**CAN Signal Extinction-based DoS Attack on In-Vehicle Network:**

We provide a novel attack technique that is undetectable by current IDS called CEDA (CAN signal extinction-based DoS attack) employs a voltage drop to destroy the CAN signal. This attack method is a kind of DoS attack, and the goal is to remove the target system instead of making it unavailable. The attack exploits a weakness in the Controller Area Network (CAN). CAN has two logical states: a recessive state and a dominant state. If both CANH and CANL are of same voltage around 2.5v it is called recessive state. The dominant state is CANH, which has a higher voltage around 3.5V compared to CANL around 1.5V. By subtracting the voltage potential of both CANH and CANL, the differential voltage is determined. If the differential voltage is less than 0.5 V, the bus will be considered in the recessive state, and if the differential voltage is greater than 0.9 V, it is considered in the dominant state. However, if the differential voltage is between 0.5 V and 0.9 V, it is neither a dominant state nor a recessive state. In this case, the bus state is not defined according to the CAN standard; this area is the gray zone. ECUs ignore messages with an undefined voltage level (gray zone).

When the attacker conducts this attack on a specific ECU by ID, the ECU continuously generates an error frame, and when the error frame reaches the threshold, the ECU becomes "bus-off." This DoS attack performs only on a CAN-based in-vehicle network. According to the paper, increasing resistance on the CAN bus can lower the differential voltage; both are inversely proportional. The attacker calculates the exact resistance to push the voltage of a specific message into the gray zone using its ID. Attackers must set up a monitoring device and keep tabs on messages in the CAN-based in-car network. Attackers can use this to determine the CAN ID of the targeted device or function and raise the resistance to stop the target ECU from sending messages to other ECUs.

**Spoofing Attack Using Bus-off Attacks against a Specific ECU of the CAN Bus:**

**Spoofing attack on CAN:** In this proposed attack, if a message is transmitted by the authorized ECU, it is intentionally set as an error, then the state is transited to the bus-off state, and the send or receive by the authorized transmission ECU is prevented.

**Bus-off Attack against an ECU:**

**1.Bus-off Attack Using the Bit Error:** By injecting bit errors into the targeted ECU, the TEC (transmit error counter) of that ECU increases. A pointless message is inserted right before the target ECU starts transmitting. As a result, the targeted ECU transmission is stored and blocked. Simultaneously, the attacker's ECU's buffer stores messages that satisfy:   
1) It must have the same CAN ID as targeted ECU.   
2) The attacker sends dominant bits in response to recessive bits sent by the target's ECU.   
As a result, as shown in FIG. 1, the attacker and target ECU communicate simultaneously, as seen in Fig. 2. These ECUs' TEC increases by 8 when the transmission bits differ. The target ECU enters the bus-off state, and TEC > 255 is set by repeating this procedure.

A diagram of a field of binary code

Description automatically generated

Figure 1 Bus-off attack using the bit error.

A diagram of a field

Description automatically generated

Figure 2 Bus-off attack using the stuff error.

**2.Bus-off Attack Using a Stuff Error:** The attacker verifies the data frame that is flowing on the CAN bus. If the data frame is sent from the targeted ECU, then the attacker transmits an error frame into that data frame. As shown in the Fig2.The target ECU detects a bit error and increases TEC by 8. By repeating this process, the target ECU enters the bus-off state and TEC > 255.

**3. Bus-off Attack in One Frame:** According to the CAN specification, ‘0’ is the dominant state and ‘1’ is the recursive state. If the dominant state continues to increase to 14 bits after error detection, the TEC increases by 8. For each time of dominant state increase in TEC of targeted ECU and this goes to bus off state (error bit 1 bit + 14 bits + 8 bits × 30), TEC > 255.

A diagram of a error

Description automatically generated

Figure 3 Bus-off attack in one frame.

Theory of Attack: When the targeted ECU is detected by CAN ID, it is transmitted to the bus-off state using the above bus-off attacks. Now the attacker sends the spoofing messages in the same cycle as legitimate messages. As a result, the receiving ECU cannot detect spoofing messages since it is receiving only spoofing messages.

A diagram of a bus error

Description automatically generated

Figure 4 spoofing attack using the bus-off attack.

**INVESTIGATION ON CYBER-ATTACKS AGAINST IN-VEHICLE NETWORK:**

**THE FUNDAMENTAL CYBER RISKS OF CONNECTED CARS:**

Passive Attacks: In passive attacks, there is no need for physical contact with the vehicle, even though it is difficult to identify if an attack has occurred.

* Man in the Middle Attack: The attacker eavesdrops on the communications between vehicles. An adversary might use the sensitive information obtained in this manner.
* Using Live Traffic Status: By analyzing the road traffic system, attackers can identify the length and timing of messages sent and received between vehicles and the road traffic server. With this information, attackers can gather details like the path the vehicle takes and the time a vehicle will be at a particular location.

Active Attacks:

* Attacks on Connected Units: Nowadays, cars have more electronic than mechanical parts. Each ECU (Electronic Control Unit) has a separate task, and all are related to the CAN (Control Area Network) bus. If an intruder can gain access to a CAN bus by a wired medium like an OBD USB port or wireless medium like the Global System for Mobile Communications (GSM), Wi-Fi, and through APIs like Short Message Service (SMS) APIs, Web-interface APIs, and mobile APIs, then the attacker can target the safety brakes, engine, and powertrain system. Once manufacturers find this, they release updates using Over the Air (OTA).
* Attacks on Fleets of Vehicles: In fleet operations, dealerships observe vehicle information using internal and external sensors. These sensors are related to the same CAN bus as the ECUs are connected to, as ECUs also need information from sensors. An attacker could plug in an end device to gain access to the CAN bus, which enables them to inject false values to force the vehicle to perform unwanted actions. The attacker would demand a ransom to release the system.