**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.

**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 keep 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.