IV. ATTACKS ON IN-VEHICLE NETWORK SYSTEM

9) **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[1]. 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[2]. 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[2].

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[2]. 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.

10) **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)[3]. 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[8].

11) **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[3]. DoS assaults may harm the braking system, causing the car to stop suddenly or not at all[3].

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)which have been infected with malware, allowing them to be controlled remotely by an attacker.

12) **Manipulation via OBD-II Port:** Attackers can gain entry to the in-vehicle network through OBD-II ports, compromised ECUs, or infotainment & telematics systems[4].

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, acess to the in-vehicle network, and installation of malware[5]. Valasek and Miller [6] 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 [7]. 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[4]. These transmissions ultimately caused the engine of a moving vehicle to fail[4].

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.

[1]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.

[2]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.

[3] 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

[4] 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>.

[5] 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>.

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

[7] 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.

[8] 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.

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

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