**A. specific attack vectors**

**Evaluation of CAN Bus Security Challenges**

**Vulnerability Assessment of the CAN Protocol**

It is essential to have a vulnerability assessment of a network to highlight security problems.

Therefore, the vulnerability assessment of the CAN protocol can be carried out based on

confidentiality, integrity, and availability.

Confidentiality means providing the data only to authorised people. However, the CAN

protocol does not have inherent cryptographic methods to ensure confidentiality. This allows an

intruder to access sensitive user data and cause an invasion of privacy.

Integrity is the accuracy, completeness, and validity of the data. The CAN bus has a CRC for

verification of integrity against the transmission errors, but it cannot prevent data injected by

malicious parties, which breaks the integrity. The protocol does not have a comprehensive integrity

check and fails to sustain integrity.

Availability means that authorised users can use the system at all times. Given the nature of

priority-based messaging, if a message with the highest priority is transmitted/inserted, the network

will be inaccessible by the lower priority nodes, and availability is violated.

The CAN bus failed to pass all three essential security criteria. Thus, it is a clear indication that

the CAN protocol does not have any security measurements against the attacks.

**Automotive Attack Surface and Existent Attacks**

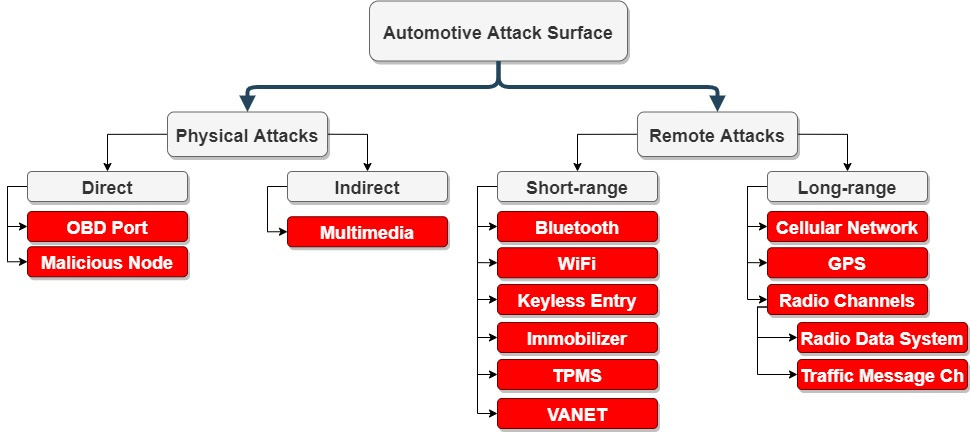
In the 1950s, automotive electronics cost only 1% of the total car cost, while it is currently 35%

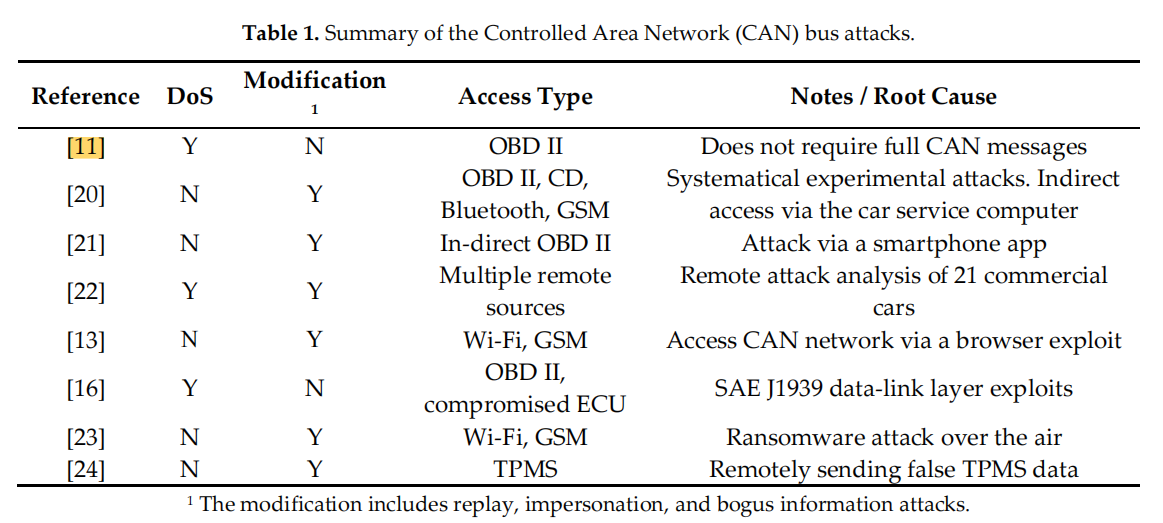
and is expected to rise to 50% in 2030 [19]. Although the rise in electronics has improved comfort,

functionality, and driving safety, it has created new attack surfaces, as shown in Figure 5. The

protocol itself is defenceless to attacks; therefore, any exploit in the current/future telematics unit or

infotainment system can disrupt the network, as summarised in Table 1.



****

The first CAN bus attack was performed on the power window by Hoppe and Dittman in 2007

[7,25]. Since then, numerous attacks have been performed. These attacks can be categorised as

physical access attacks, where the attacker should access the vehicle physically, or remote attacks,

which are implemented via wireless communication interfaces. Although attacks in the literature are

mainly physical access ones, some experts have argued that physical access to the CAN network is

not practical [26]. Therefore, current research is mainly focusing on remote access attacks.

**Physical Access Attacks**

Physical access attacks require direct or indirect access to the CAN bus network. Direct access

can be obtained by the On-Board Diagnostic (OBD) port or a malicious node. The OBD port is the

primary attack surface; hence, it has access to all of the nodes, even though network segmentation is

used.

Koscher et al. [10] manipulated the CAN and controlled various modules including essential

brake control and engine control modules through the On-Board Diagnostics II (OBD-II) port. They

released the brake and prevented its activation while the car was running 40 mph by the continuous

fuzzing method. The attack also includes the manipulation of the instrument cluster with false data,

changing engine parameters, and disabling the engine.

Due to the CAN architecture, any malicious node can listen or send a message to disrupt the

network. The attacks implemented through the OBD port can be replicated using a malicious node.

Palanca et al. [11] applied a selective denial-of-service (DoS) attack on an unmodified 2012 Alfa

Romeo Giulietta. The research showed that any person who has physical access to the network can

disrupt it, even with a simple tool. This attack does not require a full message transmission; instead,

it overwrites to the recessive bits and generates a transmission error. The contribution of this research

is that it exploited the vulnerability of the CAN standard. After this research, an alert (ICS-ALERT-

17-209-01) [27] was announced by the U.S. government. A similar research analysis was carried out

by Murvay and Groza [28] to show the limitations of the attack on different bit rates and to breach

the authentication methods.

Mukherjee et al. [16] implemented DoS attacks on the SAE J1939 standard [29], which is used in

heavy-duty commercial vehicles. They performed three separate DoS attacks: (i) sending too many

request messages for a supported Parameter Group Number (PGN) to overload the recipient ECU,

(ii) sending manipulated false request to send (RTS) and causing overflow at the recipient buffer, and

(iii) keeping the connections open via Clear to Send (CTS) messages and occupying the whole

network. This work was one of the first studies to exploit the SAE J1939 specification. Murvay and

Groza [15] implemented impersonation and DoS attacks on SAE J1939. These works showed that SAE

J1939 is vulnerable to protocol-specific attacks in addition to all CAN bus attacks.

There can also be indirect physical access attacks. These attacks require a physical object to be

inserted into the car, but adversaries do not necessarily have direct access to the network. Checkoway

et al. [20] developed an indirect access attack model, which included hacking the IT system of the car

service and accessing the CAN via computer. The attack model also included attacking via

multimedia devices (CD, USB, or MP3 player). Hoppe et al. [12] implemented an attack with a

multimedia disc. Although the attack did not breach the CAN, it may scare the driver by flashing a

warning on the screen and playing an alarm signal.

**Remote Access Attacks**

Nowadays, modern vehicles contain different types of wireless interfaces needed for

communicating with systems such as passive anti-theft, tire pressure monitoring system (TPMS),

Bluetooth, radio data, telematics, and so on. These wireless interfaces need to communicate with the

CAN, usually via a gateway ECU to protect the network. However, there are studies that have

demonstrated the hacking of a gateway ECU and gain accessed to the isolated CAN [12].

Checkoway et al. [20] compromised the TPMS, Bluetooth, FM channel, and a cellular network

of a car through reverse engineering and claimed that thieves could steal vehicles easily as doors

could be unlocked through the CAN messages. Woo et al. [21] proposed a remote attack via a

malicious self-diagnostic app. If someone uses a malicious app to monitor/diagnose the vehicle’s

situation, the adversary takes control of the vehicle remotely and performs its attack from a long

distance.

Valasek and Miller [22] carried out a remote attack survey on 12 car brands and 21 commercial

cars and identified the remote attack surfaces and their difficulties in compromising each vehicle. The

attack was three-staged. The first stage was to compromise the ECU responsible for a wireless

interface. The second stage was to inject messages to communicate with the safety-critical ECU. The

last stage was to modify the ECU to behave maliciously. While the researchers believed that the

increasing number of cyber-physical systems in the cars would increase their vulnerabilities, they

could not practically verify this because of the high number of different applications in the vehicles.

Furthermore, they also hacked a Jeep Cherokee remotely and disabled the engine in 2014 [9]. After

this attack, a public announcement that stated the vulnerability of motor vehicles against remote

attacks was published [30].

Savage and his team [31] took control of a Chevrolet Corvette’s brakes and windshield wipers

via a commercial telematics control unit in 2016. This attack indicates that the vulnerability of the

CAN can be penetrated by the aftermarket equipment and cannot be entirely addressed by the

manufacturer [32].

Nie et al. [13] implemented a remote attack on a Tesla Model S in 2016 via a wireless and cellular

interfaces. The Keen Security Lab of Tencent [14] discovered multiple attack surfaces on BMW

vehicles, which showed that even high-end commercially available cars could suffer from cyber

attacks.

Another wireless attack method is over-the-air (OTA) software updates. OTA is a cost-effective

and scalable solution that allows the manufacturers to deliver software updates remotely. However,

it is another attack surface where hackers can dive into the vehicle’s communication network. Beek

and Samani [23] implemented a ransomware attack via an OTA update.

The remote attack surface of the modern car is more substantial than the physical one, and with

the rising connectivity in cars, the number of wireless attack surfaces is increasing day by day. In the

near future, cars will be equipped with vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)

communications, which build vehicular ad hoc networks (VANETs). VANETs aim for traffic

optimisation and collision avoidance. To provide these benefits, VANETs use car sensors and have

wireless connectivity. In VANETs, spoofed messages can be received or transmitted, and as a result,

the in-vehicle communication network may be disrupted.

**B Detailed discussion of notable attacks**

**Evaluation of Attack Vectors and Risks in Automobile**

**A. Attack Vector: “Lock Picking”**

Keyless door entry allows users to open and lock car doors using a key fob with buttons that wirelessly transmit ‘*open’* and ‘*lock*’ signals. The exploit is based on a *man-in-the-middle* attack using a device that captures the transmitted signal from the key fob and simultaneously sends a jamming signal on the same frequency. The key fob user, thinking their key fob malfunctioned, tries again; this time the car door unlocks. Key fobs transmit unique, one-time codes each time they are used. The attacker’s device captured the first code, then transmits and

“sacrifices” it to unlock the door as it captures the second code transmission. As the codes have no expiration time, the attacker may use the second captured code to transmit and open the door. The same technique and device may also be used to attack garage door openers [9]. These types of attacks have been successfully demonstrated on garage door openers and several cars including Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Volkswagen, and Jaguar [10]. The work behind these types of attacks can be explained mathematically [11] while several hardware devices exist to carry out these types of attacks. For example, the Rolljam device to attack remotely operated RF signals is small and fast, OpenSesame opens garage doors using a Mattel toy, OwnStar finds, unlocks, and starts GM OnStar cars. The same technology has also been used in the amateur drone space with SkyJack, a Raspberry Pi drone that locates and attacks other drones [12]. These devices are widely available in the market, so much so that complaints were made about them to the UK’s Home Office (the government’s department charged with national security) but their sales continued unabated [13]. Protecting against these types of attacks could be addressed by the remote door control system manufacturers. Possible solutions could include the implementation of antijamming and code-grabbing resistant functions, along with updated chip firmware with time-expiring signals. The latter solution has been adopted by one manufacturer [14] but others have not yet followed suit.

**B. Attack Vector: Vehicle-Monitoring Components**

A well-studied exploitation has been related to the tire pressure monitoring system (TPMS) [8]. The TPMS transmits

information to the vehicle’s Electronic Control Unit (ECU), while continuously monitoring tire pressure to enable the ECU to trigger a dashboard warning light (in some vehicles the actual tire pressure is displayed) if tire pressure falls outside specifications. These systems are known to have been deployed without any security safeguards.

A possible passive attack can allow attackers to track vehicle movement and location using mobile or roadside tracking stations as TPMS signals can be captured up to 40 meters away from the vehicle. On the other hand, the lack of cryptographic protection of the TPS signals can enable an active attack as the vehicle’s ECU trusts any information provided from vehicle sensors. It is therefore possible to wirelessly inject spoofed signals, tricking the ECU into displaying false and even out of range tire pressure measurements. Mitigating these types of attacks can be as simple as using hardware pairings (e.g. ECU communication with sensors of specified hardware addresses) and deploying encrypted-only signal transmissions.

**C. Attack Vector: Road. Infrastructure**

As vehicles become more connected, road infrastructure components become an intrinsic part of these growing

transportation computing networks. In fact, vehicle-toinfrastructure (V2I) connectivity becomes an integral part of the environment which includes smart traffic lights, pedestrian crosswalk sensors and smart road, adaptive road signs. Exploiting vulnerabilities of road signs to alter the displayed messages may sound more like an innocent prank but it can quickly become a very serious issue. Case in point, a 2014 attack when a foreign national initially compromised five overhead highway signs in North Carolina and six others in two other states, altering their displays by indicating they were hacked by SunHacker [15]. The attack was possible due to the negligence

of the signal operators in changing the default password set by the sign manufacturer. [16] Though individual road signs have been compromised and changed to warn of zombie attacks and other farcical threats, this

is the first known case of a mass compromise of networked road signs. While the particular attack was benign, it is clear that compromised road infrastructure by a malicious actor with control over highway signage could cause major problems that may be more than traffic disruptions, particularly during an emergency. Mitigating this type of attack requires following best practices in password management for the road signs as one would expect for any other computing devise that is shipped with a default password from the manufacturer. The demonstrated attacks provided misinformation to drivers but it is easy to extrapolate how misleading information could be passed to vehicles through their sensor payload from road infrastructure assets. From the vehicle’s perspective protection has to come from secure design of sensors that provide both V2V and V2I sensing related to speed, motion, and detection of road and traffic conditions. Each one of these sensors represents a potential attack vector, so secure design should be a consideration not only in deployment but also in sensor design. There are different approaches in sensor design to mitigate attacks. For example, developing smart sensors that use linear Gaussian dynamics

techniques that are able to statistically profile expected sensor inputs and detect attacks [17].

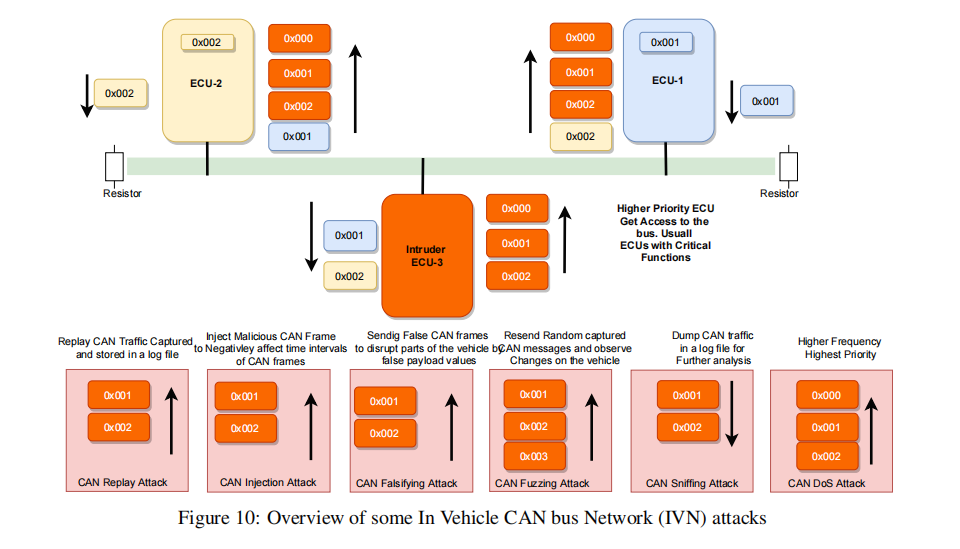
**C Summary of recent attacks**

**Cyberattacks and Countermeasures for In-Vehicle Networks**

**1 Attacks against the CAN Bus**

The classical CAN and CAN FD buses are vulnerable to various attacks. Once attackers have access from either inside or outside the vehicle, they can generate various attacks on the CAN bus network such as CAN sniffing, CAN fuzzing, CAN replay and DoS attacks. Some of the mechanisms for initiating these attacks include:

**CAN bus sniffing**: With o authentication mechanisms, encryption and broadcast transmission, it is possible to sniff the data on the CAN bus [3]. Using off the shelf OBD2 sniffer such as CANdo board, it is possible to read and analyse the data on the bus to manipulate and generate similar messages [43]. This attack can be avoided by implementing encryption to prevent exposing CAN frames. This attack is difficult to detect due to the passive nature of sniffing traffic. The next step is 13A PREPRINT - APRIL 24, 2020 to reverse engineer the raw CAN messages so that they can be used to target specific parts of the vehicle. This an important step since manufacturers tend not to publish their CAN message specification



**CAN bus fuzzing attack** CAN bus protocol lacks authentication and data integrity checking and as a result ECUs accept CAN messages and respond to them. This attack is used to send random CAN data frames, checking the bus and observing changes on the instrument panel of the vehicle. This attack looks at the impact of CAN frames on the ECUs such as observing the change in vehicle speed while injecting CAN frames [57]. It usually happens after sniffing and

analysing captured CAN messages. Also, it can be generated using a black-box, where CAN id and payload values are generated randomly without prior knowledge of the actual CAN id used. It involves sending randomly captured CAN frames and recording the outcome. Encryption is needed to prevent analysis of the captured data, along with authentication to only accept CAN frames from legitimate ECUs.

**CAN bus frame falsifying attack** This attack is used to modify CAN message payload by inserting incorrect values. For example, the attacker can inject a vehicle with incorrect parameter values. This type of modification attack is used when the CAN id is known, and the intention is to provide incorrect data payload to disrupt vehicle services. This happens due to the lack of data integrity and authentication support in the CAN bus protocol. In order to prevent this

attack, CAN bus should provide authentication to verify the source of the data before acting upon it. Usually this attack involves a small amount of data, making it difficult to detect and monitor. To detect this attack, a system should consider checking CAN id and data payload consistency in a time window.

**CAN bus injection attack** Injecting data into a CAN bus can be used to send messages at an abnormal rate [58]. The purpose of this attack is to change frequency and amount of CAN frames on the bus, and change the sequence of legitimate CAN frames and data payload. Since CAN bus does not provide authentication to check if the sender is legitimate, this attack will inject the bus with abnormal CAN traffic targeting the vehicle speed. Lack of encryption also

enables arbitrary nodes to connect to the bus. The data on the bus can then be monitored to obtain the arbitration and data field, and and generate messages to simulate events [59]. This could lead to generation of fake events that cause parts of the vehicle to behave as required by the attacker. This attack can be prevented using authentication and integrity mechanisms. The result of the attack can increase the broadcast frequency of certain CAN id which can be etected through abnormal broadcast behaviour.

**CAN bus DoS attack:** Classical CAN and CAN FD use the same mechanism to access the medium with multi access using the CAN id priority [5]. The nodes on the CAN bus use the arbitration field to determine the priority of the message and which node can occupy the bus and send data. In this case, a DoS attacked can be lunched using highest attribution id such as 0x000 to occupy the bus and make it busy by using CAN frame priority arbitration scheme and send too many highest priority frames so that other nodes cannot use the bus [43]. Also, it can use the same CAN message id of an existed ECU and by knowing its transmission rate, a DoS can be performed by incrementing the frequency time. For example, if an ECU sends a message every 200 ms, the attacker can increase the frequency by injecting the same message with higher frequency which can lead to disruption of the sensor part.

**ECU impersonation:** Once an attacker has access to the CAN bus network, the attacker can receive all the traffic broadcast on the bus. With a focused analysis of the traffic, attackers can learn the behaviour of each ECU such as it’s CAN ID, payload range and transmission rate. In this way, they can simulate ECU behaviour by sending the same data with the same frequency. An increase in the CAN messages rate will occur which generates an attack. However, if

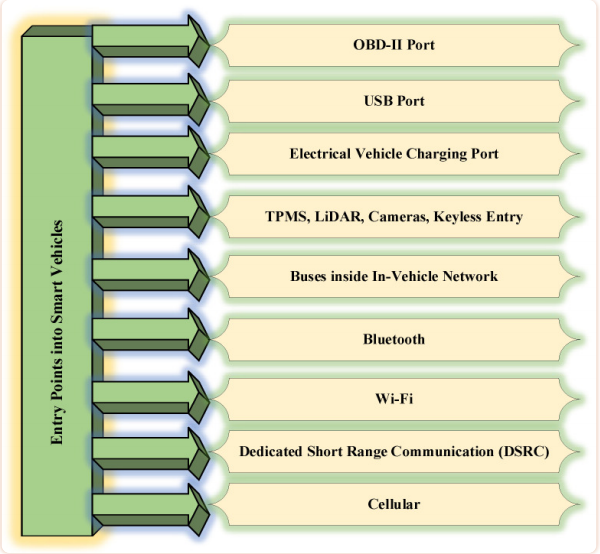
the attack was more focused, they could initiate an attack to disable particular ECUs. For example, Iehira et al. [60] introduced a sophisticated spoofing ECU attack by first performing an attack on an ECU by taking advantage of the error handling mechanism of the CAN bus protocol. This attack works by mimicking the target ECU behaviour, CAN ID and frequency. Then, the attacker ECU contradicts the target ECU by sending a dominant bit while the original ECU sends a recessive bit. This would raise an error in the ECU controller which leads, at a certain point, to disconnecting the ECU from the bus and dropping all the CAN bus communication. This enables an attacker to perform various attacks, such as an ECU impersonation attack, which is difficult to detect.

**In-Vehicle Communication Cyber Security Challenges and Solutions – PMC**

Classification of Attacks on In-Vehicle Network System for Possible Entry Points:

This paper first identifies the broad categories of attacks on in-vehicular system. These attacks

are classified into four major categories as sensor initiated, infotainment initiated, telematics iniftiated, and direct interface initiated as shown in Figure 7. There are generally two attack vectors, namely wireless access and physical access, attackers are using these attack vectors to get access to the internal networks of the vehicle. External inputs use these interfaces so that ECUs can be exploited. The attackers may use software bugs, the vehicle’s remote key (via the internet) and much more to exploit the ECUs easily. The in-vehicle network has several security issues, red search is going on to develop an advanced security framework. Wireless networks can be used for exploiting the bus system of the in-vehicle network Entry points to Smart Vehicles Smart intelligent vehicles have lots of features due to rapid development in automotive technolo gies. No security mechanism is sufficient enough to handle all security threats. With tremendous evolution in technology, hackers are also using advanced techniques to hack smart vehicles. There are several entry points to smart vehicles which are listed in Figure 8.



4.1.1. OBD-II Port

This port is used for monitoring various details such as emissions from vehicles, speed, mileage,

etc. OBD-II ports are considered the weakest link in the vehicle since the attacker may collect di agnostic data easily and subsequently get success in accessing the in-vehicle network and de ployment of malicious programs. Two types of attacks are possible on the OBD-II port, namely an in-vehicle network access attack and a Dongle exploitation attack. In the former attack type, the attacker may utilize an OBD-II port for installing the malicious device in the in-vehicle net work with the main objective of obtaining physical access. In the later attack type, dongles are fitted in the OBD-II ports. These dongles can be remotely handled and decrypted by the attacker.

**4.1.2. USB and Charging Ports**

Severe security threats are posed by the use of USB ports in the vehicle. Several examples of se vere security threats are reprogramming of the controller processor, installation of several types of malicious codes, network card tampering, and changes in operating system functionalities. Additionally, the malicious codes inside a USB pen drive or CD can be used to hack the infotain ment system. After hacking the infotainment system, hackers can easily control other parts of the vehicle such as the braking system and engine control system [32]. During the charging mechanism, Electric Vehicles (EV) are susceptible to several attacks via charging infrastructure. Additionally, the smart grid may be attacked by utilizing a charging system.

**4.1.3. Tire Pressure Monitoring System (TPMS), LiDAR and Keyless Entry Ports**

The attacker can use the TPMS for eavesdropping attack to get access to the vehicle network and perform malicious activities. LiDAR and cameras are opening the door for signal jamming attack. For keyless entry attack, the hacker tries to intercept the signal for further capturing and re directing purposes. There does not exist any adequate mechanism to protect the radio signals hence radio signals transmitted from vehicles’ keys can be easily captured by hackers. This area is open to researchers [34].

**4.1.4. Buse Network Ports**

There does not exist a communication protection mechanism for CAN. This protocol reflects a

broadcast nature and therefore each node is intended to receive the frame. This frame is not se cured by either MAC or digital signature. Confidential data can be stolen or manipulated in this protocol. The hacker can send fake frames to each node and thereby vehicle may start showing unintended behavior [35].

**4.1.5. Vehicular Communication Ports**

All the smart vehicles are enabled with Bluetooth with a range of 10 m. The mobile phone can

easily get connected with infotainment as well as telematics systems for performing a range of

activities such as making calls, streaming music etc. Through Bluetooth, hackers can get full ac cess to vehicles to perform malicious activities [36]. Almost all smart vehicles are enabled with

wi-fi. These smart vehicles can be connected to the internet through roadside wi-fi hot spots.

The low-security level at the wi-fi hot spot may expose the vehicle to several threats since wi-fi

hot spots may have outdated security mechanisms for the connection and hackers can easily tar get the vehicles through these weak access points [37]. Dedicated Short Range Communication (DSRC) is one of the onboard units. It utilizes radio fre quency for communication. It supports short-range communication for the vehicle to infrastructure as well as vehicle-to-vehicle communication. The hacker can easily get access to the vehicle

through DSRC and may perform severe undesirable activities [38]. Almost all smart vehicles are

equipped with cellular technologies (3 G/4 G/5 G, etc.). These smart vehicles are now capable of vehicle-to-infrastructure as well as vehicle-to-vehicle communication with distances of several miles. hackers can perform two types of attacks, namely jamming and eavesdropping on the cel lular networks [39].