***The Controller Area Network Protocol:***

CAN is a widely recognized vehicle bus standard utilized for in-vehicle networks. Due to its affordable price and adaptable design, which minimizes the need for a wiring harness, it is well-liked in industrial and automotive applications. CAN is a message-based protocol. All nodes can read the messages sent over the bus, and the packets contain no information about the sender or recipient of the messages. The automotive domain functions supported by the protocol include automatic start/stop, electric parking brakes, parking assistance, automatic lane detection, collision avoidance, and more.

*CAN Bus Attack Interfaces*: The attack surface in the connected car environment consists of telematics units, infotainment systems, the OBD-II port, and sensors. The attacker can inject messages into the network through direct connections, such as OBD-II, or wirelessly via telematics.

A diagram of a car

Description automatically generated

**Figure 1.** CAN bus attack interfaces [1]

*Security Issues for CAN:*

There are numerous security flaws in the CAN protocol that hackers could exploit to compromise an in-vehicle network because it was not created with security in mind.

Using malicious smartphone applications in a connected car, it is possible to carry out a long-range wireless attack in actual vehicles. The attack surface can be telematics, a Wi-Fi port, Bluetooth, or an OBD port. [2]

***Lack of Confidentiality****:*

Every node connected to the bus has the option to accept or reject frames sent over the bus by the CAN protocol. As a result, a malicious node can monitor every message that travels across the bus.

CAN bus networks do not encrypt messages. Every node can therefore see the messages traveling through the bus. Attackers can decipher those messages and utilize them to breach the in-car network.

***Lack of Authenticated Messages:***

The recipient of a message cannot tell if it is coming from a reliable source or not because the CAN frame format does not include sender and recipient information. Therefore, in CAN networks, it is not possible to guarantee the message's authenticity.[2] There are five primary categories of attacks: DoS attack, fuzzy attacks, replay attacks, spoofing, and impersonation. These primary attack types have been extensively researched in the literature and have the potential to seriously compromise the security of in-car technology.

***Classification of Attacks on In-Vehicle Networks:***

A diagram of a network

Description automatically generated

Fig 2: Classification diagram for CAN network attack types.[1]

**DoS attack:** To prevent legitimate users from accessing information systems, services, or network resources, an attacker may use a denial of service cyberattack, which involves flooding the target network with many fake requests. The CAN network is vulnerable to DoS attacks due to its arbitration mechanism for contention resolution. Figure 3 shows a scenario of a DoS attack on CAN networks.

A diagram of a can bus

Description automatically generated

**Figure 3.** A sample denial of service (DoS) attack on a CAN network [1]

**Fuzzy attack:** In this context, "fuzzy" describes how random and indiscriminate the attack is. A fuzzy attack, unlike more targeted attacks, does not require specific knowledge of the vehicle's systems and protocols. Instead, it simply floods the CAN bus with malformed messages. This makes it easier to carry out than more complex attacks that require reverse engineering of the software and protocols of the car.

For example, if the malicious ECU sends out frames with spoofed IDs for critical systems such as the engine or brakes, it may cause unintended behavior in these systems. This could result in situations where the car breaks down, deviates from its intended path, or behaves erratically, endangering the lives of occupants and other drivers.

A diagram of a can bus

Description automatically generated

**Figure 4.** A sample fuzzy attack on a CAN network [1]

**Replay attack and spoofing**:

When a hacker gains control of an ECU, they can replay messages sent over the bus after sniffing them, which can lead to dangerous circumstances. Because the message syntax of this kind of attack imitates a real CAN message, it is difficult to identify. A replay attack example is shown in Figure 5. Spoofing is a type of attack in which a malicious node sends messages with a fake ID that is identical to a legitimate node. Because there is no message authentication on the CAN bus, the recipient node may conclude that the message is from a legitimate node.

However, it is challenging to distinguish between malicious and legitimate nodes. Figure 5 also provides an illustration of the spoofing attack.

A diagram of a bus

Description automatically generated

**Figure 5.** Sample CAN bus attacks (spoofing and replay).[1]

**Impersonation attack:** Impersonation is a type of attack in which a malicious node is planted in the CAN bus, impersonates a legitimate node, and takes over its functionality, effectively disabling the legitimate node's operation. Attacks of this kind have the potential to cause unexpected behavior in the vehicle, putting both it and its surroundings in danger. Figure 6 shows an attack by impersonation.

A diagram of a bus

Description automatically generated

**Figure 6.** Illustrating an impersonation attack [1]

**References:**

[1] Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on

Blockchain Narayan Khatri 1, Rakesh Shrestha 2 and Seung Yeob Nam 1

[2] In-Vehicle Communication Cyber Security: Challenges and Solutions

Rajkumar Singh Rathore 1, Chaminda Hewage 1 , Omprakash Kaiwartya 2, and Jaime Lloret.

[3] Security and Privacy for In-Vehicle Networks Hendrik Schweppe, Yves Roudier.