their effectiveness -Latest advancements in securing automotive networks - Recommendations and potential future directions for enhanced security