**1. 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.

**2. 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]

**3. Lock Picking 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.

**4. Denial of Service (DoS)/Distributed DoS (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.

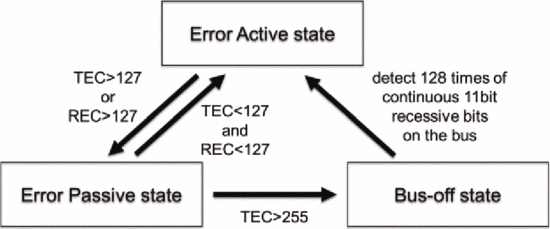
**5. Bus-off Attack**   
Using the CAN protocol's error-handling characteristics, a bus-off attack compels the target node to enter the bus-off state. In the bus-off state, a node cannot transmit/receive any messages[17]. A bus-off attack aims for the frame collisions.

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.

**6. 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 1: 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 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.

**7. 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].

**8. 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​​.

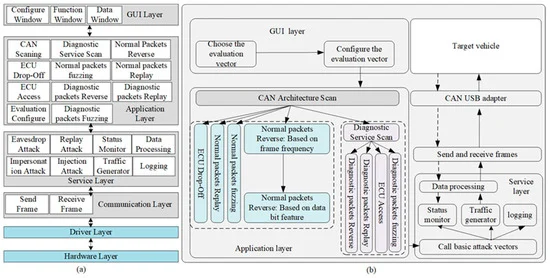
One practical approach to evaluating and mitigating the risk of replay attacks on CAN is the use of a security evaluation tool like CANsec. This tool can monitor changes in vehicular status, log evaluation activities, and replay captured CAN frames to test the vulnerability of the network to replay attacks. Experiments conducted using CANsec on a vehicle revealed that the replay attack was indeed effective 

Figure 2: CANsec Architecture[12]

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].

**9. Malicious Diagnostic 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.

**10. 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.

**11. 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.

**12. 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].

**13. Manipulation via OBD-II Port**  
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.

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.

Automotive Control Networks, Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Cybersecurity, Attack Vectors, Vulnerabilities, Threat Landscape, Security Measures, In Vehicle Control 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. 149690–706. *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.