Wireless Threats Against V2X Communication

Axel Boström[1], and Franz Wotawa[2,*]
TU Graz, Institute of Software Technology, Graz, Austria
axel.bostroem@student.tugraz.at, wotawa@ist.tugraz.at
*corresponding author

Abstract—As the automotive industry increasingly relies on wireless technologies, a new attack surface emerges, posing significant security threats to modern cars. This paper investigates the vulnerabilities and risks of wireless vehicle attacks, including eavesdropping, message tampering, spoofing, and jamming. It highlights vulnerabilities in the CAN bus communication interface. By exploring these attacks and their potential consequences, this paper aims to shed light on the urgent need for robust security measures to safeguard the safety and privacy of vehicle owners. The focus is on understanding the evolving landscape of wireless threats in the automotive industry, providing valuable insights for researchers, practitioners, and stakeholders involved in developing effective countermeasures and enhancing overall vehicle security. In contrast to other research articles, this paper presents the ISO/SAE DIS 21434 standard, which offers a systematic and structured approach to enhance cybersecurity in the automotive industry, even in the face of emerging wireless threats. In addition, this paper highlights notable examples of attacks on modern cars, where researchers gained access to vehicle systems through wireless vulnerabilities, demonstrating the potential dangers of interconnected car systems to illustrate the real-world implications.

Keywords–V2X communication; security threats; automotive software; V2X standards

1. Introduction

Autonomous vehicles and Internet-of-Vehicles (IoV) technologies are rapidly evolving. These vehicles have advanced sensors, GPS, entertainment systems, and autopilot features, making driving easier and safer. However, with such technology comes new threats, particularly in cyber attacks. Companies investing in this field compete to release the latest and safest autonomous cars, while security measures in these cars will have to keep up with new threats and methods of attack being developed [1].

One of the main concerns is that modern-day vehicles have millions of lines of code involved in building the software and hardware for modern autonomous cars. In fact, there are over 100 million lines of code in an autonomous car, which all have to be checked for bugs, errors, and fail-safes to ensure safe public release [1].

Alarming flaws have been found within the software of modern cars. For instance, one white hat hacker group was 2021 able to compromise the autopilot function of a Tesla Model S. Another group found a way to remote-control a Jeep to such an extent that they had complete control over every function of the car, including the engine. These incidents prove that the design of either hardware or software in autonomous cars can be compromised and abused for harming people or collecting data on people's location [1].

Vehicle to Everything (V2X) is crucial for the Intelligent Transport System (ITS) to improve road safety and traffic management by exchanging information between vehicles and various components of the ITS, such as pedestrians, transport infrastructure, and Internet gateways [2]. V2X enables communication between Onboard Units (OBUs) in vehicles with other vehicles, road infrastructure, pedestrians, and networks. V2X communication messages contain information about traffic conditions such as accidents and traffic jams, allowing drivers to take early action [3].

While V2X communication technologies aim to enhance transportation infrastructure, they also bring forth potential security threats. Vehicles can transmit fake data to other vehicles, causing traffic disruptions or accidents. As attackers may have physical access to portions of the system, detecting and preventing attacks is critical for the widespread implementation of V2X systems. Security breaches can result in data loss, component malfunction, and environmental harm. Thus, securing V2X communication platforms is imperative for successful design and implementation [4].

This paper aims to provide a comprehensive overview of the current threats to V2X communication to complement existing exhaustive surveys. Sedar et al. [5] provide a comprehensive survey on V2X security mechanisms and explain differences to previously published surveys like [2] and [6]. Yoshizawa et al. [7] published another most recent survey, which also captures privacy issues. Other surveys dealing with specialized issues like testing and authentication are [8] and [9] respectively. In this paper, we rely on previous work, including these studies, but focus on practitioners and current standards dealing with V2X communication and ensuring security.

We structure this paper as follows: We start with introducing the background. Afterward, we discuss some of the most common wireless attacks that target V2X communication systems and explore techniques to protect V2X communication against such attacks. Finally, we conclude with a discussion of the key takeaways from this paper. Throughout the paper, we aim to enhance the understanding of the security challenges associated with V2X communication and contribute to the ongoing efforts to develop effective countermeasures against these threats.

2693-9177/23/$31.00 ©2023 IEEE
DOI 10.1109/QRS60937.2023.00058

2. BACKGROUND

This section provides an overview of the necessary background information related to V2X communication. This overview includes information on the standards and protocols used for communication, such as DSRC, LTE-V2X, and real-world scenarios comprising security threats. By understanding these foundational concepts, readers are better equipped to understand the security challenges connected vehicles face and the developed solutions to address them.

2.1 The Importance of Security in Wireless Networks

The CIA triad stands for Confidentiality, Integrity, and Availability. With the addition of Authentication, it is commonly called CIA-A. This model is commonly used in developing security systems and is a basis for finding vulnerabilities and creating solutions. CIA-A helps guide security teams by separating the four ideas into focal points, making it easier to address each concern. When we meet all three standards, the organization's security profile is more robust and better equipped to handle threats.

- **Confidentiality**: Involves efforts to keep data private and prevent unauthorized access. Direct attacks, human error, or insufficient security controls can compromise Confidentiality. To fight against confidentiality breaches, organizations can classify and label restricted data, enable access control policies, encrypt data, and use Multi-Factor Authentication (MFA) systems.
- **Integrity**: Involves making sure data is authentic, accurate, and reliable. Compromising integrity can be done intentionally or accidentally. Organizations can use hashing, encryption, digital certificates, digital signatures, and employ trustworthy Certificate Authorities (CAs) to protect integrity. A method for verifying integrity is non-repudiation.
- **Availability**: Data is useless unless available to those who need it. Power outages, natural disasters, or deliberate sabotage can compromise availability. Organizations can use redundant networks, servers, and applications to ensure availability, upgrade software packages and security systems, and have backup and disaster recovery plans [10].
- **Authentication**: Authentication means that only authorized users should be able to access information. Key management and distribution are critical components of Authentication and must be adequate to meet system requirements [11].

2.2 Regulations and Safety Standards

2.2.1 American Federal Motor Vehicle Safety Standard

In 2015, the American National Highway Traffic Safety Administration's (NHTSA) proposed the establishment of the Federal Motor Vehicle Safety Standard (FMVSS) No. 150 for Vehicle to Vehicle (V2V) communication systems. The proposed rule would require certain passenger cars, Multipurpose Passenger Vehicles (MPVs), trucks, and buses having a gross vehicle weight rating of 4,536 kilograms or less to be equipped with V2V communication technology that sends and receives Basic Safety Messages (BSMs) to and from other vehicles. The proposed rule is extensive and covers various areas such as communication technology, BSM format and communication protocols, spectrum use, BSM authentication, misbehavior detection and reporting, cyber security, and consumer privacy. The NHTSA proposes to mandate Dedicated Short Range Communication (DSRC) technology for V2V communication and considers alternatives inter-operable with DSRC [12].
The NHTSA also proposes requirements for message authentication, misbehavior detection and reporting, and cyber-security to ensure a secure communication environment. The proposed rule would mandate that all V2V devices sign and verify their BSMs using a Public Key Infrastructure (PKI) based Security Credential Management System (SCMS) and performance requirements and test procedures for BSM transmission and the signing of BSMs. The agency also considers two alternatives; the first alternative does not specify architecture or technical requirements for message authentication, and a receiver of a BSM message must be able to validate the contents of a message to confirm that it originated from a single valid V2V device and was not altered during transmission. The second alternative does not propose a specific message authentication requirement, and BSM messages would be validated with a checksum or other integrity check, passed through a misbehavior detection system to filter malicious or misconfigured messages, and implementers would be free to include message authentication as an optional function [12].

2.2.2 European Standards and Regulations

The new Vehicle General Safety Regulation, which took effect on July 6, 2022, introduces mandatory advanced driver assistance systems and establishes the legal framework for approving automated and fully driverless vehicles in the European Union (EU). These safety measures aim to protect passengers, pedestrians, and cyclists, with an estimated impact of saving over 25,000 lives and preventing at least 140,000 severe injuries by 2038. The regulation empowers the European Commission to develop technical rules to approve fully driverless vehicles, positioning the EU as a pioneer in this field. Implementing these rules is expected to enhance public trust, drive innovation, and improve the competitiveness of Europe's car industry [13].
Within the European Union, there are many initiatives to utilize and advance V2X communication models to enhance road safety. One such initiative is the European Telecommunications Standards Institute Cooperative Intelligent Transport Systems (ETSI C-ITS), which aims to facilitate real-time information exchange between vehicles and infrastructure, enabling cooperative interactions and improving traffic efficiency and safety. Another notable initiative is VI-DAS, the Vision Inspired Driver Assistance System, which aims to design next-generation connected Advanced Driver Assistance Systems. VI-DAS leverages sensors, data fusion, machine learning, and cloud infrastructure advancements to better understand driver behavior, vehicle context, and scene analysis. These initiatives highlight the EU's commitment to using V2X communication

for enhanced road safety and advancing the capabilities of intelligent transportation systems [14], [15].

2.2.3 ISO/SAE 21434

The ISO/SAE 21434 is a cybersecurity standard for road vehicles, as described in the article by Macher et al. [16], which provides a comprehensive overview of the standard's key aspects and guidelines. The standard aims to establish a structured process for ensuring cyber secure design, reduce the potential for successful cyberattacks and the likelihood of losses, and provide consistent means of responding to cybersecurity threats across the global automotive industry. This standard is designed for road vehicles and sets minimum criteria for automotive cybersecurity engineering. The standard encourages a risk-oriented approach for prioritizing actions and systematically determining cybersecurity measures. ISO/SAE 21434 is structured into the following sections:

1) establishes the scope of the standard, outlining its intended application and purpose.
2) provides normative references, listing other standards for implementing automotive cybersecurity.
3) defines and explains the abbreviated terms and definitions used throughout the document to ensure consistent understanding.
4) is an informative section that describes the vehicle ecosystem, organizational cybersecurity management, and the overall automotive lifecycle. It provides context for the implementation of cybersecurity measures.
5) focuses on the organizational aspects of cybersecurity, including developing a cybersecurity strategy, policy, and objectives.
6) addresses risk management requirements, which involve assessing potential threats and determining their potential impact on road users.
7) is dedicated to the concept phase and covers defining cybersecurity goals based on threat analysis and risk assessment. It also specifies the cybersecurity requirements necessary to achieve those goals.
8) outlines the implementation and verification of cybersecurity requirements during the product development phase.
9) focuses on the automotive lifecycle's production, operation, and maintenance phases. It specifies requirements to ensure the implementation of cybersecurity measures in the produced item and covers cybersecurity activities conducted in the field.
10) describes supporting processes, including organizational processes necessary for effective cybersecurity implementation.

Section 8 focuses on product development and is divided into different phases: system development, hardware development, software development, verification and validation, and post-development release. Best practices for cybersecurity design mentioned include principles like least privilege, Authentication, authorization, and end-to-end security. System integration is verified through various methods such as requirement-based testing, interface testing, penetration testing, vulnerability scanning, and fuzz testing. Hardware design considerations include domain separation, self-protection, prevention of bypassing security functionalities, and secure initialization. Identifying and analyzing interfaces related to cybersecurity is essential to assess vulnerabilities and potential entry points for attacks.

2.3 V2X Communication

V2X communication systems consist of various communication modes, including vehicle-to-vehicle, vehicle-to-pedestrian (V2P), vehicle-to-infrastructure (V2I), vehicle-to-cloud (V2C), vehicle-to-network (V2N) as well as vehicle to infrastructure to vehicle (V2I2V) communications. These systems use either IEEE 802.11p-based technology operating in the 5.9 GHz frequency or LTE-based technology [4].

The IEEE 802.11p-based ad-hoc V2X communication approaches are DSRC in the United States and C-ITS in Europe. These technologies are already deployed in several countries and mainly use broadcast and unicast/multicast networking patterns suitable for various V2X applications. The physical transmission and Medium Access Control (MAC) for DSRC and C-ITS are the same based on IEEE 802.11p standards [4]. V2X communication enables vehicles to communicate with other vehicles, infrastructure, and vulnerable road users using different connectivity modes. V2X communication is facilitated by onboard units (OBUs) equipped with computational power and a networking protocol stack for exchanging information with neighboring vehicles and infrastructure located in their vicinity. OBUs use 802.11p/PC5 interfaces for direct communication in V2V, V2I, and V2P modes and the Uu interface for network-based communication in V2N mode. Roadside Units (RSUs) act as gateways between OBUs and the communication infrastructure, extending the short-range communication capabilities. RSUs also offer Internet access, security key distribution, and real-time traffic data distribution. Roadside users, such as pedestrians, cyclists, and motorcyclists, can participate in V2P communication using intelligent personal devices. Base stations facilitate V2N connectivity for V2X terminals by broadcasting received data from several V2X terminals using the Uu interface on the downlink. Edge/central cloud servers combine information from multiple sources at a central location, obtaining a holistic view of all connected entities, traffic information, roads, and infrastructure [5].

Messages are exchanged to support safety, traffic, and infotainment applications and are categorized into four types: periodic, local event triggered, global event triggered, and emergency vehicle messages. Each message type has a specific purpose and is sent through different communication links with varying latency levels [6].

2.4 IEEE 802.11p-based V2X Communication

2.4.1 DSRC

The DSRC technology is designed to support various vehicular communication-based applications and is under active development in the United States and other countries. DSRC is

mainly deployed to enable collision prevention applications, and the U.S. Department of Transportation estimates that DSRC-based V2V communication can prevent up to 82% of all crashes involving unimpaired drivers, potentially saving thousands of lives and billions of dollars [17].

DSRC-based V2X communication technologies have many potential benefits in improving road safety. The onboard system of a vehicle can provide the driver with feedback in the form of audio, visual, or haptic warnings to avoid potential collisions or hazards. The US Department of Transportation has collaborated with automakers to study the feasibility of V2V safety applications, such as forward collision warning, blind-spot warning, and emergency electronic brake lights. DSRC can also be used for other applications such as navigation assistance, electronic payments, and traffic updates [17].

DSRC utilizes IEEE 802.11p Wireless Access for Vehicular Environments (WAVE) at the Physical Layer (PHY) and MAC layers and a suite of IEEE 1609 standards at the middle of the stack for Channel Switching, Network Services, and Security Services, respectively. For the Network and Transport layers, DSRC supports Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) from the Internet Engineering Task Force (IETF). The choice between using the WAVE Short Message Protocol (WSMP) or IPv6+UDP/TCP depends on the specific application requirements, with WSMP being used for single-hop messages and IPv6 for multi-hop packets [17].

In order to support V2X communication, IEEE 802.11p provides guidelines for using the 5.9 GHz band that enables vehicles to exchange information with other vehicles, roadside infrastructure, and other devices. The standard specifies the PHY and MAC layer protocols for V2X communication, including message formats, packet structures, and transmission procedures. It also addresses channel access, security, and Quality of Service (QoS) [18]. The 5.9 GHz band is allocated by the FCC for DSRC operation in the United States and is divided into seven 10 MHz channels with a 5-MHz guard band at the low end. Pairs of 10 MHz channels can also be combined into a 20 MHz channel. The testing of DSRC in the US has focused on 10 MHz channels due to the desire to support many parallel types of applications, and physical testing suggests that this width is well-suited to the delay and Doppler spreads in the vehicular environment. However, it is an open question whether channel congestion concerns, particularly in the channel used for V2V safety communication, might be better addressed with the increased capacity of a 20 MHz channel [17].

2.4.2 ETSI C-ITS

ETSI C-ITS is a European standard for Cooperative Intelligent Transport Systems that aims to improve road safety, traffic efficiency, and environmental sustainability. It enables vehicles, infrastructure, and other road users to communicate, exchanging real-time information about traffic conditions, hazards, and events. This information can support various applications, such as collision avoidance, traffic management, and ECO-driving [15].

ETSI C-ITS uses various technologies, wireless communication, GPS, and sensors to gather and share data in real-time. Specifically, it uses the IEEE 802.11p wireless communication standard and the ETSI ITS-G5 protocol to enable communication between vehicles and infrastructure. The primary communication channel is a short-range wireless technology that operates on the 5.9 GHz frequency band, similar to the DSRC standard used in North America. It allows for direct communication between vehicles and infrastructure and between vehicles themselves. Cellular networks and satellite systems are used for more long-range communication and to provide coverage in areas where short-range communications are unavailable [15].

2.4.3 Network Security - IEEE 1609.2

The IEEE 1609.2 standard sets out Security Services (SS) for WAVE that provide Confidentiality, Integrity, and Authentication for DSRC and ETSI C-ITS communication. These SS mechanisms and procedures are implemented at the Network and Transport layers of the DSRC protocol stack. For Confidentiality, the standard uses symmetric key cryptography with a shared secret key established before communication begins. A MAC code mechanism is used to ensure message integrity. The standard uses digital certificates issued by a trusted Certificate Authority (CA) to authenticate vehicles and infrastructure, containing the public key, identity, and CA digital signature. Using Security Services Protocol Data Units (SPDUs) and security certificates, DSRC devices can securely perform safety-critical operations such as collision avoidance and emergency response. [19].

Safety messages are transmitted in a non-encrypted format, while security information messages are encrypted. Strong elliptic curve cryptographic mechanisms are used, and certificates are pseudonymized to protect privacy. However, the protocol is vulnerable to various critical attacks, for example, malware, black hole, GPS spoofing, and DoS. Additionally, the limited bandwidth and channel capacity of the 802.11p standard limit the applicability of matured security solutions from other communication systems [5].

DSRC also suffers from short-range characteristics and limited line-of-sight communications, resulting in intermittent connectivity when moving at high speeds. The channel access mechanism in DSRC results in significant channel access delay in high vehicular traffic scenarios, and the absence of a handshake and acknowledgment mechanism leads to a hidden node problem, resulting in poor link performance and unreliable broadcast service [20].

2.5 Cellular-V2X Communication

Cellular-V2X (C-V2X) communication includes cellular-based communication such as LTE, 5G, and in the future, most likely, 6G.

2.5.1 LTE-V2X

LTE-V2X communications involve V2V, V2I, V2N, and V2P communications, which allow vehicles to exchange information directly or with the help of infrastructures such as Evolved Node B (eNB) or RSUs. RSUs can broadcast information related to an emergency scenario or traffic condition to a group of user equipment. V2N communications involve vehicular UE and serving entities for V2N applications. The EPC of the LTE network can connect to an ITS server for various vehicular services. V2P supports the exchange of messages between vehicles and pedestrians [20].

The 3GPP developed cellular standards for V2X communication based on LTE technology, which has evolved into the 5G NR-V2X standardized in Release 16. The 3GPP specifies the lower layers of the C-V2X protocol, while the upper layers are reused from DSRC and ETSI C-ITS standards. This layer separation allows existing applications developed on DSRC or ETSI C-ITS to be used with C-V2X, ensuring interoperability. C-V2X provides two radio interfaces, Uu and PC5, to support various vehicular use cases [5].

The Uu interface operates within the coverage area of the base station and is used for V2I and V2N communication. It allows long-range dissemination of V2X messages through the cellular core network but is more suitable for latency-tolerant use cases. The PC5 interface enables direct communication between vehicles, roadside units (RSUs), and other road users without routing every message through the base station. It is ideal for time-critical safety use cases, offering low latency communication with enhanced range, reliability, and non-line-of-sight performance. The PC5 interface supports both centralized and decentralized scheduling modes, allowing vehicles to operate with or without cellular coverage [5]

Some advantages LTE-V2X communications offer over DSRC-based V2X communications are that LTE provides ubiquitous coverage for V2I/V2N services, supports high mobility of vehicles, prevents hidden node problem, supports efficient safety message dissemination, performs better in NLOS environments, and has a high data rate and capacity [20].

2.5.2 Cellular-V2X Security

In LTE-V2X, security features include Authentication, authorization, and encryption for PC5 and Uu interfaces. 5G-V2X can leverage similar security functionalities, but specific security requirements for NR-PC5 are not defined. Integrating SDN and NFV in 5G introduces new security challenges, and measures have been standardized to enhance security and privacy in various domains. However, security and performance remain important concerns for the successful deployment of 5G-V2X systems [5].

2.5.3 5G-V2X

The 5G-V2X technology introduces enhancements to the existing C-V2X technology, providing improved reliability, lower latency, higher throughput, and enhanced positioning for vehicular communication. These enhancements aim to support advanced V2X use cases, including advanced and autonomous driving, without relying solely on the cellular network. The NR-PC5 sidelink, a short-range direct communication mode, is a key feature of 5G V2X, offering robust V2X operation even without GPS coverage and providing time synchronization for effective communication [5].

2.6 Control Area Network

BOSCH developed the Control Area Network (CAN) as a multi-master message broadcasting system with a maximum signaling rate of 1 megabit per second [21]. Unlike traditional communication systems, CAN broadcasts many short messages to the entire system, and all devices on the network can decide whether a message is relevant or not. This structure allows modifications to the network with minimal impact and non-transmitting nodes to be added without modifying the network [22].

2.6.1 CAN Messages

CAN messages have a priority feature that helps determine which message gets transmitted first when multiple messages are sent simultaneously. This priority feature ensures that the highest priority message is transmitted smoothly without any interruptions [22]. CAN also has error capabilities where each frame's contents are checked for errors using a Cyclic Redundancy Code (CRC). If a frame has errors, it is disregarded by all nodes, and an error frame can be transmitted to signal the error to the network. The controller can differentiate between global and local errors. If too many errors are detected, individual nodes can stop transmitting errors or disconnect themselves from the network completely [22].

CAN is a decentralized network architecture where any node can write a CAN frame onto the network if the bus is idle. The transmitted CAN frame does not contain addresses for transmitting or receiving nodes but rather a unique arbitration ID that all nodes receive. Each node determines whether to accept the frame based on this ID. If multiple nodes transmit simultaneously, the node with the highest priority (i.e., the lowest arbitration ID) gains bus access, ensuring deterministic communication among the nodes [22].

2.6.2 On-Board Diagnostics

The Onboard Diagnostic (OBD-II) port is a 16-pin connector in all modern cars that provides access to the CAN bus. It was initially created to be used by mechanics for downloading diagnostic data and running tests. However, a market is now emerging to allow car owners to access the same data via their mobile devices or over the Internet. The OBD-II port provides raw access to the CAN bus, potentially allowing direct manipulation of CAN traffic in the vehicle. This CAN bus access can result in control over safety-critical functions [23].

2.6.3 Electronic Control Unit

Electronic Control Units (ECUs) entered production vehicles in the late 1970s to improve efficiency and reduce pollutants

in response to the California Clean Air Act and to increase gasoline prices. Since then, ECUs have been integrated into every aspect of a car's functioning, including the throttle, transmission, brakes, passenger climate, lighting controls, external lights, and entertainment. The amount of software in luxury sedans has grown from virtually nothing to tens of millions of lines of code spread across 50-70 independent ECUs. Many features require complex interactions across ECUs, such as Electronic Stability Control (ESC) systems and Active Cruise Control (ACC) systems, which monitor individual wheel speed, steering angle, throttle position, and various accelerometers. The typical car contains multiple buses, generally based on the CAN standard, covering different component groups. Such buses could be physically isolated but are "bridged" to support subtle interaction requirements [24].

3. Common Wireless Threats in Modern Automotive Systems

The increasing use of V2X communication in connected vehicles has introduced new possibilities for cyber attackers to exploit vulnerabilities and launch wireless attacks that can compromise the confidentiality, integrity, availability, and authentication of V2X systems. This section will discuss some of the most common wireless attacks that can target V2X communication systems. We present currently known vulnerabilities, some known ways these attacks could be performed, and some real-life scenarios where vehicles have already been attacked.

3.1 Common Types of Wireless Attacks

Modern cars face an array of wireless attacks that can threaten their security. In this subsection, some of the most common wireless attacks will be presented, such as jamming, replay attacks, spoofing, and Man-in-the-Middle (MitM) attacks.

3.1.1 Eavesdropping

Eavesdropping is an attack in which an unauthorized third party attempts to intercept the communication between two legitimate parties. The eavesdropper aims to access sensitive information transmitted over the communication channel, including confidential or private data [29]. Broadcast messages in IEEE 802.11p are considered non-confidential, but location-based and transactional data are encrypted. In LTE-V2X, communication is encrypted using pre-shared secret keys issued by the authentication center, making it difficult for external attackers to collect information [6].

An eavesdropping attack can be performed by intercepting CAN frames broadcast to all nodes on an in-vehicle network. These can be accessed via interfaces like the OBD port or telematics system. By analyzing the historically recorded frames, attackers can discover different functions and weaknesses on selected ECUs using a custom program such as CarShark, built to intercept frames and data sent by the CAN system [1].

3.1.2 Black-hole/Grey-hole Attack

In a black-hole attack, an attacker drops all packets they receive, while in a grey-hole attack, the attacker drops a percentage of packets to avoid detection. Both attacks create a hole in the network where no packets can move through. The IEEE 802.11p authentication process can prevent external attackers but not internal attackers. LTE-V2X eliminates external attackers through mutual authentication between UEs and the core network, but internal attackers are still possible in some cases. When two UEs are out of network coverage, communication with other UEs with revoked credentials is possible. In partial D2D coverage, a compromised relaying node could drop packets and block communication with eNB. The broadcast of warning packets can help reduce the effect of the attack due to the diffusion of multiple copies over the network [6].

3.1.3 Man-in-the-Middle

The MitM attack involves a malicious node intercepting V2V, V2I or V2N communications. There are two different types of MitM attacks: passive and active. In an active MitM attack, the attacker can, for example, inject false information and drop or delay messages. In a passive MitM attack, an attacker eavesdrops on the communication between legitimate vehicles without altering the content. By positioning themselves in the middle, the attacker gains control over the communication link while the communicating vehicles remain unaware of the breach of privacy. This attack can lead to various consequences, such as map poisoning, where false content is injected into the map database, causing incorrect navigation instructions or unavailability of critical information [5].

3.1.4 Denial of Service

A Denial of Service (DoS) attack involves flooding a host with excessive information to overwhelm it, making the host incapable of receiving or processing legitimate data. In vehicular networks, the RSU is the primary target for attackers since it handles the authentication, management, and updating of vehicles and their data. Blocking the attacker's IP address is the simplest way to prevent DoS attacks. However, attackers can use multiple IP addresses in distributed attacks, making it challenging to mitigate and combat these attacks. They can be performed on both RSUs and other vehicles on the network, making them more challenging to block [11].

IEEE 802.11p MAC is vulnerable to flooding attacks as the attacker can exploit the so-called binary exponential back-off scheme and the network allocation vector field. In LTE-V2X, the attacker can use resource scheduling information, inject packets during the UE's active mode, or impersonate other UEs to send fake reports, causing flooding attacks. Flooding attacks can cause a delay in transmitting data, cause a conflict at eNB, and eNB may stop accepting new requests [6].

3.1.5 Jamming

Jamming attacks can be used to corrupt data or jam channels, which can affect both IEEE802.11p and LTE-V2X physical

TABLE I
SUMMARY OF WIRELESS ATTACKS AND V2X COMMUNICATION SYSTEMS.

Attack	Compromised Security Requirement(s)	Layer(s)	Internal or External	Active or Passive	Reference(s)
Eavesdropping	Confidentiality, Privacy	Physical	External	Passive	[25], [5],[1],[6]
Black-hole/Grey-hole Attack	Integrity, Availability	Application, Transport, Network	External	Active	[6],[26],[11]
MitM	Confidentiality, Integrity, Availability, Authentication	Application, Transport, Network, Data Link, Physical	External	Active	[5],[27]
DoS	Availability	Application, Transport, Network, Data Link, Physical	External	Active	[5],[25],[4],[1],
Jamming	Availability	Physical	External	Active	[5],[4],[1],[6]
Spoofing	Authentication	Physical	External	Active	[5],[1],[6]
Message Tampering	Integrity	Application, Transport, Network, Data Link, Physical	External	Active	[5],[6],[4],
Replay Attacks	Integrity	Application, Transport, Network, Data Link	External	Active	[28],[5],[4],[1],[6],[11]
Impersonation	Authentication, Integrity	Application, Transport, Network, Data Link	Internal	Active	[6],[5],[11]

layer, as they are both based on orthogonal frequency-division multiplexing. The use of directional antennas can reduce the impact of this type of attack and allow vehicles to avoid the jamming area [6]. GPS jamming occurs when an adversary blocks GPS signals. Although the selling or use of GPS jamming equipment is illegal in most parts of the world, it can also be achieved through legal and low-cost Software Defined Radio [1].

3.1.6 Spoofing

Spoofing is an attack where the attacker sends fake signals to deceive the receiver. GPS spoofing happens when someone uses a radio transmitter to send counterfeit GPS signals to a receiver antenna to counter a legitimate GPS satellite signal. Advanced GPS spoofing techniques now make cars vulnerable to GPS signal spoofing. Spoofing attacks can also occur when the compromised node sends messages with a fake location or time. Message spoofing attack is another type of spoofing where the attacker provides incorrect location information to the vehicles in the network. Spoofing attacks may facilitate other attacks where vehicle identification is used as the tool for launching attacks. To prevent spoofing attacks from being carried out, plausibility checks are required to detect the fake location and time [1], [6], [2].

3.1.7 Message Tampering

Message tampering attacks involve spreading bogus or modified messages that harm vehicles and put them in danger. In IEEE 802.11p, internal attackers may use their digital certificates to sign false messages, but detection schemes can include them in certificate revocation lists. In LTE-V2X, external attackers cannot inject or alter packets due to encryption, but internal attackers can inject false information as the integrity algorithm is only applied on signaling packets [6].
Attackers can perform message tampering attacks using the methods of frame falsifying and frame injection. With frame falsifying, attackers can design their attack by sending fake frames with false data through the CAN bus to mislead corresponding legitimate ECUs. Attackers can also perform frame injection by using a malicious node as a starting point, such as a laptop, reprogrammed ECU, or infected telematics system, and setting appropriate frames' ID to make the target

node on the CAN bus accept these fake frames. These attacks can lead to incorrect information displayed on the instrument panel cluster, which may fool the driver and cause dangerous behaviors [1].

3.1.8 Replay attacks

Replay attacks are a variant of MitM attacks where valid transmission data is repeated or delayed, often targeting communications between vehicles and RSUs in vehicular networks. Intercepting a message containing the encryption key or password would enable an attacker to authenticate itself later, and these attacks are difficult to mitigate since it is almost impossible for a vehicle or RSU to detect an ongoing attack. Mitigation methods include strong encryption, virtual private networks, and time-delay variation. Replay attacks can be particularly effective, allowing attackers to send valid frames to the CAN bus and perform various actions, such as starting the engine and driving the car away [11], [1].

3.1.9 Impersonation

Impersonation attacks in vehicular networks involve malicious nodes that mimic RSUs or other vehicles to deceive users into disclosing their authentication information. The attackers could then use this information to access classified data or to impersonate other parties. Attackers could gain priority and reduce network congestion by impersonating an emergency vehicle. Encryption, localization, and clustering are among the mitigation strategies to counter impersonation attacks [11]. For LTE-V2X systems, a malicious vehicle can impersonate a legal vehicle and gain access to the LTE-V2X system by sending the victim vehicle's identity and certificate to a legal eNodeB during the authentication procedure. As a result, the malicious vehicle is regarded as legitimate, enabling it to transmit fake V2X messages and potentially spread false traffic information or disrupt the stability of a platoon from the inside [30].

3.2 Methods of Carrying Out Wireless Attacks

There are several ways wireless attacks could be performed, most of them by finding vulnerabilities in a car's communication interfaces. The attacks can be performed via indirect physical access, short-range wireless access, and long-range wireless access [31].

3.2.1 Indirect Physical Access

A car can be attacked via indirect access using the OBD port, CD player, and USB port. The OBD port can be attacked by compromising the diagnostic device being plugged into it. At the same time, the CD player can be tricked into installing malicious software by inserting a CD with a specific name or playing a malicious music file. Similarly, a corrupted file on a USB key or a compromised device like a smartphone can also perform an attack against the ECU it is connected to [31].

3.2.2 Short Range Wireless Access

Short-range attacks can be direct or indirect and involve short-range wireless communication technologies. Examples include wireless pairing of mobile devices, car-to-car communications, TPMS, and wireless unlocking. These attacks can lead to data retrieval, eavesdropping, and the compromise of the ECU responsible for the communication network. Some attacks can also be extended beyond their short range through relays or more powerful antennas [31].

3.2.3 Long Range Wireless Access

Access via this medium requires a long-range transmission channel and the compromise of an intermediary device. One example is the app store provided by some car manufacturers. A successful attack against the online store or a program sold on it containing a Trojan horse could have serious large-scale consequences. Another example is the installation of a backdoor into an ECU of a vehicle compromised through any of the previously described attacks. Broadcasts of certain signals can trigger the execution of a series of instructions in any compromised vehicle in the range of these broadcasts. Catastrophic scenarios can be imagined by combining such techniques with a significant number of previously infected vehicles [31].

3.3 Components of Modern Automated Cars

Modern cars have interconnected layers, including the Sensing, Communication (e.g., using a CAN bus), and Control layers. Compromising any of these layers can result in serious security breaches [1]. Note that this paper primarily focuses on attacks against the communication layer of modern automated cars. However, it is essential to acknowledge the severe nature of attacks against the sensing and control layers and highlight their potential consequences. Attacks on the communication layer can serve as a gateway to compromising the entire vehicle system, including its sensing and control functionalities.

a) Sensing Layer

Various types of attacks can be carried out on the sensing layer of autonomous vehicles, including GPS jamming and spoofing attacks, Millimeter Wave (MMW) attacks, LiDAR sensor attacks, ultrasonic sensor attacks, and camera sensor attacks. Countermeasures depend on the type of sensor being used and include strategies such as advanced signal-processing-based techniques, encryption-based defenses, moving MMW radar frequency to over 100 GHz, combining multiple wavelength LiDAR, and using V2V communication. It is important to note that even with these countermeasures in place, determined attackers with large budgets may still be able to carry out successful attacks [1].

b) Communication Layer

Due to the lack of encryption and authentication in the in-vehicle communication layer, attackers can intercept CAN frames and sniff for important information, falsify frame data to mislead ECUs, inject frames with false information, perform replay attacks, and launch denial of service attacks. The absence of authentication and encryption in the CAN bus

system allows attackers to access a malicious node, such as a laptop, reprogrammed ECU, or telematics system infected by malware. Without proper security measures, these attacks can cause dangerous behavior or even harm to drivers and passengers. Adding encryption and authentication to enhance in-vehicle network security can provide confidentiality and reliability for CAN frames. However, it is a complex process that requires efficient key management to prevent attackers from accessing private keys. Furthermore, implementing authentication and encryption can degrade transmission efficiency, potentially affecting time-critical components, and must be balanced with security needs [1].

c) Control Layer

There are potentially life-threatening dangers of attacks on the control layer of a vehicle since it is responsible for the steering, brakes, engine, and transmission. Compromising this layer can have catastrophic consequences, especially when the car moves on a highway. The vulnerability of the control layer is highlighted when both the sensing and communication layers are compromised, as attackers can trick the car into ignoring the message sent by the sensors, putting the driver and other road users at risk. Some control layer attacks are control override, injection, and in-vehicle network access attacks. Some measures to counter this include implementing code obfuscation and proper code signing of new firmware to prevent malicious code and ensuring that only certified and well-tested apps can connect with the car's internal organs via smartphone technology [1].

d) CAN Security Issues

The CAN protocol has inherent weaknesses, such as its broadcast nature, which allows a malicious component to snoop on all communications or send packets to any other node on the network. It is also vulnerable to DoS attacks and does not contain authenticator or source identifier fields, making distinguishing between legitimate and malicious components difficult. These weaknesses can be exploited to control all the other components on the bus through a single compromised component [24].

In [24], the authors gained control of various electronic components in a modern automobile, including the brakes, engine, and door locks, using only a laptop computer and an off-the-shelf radio. Several vulnerabilities were identified and exploited by sending specially crafted CAN packets over the car's CAN bus, which is the primary communication network used by the car's various ECUs. An attacker could access the car's internal network through physical access to the OBD-II port or by inserting a malicious component into the car's parts supply chain.

Eavesdropping on the CAN bus in vehicles is possible due to the lack of encryption, allowing adversaries to gather information by sniffing CAN frames. Eavesdropping attacks can be seen as a gateway to more significant attacks. In one study, researchers used captured CAN frames to identify the ID of a specific node they planned to attack. They then implemented a DoS attack by manipulating the data from the parking sensor. Eavesdropping attacks also put personal information is also at risk. In a separate study, researchers identified the vehicle's driver solely based on the sensory data transmitted through the CAN bus, even with just one piece of data, such as the brake pedal [25].

3.4 Examples of Attack Scenarios

In recent years, many attacks and vulnerabilities have emerged targeting vehicles utilizing V2X communication. These attacks exploit various techniques, as discussed in 3, to manipulate messages and disrupt traffic flow, posing potential risks to the safety of drivers and passengers alike.

a) The Jeep Cherokee Hack

In 2015, researchers Miller and Valasek successfully executed a remote hack on a Jeep Cherokee, demonstrating the vulnerability of modern cars. Using the Uconnect feature, an Internet-connected computer system in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks, the researchers were able to gain access to the vehicle's internal computer network, known as a CAN bus, from anywhere in the country through the car's cellular connection. Once inside the network, they silently rewrote the firmware of the entertainment system's chip, allowing them to send commands to physical components like the engine and wheels [32]. Although the researchers limited the release of their tool, many of the dashboard hijinks and GPS tracking that they demonstrated are possible with the code they published. They shared their research with Chrysler for nine months, allowing the company to release a patch before the Black Hat conference. Chrysler acknowledged the vulnerability and committed to providing customers with the latest software updates to secure their vehicles against potential vulnerabilities. This research highlights the potential risks and vulnerabilities of the connected car, urging car manufacturers to prioritize security measures in their designs [32].

b) Keyless Car Theft Attack

Modern cars use keyless entry systems, allowing users to lock and unlock their vehicles without physical keys, which has introduced new vulnerabilities to modern cars. Remote Keyless Entry (RKE) systems utilize unidirectional Radio Frequency (RF) transmission between a key fob and the car. In traditional RKE systems, a fixed code was used, making them susceptible to replay attacks. Rolling codes were introduced to address this, generating a unique code for each operation. However, even rolling code-based systems are not immune to attacks, as demonstrated by the RollJam attack by Samy Kamkar. These attacks, which can be conducted with relatively cheap hardware and software, highlight the need for effective countermeasures. To mitigate these threats, an authentication mechanism based on hashing and asymmetric cryptography could be used to enhance security for RKE systems [28].

c) Tesla Autopilot Hack

Keen Security Lab conducted security research on Tesla vehicles and shared their findings at Black Hat USA conferences in 2017 and 2018, as described in [33]. Building on their previous work, they analyzed the Tesla Autopilot ECU (APE) and its CAN messaging functions. By exploiting a design weakness in the lane recognition system while the vehicle was in Autosteer

mode, they successfully gained remote control of the steering system without physical contact.

In addition, the researchers developed an optimization algorithm to create adversarial examples that disrupted the auto wipers function, which relied solely on camera data. They demonstrated the effectiveness of their adversarial example attack in the physical world. Furthermore, they identified a potential risk in the lane recognition system, showing that minor changes on the road could mislead the Tesla car into the reverse lane.

The research contributions can be summarized as follows: Firstly, they demonstrated the ability to remotely gain root privilege of the APE and control the steering system. Secondly, they successfully disrupted the auto wipers function using adversarial examples in real-world conditions. Lastly, they showed the potential for misleading Tesla vehicles into the reverse lane with minimal road modifications. Through their research, Keen Security Lab highlighted the importance of addressing these vulnerabilities to enhance the security and safety of Tesla vehicles equipped with Autopilot.

3.5 Attack Motivation and Capabilities

In analyzing the attacker's capabilities and motivations within a network, an attacker's model is defined based on three dimensions: internal and external, malicious and rational, and active and passive, as defined in [34]. This paper focuses on analyzing internal and external attacks and classifying them as active or passive and also works under the assumption that all attackers have malicious intent.

Internal attacks are initiated by fully authorized nodes that bypass the authentication model, allowing them to exploit vulnerabilities and launch attacks. External attacks are launched by unauthorized nodes that do not have legitimate access to the network. In the case of external attacks, implementing a secure authorization model can help minimize their impact [6].

The distinction between internal and external is essential in understanding network attacks. Internals (or insiders) are authenticated members of the network who have legitimate access and can communicate with other members. They typically possess a certified public key, which gives them more extensive opportunities to exploit vulnerabilities and launch attacks. Insiders may also have insider knowledge of the network and its specific protocols. In contrast, externals (or outsiders) face limitations in the diversity of attacks they can execute because they need more authorized access and insider knowledge [34].

A malicious attacker has the goal of causing harm to the network's members or disrupting its functionality without any personal benefit. Their primary focus is inflicting damage, and they are willing to use any means necessary, disregarding the costs and consequences involved. On the other hand, a rational attacker seeks personal gain from their attacks, making their behavior more predictable. Their actions are driven by the pursuit of personal profit, which influences their choice of attack methods and targets [34].

An active attacker can generate malicious packets or signals, directly interacting with the network infrastructure or targeted devices. They can launch different types of attacks, including injecting false data, modifying messages, or initiating DoS attacks. A passive attacker adopts a passive approach, primarily focusing on eavesdropping and monitoring the wireless communication channel. Their objective is to intercept and analyze network traffic, intending to gather sensitive information without actively disrupting the network's operations [34].

3.6 Countermeasures

To address the vulnerabilities of the V2X communication protocols, researchers and practitioners have developed a range of countermeasures to mitigate the risks associated with wireless attacks.

3.6.1 Cryptography

We can use several encryption schemes to protect the V2X communication network. Symmetric encryption involves using a single key to both encrypt and decrypt data. It is simple and fast, making it suitable for storing data in a centralized location. However, it is less commonly used for point-to-point communication. On the other hand, asymmetric encryption uses a two-key system where a public key is used to encrypt data, and a private key is used to decrypt it. It is slower than symmetric encryption but offers enhanced security. Different authentication and secure communication methods in vehicular networks are proposed using asymmetric encryption [11].

Public Key Infrastructure (PKI) based asymmetric cryptography is a security approach that involves a trusted third party managing public keys and ensuring security in C-ITS. It comprises computer systems, policies, and people handling public key certificates. The IEEE 1609.2 standard recommends using PKI for secure V2X communication. The standard specifies using ECDSA (Elliptic Curve Digital Signature Algorithm) for fast authentication and non-repudiation, despite the computationally intensive operations it requires [5].

Cryptography-based solutions could protect against attacks on V2X networks such as DoS, MitM, impersonation, and replay attacks [5]. However, these solutions may not be practical due to challenges in managing and maintaining keys in a decentralized and heterogeneous environment. Moreover, the limited capabilities of sensors and transceivers in V2X networks make sophisticated encryption techniques not easy to implement [29].

3.6.2 Network Security

The security of CAN and ECUs in vehicles is lacking, rendering them vulnerable due to their connections to external devices and various communication technologies. Intrusion Detection Systems (IDSs) are recommended to mitigate these risks, with two main types: signature-based detection, which compares incoming data to known attack signatures, and anomaly-based detection, which identifies deviations from normal behavior [11].

Various studies propose IDS techniques for securing intelligent cars. Signature-based IDSs target specific attacks, while

anomaly-based IDSs use methods like clock-based analysis, statistics, or machine learning algorithms to detect abnormal communication network behavior [11].

However, these techniques face challenges. Signature-based detection may struggle with new or unknown attacks, resulting in high false-negative rates. Anomaly-based detection encounters difficulties in defining accurate baselines, leading to high false-positive rates. Nonetheless, ongoing advancements in data analysis and machine learning are expected to improve the performance of these approaches, addressing the security concerns in intelligent cars [11].

4. Conclusion

In conclusion, wireless attacks on modern cars present significant security threats that require attention and countermeasures to ensure the safety and privacy of vehicle owners. The complexity of implementing these attacks varies, but vulnerabilities in communication interfaces, such as the CAN bus, make eavesdropping, message tampering, and other attacks relatively straightforward. The effects of these attacks can be wide-ranging and potentially dangerous, compromising confidentiality, disrupting communication networks, and even enabling unauthorized access or control over critical vehicle functions. Mitigating these attacks requires a comprehensive approach that combines technological advancements and security measures, including encryption, authentication, integrity algorithms, localization, clustering, and warning systems. The examples of the Jeep Cherokee Hack, the Tesla Autopilot Hack, and the Keyless Car Theft Attack highlight the vulnerabilities associated with increased connectivity in vehicles and emphasize the need for enhanced security measures.

Taking a proactive stance towards security is crucial, and understanding the motivations and intentions of attackers is essential for assessing risks and implementing effective countermeasures. Categorizing attackers based on their internal or external status, malicious or rational behavior, and active or passive engagement provides insights for tailoring defenses and strategies.

The ISO/SAE DIS 21434 standard provides valuable guidelines for automotive cybersecurity, offering a risk-oriented approach to identify and mitigate threats. Although it does not explicitly address wireless attacks, incorporating the standard's processes and maintaining effective communication channels between cybersecurity and functional safety engineering can enhance cybersecurity in the automotive industry. By learning from past attacks, implementing robust security measures, and following a systematic approach, the industry can work towards building safer and more secure vehicles, ensuring the protection of drivers, passengers, and their data.

Acknowledgment

ArchitectECA2030 receives funding within the Electronic Components and Systems For European Leadership Joint Undertaking (ESCEL JU) in collaboration with the European Union's Horizon2020 Framework Programme and National Authorities under grant agreement 877539. All ArchitectECA2030-related communication reflects only the author's view, and the Agency and the Commission are not responsible for any use that may be made of the information it contains. The work was partially funded by the Austrian Federal Ministry of Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK) under the program "ICT of the Future" project 877587.

References

[1] S. G. Philipsen, B. Andersen, and B. Singh, "Threats and attacks to modern vehicles," in *2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 2021, pp. 22–27.

[2] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," *Computer Networks*, vol. 169, p. 107093, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619305857

[3] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for v2x communications," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 244–266, 2020.

[4] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (v2x) communication platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693–713, 2020.

[5] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of v2x cybersecurity mechanisms and future research paths," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 325–391, 2023.

[6] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for v2x communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128618306157

[7] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in v2x communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, jan 2023. [Online]. Available: https://doi.org/10.1145/3558052

[8] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (v2x) testing," *Sensors*, vol. 19, no. 2, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/2/334

[9] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209617302267

[10] Fortinet, "Cia triad," https://www.fortinet.com/resources/cyberglossary/cia-triad.

[11] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, "Attacks and defences on intelligent connected vehicles: a survey," *Digital Communications and Networks*,

vol. 6, no. 4, pp. 399–421, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S235286481930197X

[12] N. H. T. S. Administration, "FMVSS No. 150 Vehicle-To-Vehicle Communication Technology For Light Vehicles," *Federal Register*, vol. 80, no. 96, pp. 28 958–28 989, 2015. [Online]. Available: https://www.federalregister.gov/documents/2015/05/13/2015-08880/federal-motor-vehicle-safety-standards-vehicle-to-vehicle-communications

[13] E. Commission, "New rules to improve road safety and enable fully driverless vehicles in the eu," Press Release. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312

[14] EUROPEAN COMMISSION, Innovation and Networks Executive Agency, "VI-DAS: Vision Inspired Driver Assistance System," Horizon 2020 Research and Innovation Programme, Brussels, Deliverable Grant Agreement Nr 690772, September 2020, specifications of the network and cloud infrastructure. [Online]. Available: https://cordis.europa.eu/project/id/690772

[15] E. Commission, "Study on the deployment of c-its in europe: Final report," Framework Contract on Impact Assessment and Evaluation Studies in the Field of Transport, Technical report MOVE/A3/119-2013/Lot No 5 "Horizontal", 2017.

[16] G. Macher, C. Schmittner, O. Veledar, and E. Brenner, "Iso/sae dis 21434 automotive cybersecurity standard - in a nutshell," in *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops*, A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, and P. Ferreira, Eds. Cham: Springer International Publishing, 2020, pp. 123–135.

[17] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[18] IEEE, "Ieee standard for wireless access in vehicular environments (wave) - resource manager - amendment 6: Wireless access in vehicular environments," *IEEE Std 802.11p-2010*, 2010.

[19] "Ieee approved draft standard for wireless access in vehicular environments–security services for applications and management messages," *IEEE Std 1609.2-2022 (Revision of IEEE Std 1609.2-2016)*, pp. 1–349, 2023.

[20] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and solutions for cellular based v2x communications," *IEEE Communications Surveys Existing & Tutorials*, vol. 23, no. 1, pp. 222–255, 2021.

[21] S. Corrigan, "Introduction to the controller area network (can)," *Texas Instruments*, 2007.

[22] N. Instruments, "Controller area network (can) overview." [Online]. Available: https://www.ni.com/sv-se/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/controller-area-network--can--overview.html

[23] D. Klinedinst and C. King, "On board diagnostics: Risks and vulnerabilities of the connected vehicle," CERT Division, Software Engineering Institute, Carnegie Mellon University, Tech. Rep., April 2016.

[24] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[25] M. Bozdal, M. Samie, and I. Jennions, "A survey on can bus protocol: Attacks, challenges, and potential solutions," in *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 2018, pp. 201–205.

[26] Y. Wang, Z. Qi, X. Sun, Z. Xiang, and Y. Chen, "Recent development of security issues of black hole and gray hole attacks in v2x network," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 2020, pp. 1–6.

[27] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors (Basel)*, vol. 18, no. 11, p. 4040, 2018. [Online]. Available: https://doi.org/10.3390/s18114040

[28] R. P. Parameswarath and B. Sikdar, "An authentication mechanism for remote keyless entry systems in cars to prevent replay and rolljam attacks," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, 2022, pp. 1725–1730.

[29] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for v2x communication," 2020.

[30] P. Zhu, K. Zhu, and L. Zhang, "Security analysis of lte-v2x and a platooning case study," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 532–537.

[31] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 2013, pp. 1–12.

[32] A. Greenberg. (2015, July) Hackers remotely kill a jeep on the highway—with me in it. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[33] T. K. S. Lab, "Experimental security research of tesla autopilot," 2021. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf

[34] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *2007 2nd International Conference on Pervasive Computing and Applications*, 2007, pp. 424–429.