Accident Analysis and Prevention 148 (2020) 105837

Contents lists available at ScienceDirect

Accident Analysis and Prevention

journal homepage: www.elsevier.com/locate/aap

Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions

Shah Khalid Khan *, Nirajan Shiwakoti, Peter Stasinopoulos, Yilun Chen

School of Engineering, RMIT University, Carlton, Victoria 3053, Australia

ARTICLE INFO

Keywords:
Connected and autonomous vehicles (CAVs)
Electronic control units (ECUs)
Cybersecurity
CAVs communication framework
Driverless cars

ABSTRACT

Modern-day Connected and Autonomous Vehicles (CAVs) with more than 100 million code lines, running up-to a hundred Electronic Control Units (ECUs) will create and exchange digital information with other vehicles and intelligent transport networks. Consequently, ubiquitous internal and external communication (controls, commands, and data) within all CAV-related nodes is inevitably the gatekeeper for the smooth operation. Therefore, it is a primary vulnerable area for cyber-attacks that entails stringent and efficient measures in the form of "cybersecurity". There is a lack of systematic and comprehensive review of the literature on cyber-attacks on the CAVs, respective mitigation strategies, anticipated readiness, and research directions for the future.

This study aims to analyse, synthesise, and interpret critical areas for the roll-out and progression of CAVs in combating cyber-attacks. Specifically, we described in a structured way a holistic view of potentially critical avenues, which lies at the heart of CAV cybersecurity research. We synthesise their scope with a particular focus on ensuring effective CAVs deployment and reducing the probability of cyber-attack failures. We present the CAVs communication framework in an integrated form, i.e., from In-Vehicle (IV) communication to Vehicle-to-Vehicle (V2X) communication with a visual flowchart to provide a transparent picture of all the interfaces for potential cyber-attacks. The vulnerability of CAVs by proximity (or physical) access to cyber-attacks is outlined with future recommendations. There is a detailed description of why the orthodox cybersecurity approaches in Cyber-Physical System (CPS) are not adequate to counter cyber-attacks on the CAVs. Further, we synthesised a table with consolidated details of the cyber-attacks on the CAVs, the respective CAV communication system, its impact, and the corresponding mitigation strategies. It is believed that the literature discussed, and the findings reached in this paper are of great value to CAV researchers, technology developers, and decision-makers in shaping and developing a robust CAV-cybersecurity framework.

1. Introduction

In the last few decades, the transition of automotive systems from electromechanical to electronic and software-driven systems has changed the dynamics of the automotive vehicle industry. There is a massive increase in the software-contents due to built-in applications in the vehicle's Electronic Control Units (ECUs) (Möller and Haas, 2019). This is attributed to the enhanced sophistication of the fundamental control systems but is also representative of more technological growth than hardware advancement, and these innovations are primarily occurring in the automobile, electronics, software, and telecommunications sectors, as shown in Fig. 1. This boom aims to adopt the emerging technologies developed for fully automated cars, predictive intelligence, Advanced Driver Assistance System (ADAS), V2X communication, state-of-the-art infotainment/telematics systems, and shift to connected and autonomous driving. Connected and Autonomous Vehicles (CAVs) utilise wireless networks and sensors to collect traffic and other critical information while their driving is governed by one of the six automation stages (SAE-International, 2018). Levels range from 0 to 5; SAE Level 0 means human driver performing all tasks related to the vehicle operation, and SAE Level 5 is the full autonomous navigation without human involvement. Based on these policy concepts, an automated vehicle at levels 4 and 5 is a self-driving car, but a self-driving vehicle at level 3 is not automated because it is restricted in the operating area and needs a human driver who can take over as appropriate.

The digitalisation of the automotive industry would generate $3.1 trillion in socio-economic benefits and $67 billion in business revenue (West, 2016). Various firms, from mainstream automotive makers like

* Corresponding author.
E-mail address: s3680269@student.rmit.edu.au (S.K. Khan).

https://doi.org/10.1016/j.aap.2020.105837
Received 19 May 2020; Received in revised form 12 August 2020; Accepted 3 October 2020
Available online 26 October 2020

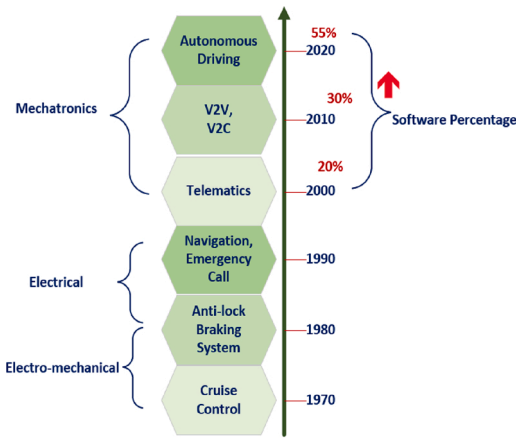

Fig. 1. Digital transformations in the automotive industry (Source: Authors' synthesis).

Volkswagen to internet-based businesses such as Google and Apple are spending immense human resources and capital in the production of CAVs (Behere and Torngren, 2015). These vehicles will be inter-connected, having access to the internet and interact with the surrounding environment through various sensors without the driver's involvement (Gehrig and Stein, 1999). The consequence of this transition is that the CAV should be a fully-fledged cyber-physical system (CPS), a collaborative network of electronic components regulating mechanical parts (Scalas and Giacinto, 2019).

Connected and autonomous driving technology accelerates the need for continuous communication between the CAV-ECU and a range of cloud services. It will develop sophisticated computing and efficient vehicle manoeuvring techniques, along with the prospect of delivering new software upgrades and other relevant content. As a result, the key to the successful integration of CAVs into the Intelligent Transport System (ITS) is the seamless internal and external communication within all CAV-related nodes. CAVs communication is the primary area vulnerable to cyber-attacks, requiring a rigorous and efficient approach in the form of cybersecurity. Cybersecurity is a set of technologies, procedures and activities designed to secure devices, files, networks and systems from interference, disruption or unwanted exposure to cyber-attacks.

Cyber-attacks in the CAVs communication contribute to two security issues, i) limited access: showing that CAV has an established wireless connection, but still does not have access to the internet, and ii) limited computational capacity: halting or stopping any calculation/judgment by the CAV that requires both arithmetical and non-arithmetic measures to follow an algorithm or a well-defined model. These vulnerabilities lead to unforeseen assault scenarios and may pose vital hazards to CAV-users and infrastructure (El-Rewini et al., 2019).

In July 2015, Fiat Chrysler recalled 1.4 million cars due to doubts about car software and alleged remote control. Software coding errors caused the Nissan Leaf to be hacked using the Nissan Connect EV application. An error has made it possible for hackers to remotely access in-car infotainment system and display driver identification details (Morris and Madzudzo, 2018).

Worldwide research shows many vulnerabilities and uncertainty in CAVs in terms of cyber-attacks. In this uncertainty are several possibilities for autonomous vehicle technology to underdeliver on its promise of safety and security; and, instead, become a net burden on society (Stasinopoulos et al., 2020). There is a range of continuing initiatives to maintain the protection and security of CAVs, which are primarily focused on the extension of strategies currently utilised to secure different cyber and physical elements. However, there is no structured paradigm for CAVs that tackle protection in a unified framework that addresses; i) hardware challenges, (ii) network challenges, (iii) human threats, as well as iv) software risks. The current literature lacks; i) the transparent picture of all the possible interfaces for cyber-attacks in a consolidated form, and ii) the analysis of all possible avenues for the cessation of cyber-attacks on the CAVs. Potential cybersecurity mitigation strategies in CAVs are mostly demonstrated for specific scenarios without considering the overall picture of CAV operation in an integrated ITS. Adversaries access to CAVs through proximity (or physical) access is a doorway for hackers, which needs an in-depth understanding and analysis. Similarly, synthesis from a review of existing literature shows that among the CAVs security performance evaluation metrics availability, authenticity and confidentiality are discussed in detail by various researchers. The scope of integrity is comparatively less discussed; however, reliability, robustness, and trustworthiness performance metrics are still subject to in-depth research and review, as depicted in Fig. 2 (Lopez et al., 2019; Möller and Haas, 2019). The purpose of this study is to address these limitations and to assess critical areas for the advancement of CAVs in combating cyber-attacks.

1.1. Contributions of the study

Currently, there is a lack of systematic and comprehensive review of the literature on cyber-attacks on the Connected and Autonomous Vehicles (CAVs), respective mitigation strategies, anticipated readiness, and research directions for the future. Our study aims to fulfil these knowledge gaps in the existing literature. The main contributions of this study are as below:

1) We described in a structured way a holistic view of potentially critical avenues, which lies at the heart of CAV cybersecurity research. We analyse their scope with a particular focus on ensuring effective mass deployment of CAVs and reducing the likelihood of cyber-attack failures.
2) For each potential avenue, we present a taxonomy of different threats and illustrate the generalization of attack surfaces for autonomous and connected vehicle applications.
3) Moving forward, we present the CAVs communication framework in an interconnected manner, i.e., from In-Vehicle (IV) communication to Vehicle to Everything (V2X) communication with visual flowcharts and pictorial representations to provide a clear description of all future cyber-attack interfaces.
4) We highlight and emphasized that why conventional CPS cybersecurity approaches are not adequate to counter cyber-attacks on CAVs. Subsequently, we review and synthesis a consolidated summary table and description of CAVs cyber-attacks, the respective CAV-communication system, and the corresponding counterstrategies with future directions.

Fig. 2. Performance evaluation metrics for CAVs security (Source: Authors' synthesis).

5) Finally, the vulnerability of CAVs to adversaries by proximity (or physical) access to cyber-attacks is synthesized. There is a segregation of cyber-attacks in the relevant performance evaluation metrics. We illustrate research gaps with future directions for each potential avenue, which needs further investigation.

The paper is organized as follows. The next section briefly explains the methodology used for the study. We then present the state-of-the-art to enlighten the scope, challenges, defensive strategies, anticipated readiness, and research gaps of cyber-attacks in CAVs. Finally, we conclude by summarizing the major contributions of this study. A list of the abbreviations used in this manuscript is provided in Table 1.

2. Methodology

Literature was retrieved from online archives, including Web of Science, Google Scholar, TRID, and SCOPUS using Boolean operators. Books, news articles, and relevant industry reports were also used to supplement background research. Specific keywords that were used include; "connected and autonomous vehicle/cars (s)", "driverless", "driverless vehicle/car (s)", and "automated vehicle/car (s)" in combination with i) cybersecurity-related terms-"cybersecurity", "hacking", "attack(s)", "hacker(s)", "cyber-attack(s)", ii) safety-related terms-"safety", "accident(s)", "crash(es)", "concerns", "risk(s)", and iii) privacy-related terms-"privacy", "data protection", "surveillance", "location", and "tracking". Cybersecurity for AV vehicles got attention in the past decade, and therefore post-2010 literature is considered. The literature search was further intensified by forward and backward snowballing in the related papers with the intention of having a thorough analysis of the topic, putting together the content and drawing some relevant conclusions for a robust CAV-cybersecurity framework.

Table 1
A list of abbreviations used in this study.

Abbreviation	Explanation
ADAS	Advanced Driver Assistance System
AI	Artificial intelligence
BCM	Body Control Module
CAN	Controller Area Network
CAV	Connected and Autonomous Vehicles
CPS	Cyber-Physical System
DSRC	Dedicated Short-Range Communication
DoS	Denial of Service
ECM	Engine Control Module
ECU	Electronic Control Units
ITS	Intelligent Transport System
IV	In-Vehicle
JTAG	Joint Test Action Group
LIN	Local Interconnect Network
ML	Machine Learning
MOST	Media oriented systems transport
NCM	Navigation Control module
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
PEPS	Passive Entry Passive Start
RAT	Routine Activity Theory
RFID	Radio Frequency Identification
TCM	Transmission Control Module
UWB	Ultra-wide band
V2C	Vehicle to Cloud
V2I	Vehicle to Infrastructure
V2R	Vehicle to Road
V2IoT	Vehicle-to-IoT
V2V	Vehicle-to-Vehicle
V2X	Vehicle to Everything
VANET	Vehicular ad-hoc Network
VCM	Vehicle Control Module
VCS	Voice Controllable Systems
VVS	Vehicle Vision systems

3. State-of-the-Art

This section is structured into seven subsections, identifying six avenues for identifying, tracking, and preventing cyber-attacks on the CAVs as shown in Fig. 3. Literature synthesis shows that stakeholders ought to work on these factors to ensure; i) seamless roll-out of CAVs, ii) efficient mass implementation of the CAVs, and ii) a decrease in the risk of cyber-attack vulnerabilities.

The first potential avenue outlines the CAVs communication framework in an integrated form, i.e., from IV communication to V2X communication with a visual flowchart to provide a transparent picture of all the interfaces for potential cyber-attacks including CAV wireless communication technologies. The second avenue demonstrates the susceptibility of CAVs to adversaries by synthesising proximity (or physical) exposure to cyber-attacks. Then, it describes the scope and importance of CAVs supply chain for the detection and eradication of cyber-attacks. It is followed by avenue on how psychologists and human-factor researchers can augment cybersecurity in CAVs by exploring behavioural models and learning from criminology theory to reduce the risk of a successful attack. Moreover, there is a concise overview of the regulatory regulations and policy framework avenue for fostering smooth deployment and operation of the CAVs on highways. Furthermore, the significance of an integrating mechanism avenue for ensuring acceptable levels of cybersecurity risks in the CAVs is highlighted and emphasised. Finally, we illustrate research gaps for each potential avenue, which needs further investigation.

3.1. CAVs communication framework

The key benefit of CAVs is the potential to interact with other vehicles, the smart road technology network, and other internet-connected applications, thereby improving driving behaviour and road safety (Ali et al., 2020a, 2020b). Several facets of autonomous transport rely on these interactions, such as platooning, shared route management, and so on. As a result, there has been a growing interest in the creation of reliable vehicle communication. At the same time, the ubiquitous nature of communication components is making it a sweet point for white-hat hackers. Based on the literature review, the leading automotive company reports, and the study of relevant govt research bodies, CAVs communication framework is illustrated in Fig. 4. This figure presents the CAVs communication framework for all possible interfaces in the form of a flow-chart. The rationale for presenting this is three-fold:

1) It is imperative to have a systematic understanding of the CAVs communication framework.
2) It is beneficial for monitoring, assessing, tracking, and combating potential cyber-attacks on various communication interfaces.
3) It will facilitate the development of a robust CAVs cybersecurity-by-design paradigm by application developers.

CAVs communication framework can be classified into two main categories; i) In-Vehicle (IV) communication, and ii) Vehicle to Everything (V2X) communication. Both these facets of CAVs (Fig. 4) are explained and synthesised in detail in the following sub-sections.

3.1.1. In-vehicle (IV) communication

The IV communication as presented in Fig. 4 involves; a) data flow of sensors, b) intra-vehicle communication, and c) coordination of ECUs. In Fig. 5 below, we present the relationship of attack vectors in IV communication in an automated vehicle. As shown in Fig. 5, different types of sensors (e.g., LIDAR, camera, Laser, etc.), Electronic control units (ECUs) (e.g., engine control module, transmission control module, etc.) and intra-vehicle communication (e.g., Local Interconnect Network (LIN), Controller Area Network (CAN), Ethernet, etc.) need to work together to guide and navigate the automated vehicle in the transport network. In the next sub-sections, the components of IV communication

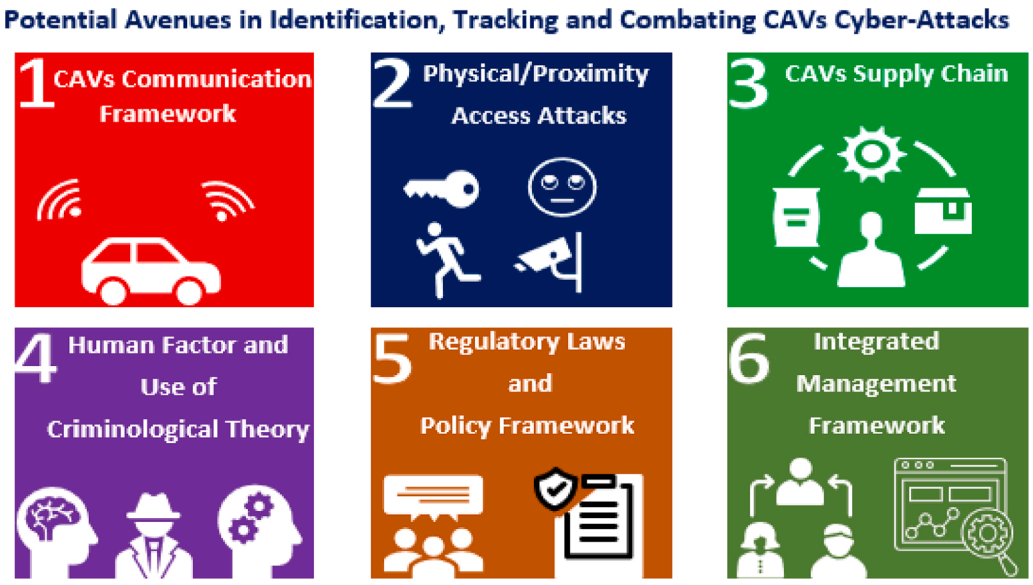

Fig. 3. A holistic view of potential avenues essential in combating CAVs cyberattacks (Source: Authors' Synthesis).

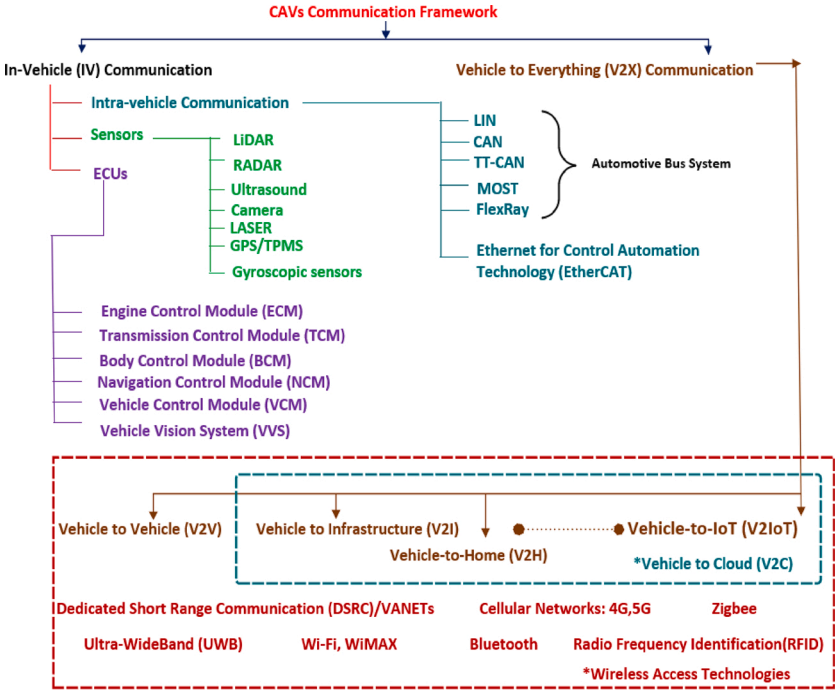

Fig. 4. CAVs communication framework (Source: Authors' synthesis).

and the cyber-attack vectors are described in more detail.

3.1.1.1. Sensors' data flow. The data flow of the sensors is the correspondence between the external physical environment and the CAV-computer unit. Autonomous vehicles are mounted with a variety of sensors that gather an understanding of the environment. Types of autonomous vehicle-mounted sensors include LASER, RADAR, LiDAR, GPS, TPMS, Camera, Ultrasonic and Gyroscopic sensors, all contributing to better vision and recognition algorithms (Levinson et al., 2011; Raiyn, 2018). The input obtained from these sensors enhances the capacity of vehicles to navigate.

3.1.1.2. Intra-vehicle communication. Intra-vehicle communication consists of automotive bus systems, interaction through the On-Board Diagnostics (OBD) device or dongle, and the Automotive Ethernet for Control Automation Technology-EtherCAT. Premium segment automobiles would have 5 bus systems which are; i) LIN (Local Interconnect Network): is a bus protocol used for low-cost multiplexed connectivity in automobile networks designed for high latency and specialised error management with a data rate of up to 10 Kbps, primarily used for electric seats, mirrors and tailgates, ii) Controller Area Network (CAN): is the most widely used bus interface allowing various components to connect with each with other having a speed of 1 Mbps. Typical uses include ABS, power rail, and engine management (Krishnapriya et al., 2012), iii) TTCAN and Flex-Ray: is CAN equivalent with a data rate of up to 10 Mbps, mostly used in the areas of the engine, braking, suspension, acceleration, steering, and diagnostics, iv) MOST (Media oriented systems transport): is designed for digital data transfer utilising optical fibre

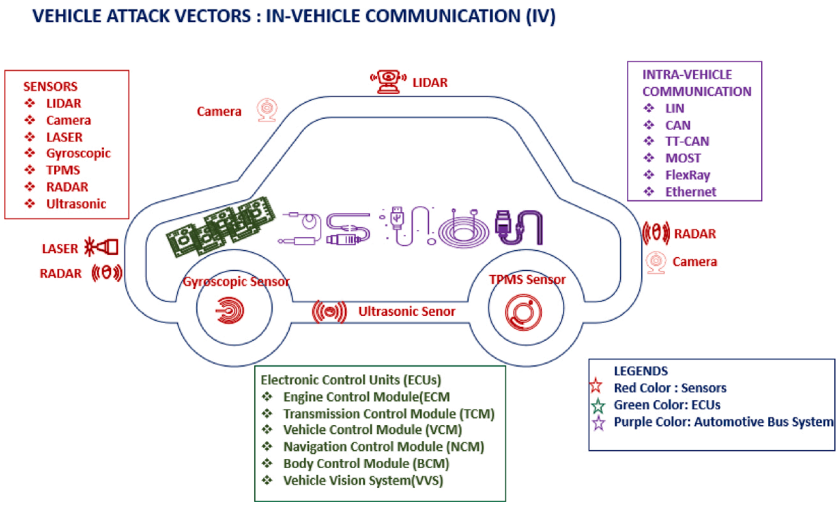

Fig. 5. Cyber-attack vectors in CAVs In-Vehicle (IV) Communication (Source: Authors' synthesis).

cables or coaxial cables. It has faster transmission rates than LIN, CAN and Flex Ray with a data rate of up to 23 Mbps. It is primarily used for video plays and car infotainment systems, and v) Automotive Ethernet: its use is still minimal but will play a crucial position in the next phase of automotive networks. The broad bandwidth is a valuable attribute for new automobiles with trade between cost and weight.

3.1.1.3. ECUs coordination. The coordination of ECUs is the exchange of information for the control of a series of actuators to ensure optimum CAV performance. ECUs are the embedded controller that controls one or more of the automobile's subsystems. Examples of different ECU units according to their importance are Transmission Control Module (TCM), Engine Control Module (ECM), Navigation Control module (NCM), Body Control Module (BCM), Vehicle Control Module (VCM), and Vehicle Vision systems (VVS) (Al Zaabi et al., 2019).

3.1.2. Vehicle to everything (V2X) communication

The key aspect of the ITS is that CAVs have the communication capability to interact with each other or with the other sections of the transport network. V2X communication can be classified into Vehicle to Cloud (V2C) and Vehicle to Vehicle (V2V) communication. V2C communication ranges from Vehicle to Infrastructure/Road (V2I/V2R) to Vehicle-to-IoT (V2IoT) interactions. Moreover, the primary wireless communication technologies that will enable the operation of CAVs are shown in Fig.4, and the CAVs V2X communication attack vectors are depicted in Fig. 6 and explained below:

i) Dedicated Short-Range Communication (DSRC)/VANETs: is a protocol stack that allows low latency, secure and high-speed communication (Dey et al., 2016; Liu et al., 2020).
ii) Cellular Network: The DSRC suffers from low bandwidth, so cellular networks are deemed to be the successful candidates. 3GPP has developed LTE (4 G) for V2X communication and is currently focused on V2X communication integration into 5 G-New Radio (Muhammad and Safdar, 2018; Khan et al., 2020).
iii) Zigbee: is a short-range networking protocol designed for low-speed communication. In El-Rewini et al. (2019), the authors suggested the usage of Zigbee within V2C communication, ADAS, and Forward Collision Alert System.
iv) Ultrawideband (UWB): is another form of wireless networking and can transfer large data speeds at low transmitting strength. UWB has been introduced in VANET for accident avoidance and vehicle positioning systems, and defence to counter relay attacks in Passive Entry Passive Start (PEPS) system (El-Rewini et al., 2019).

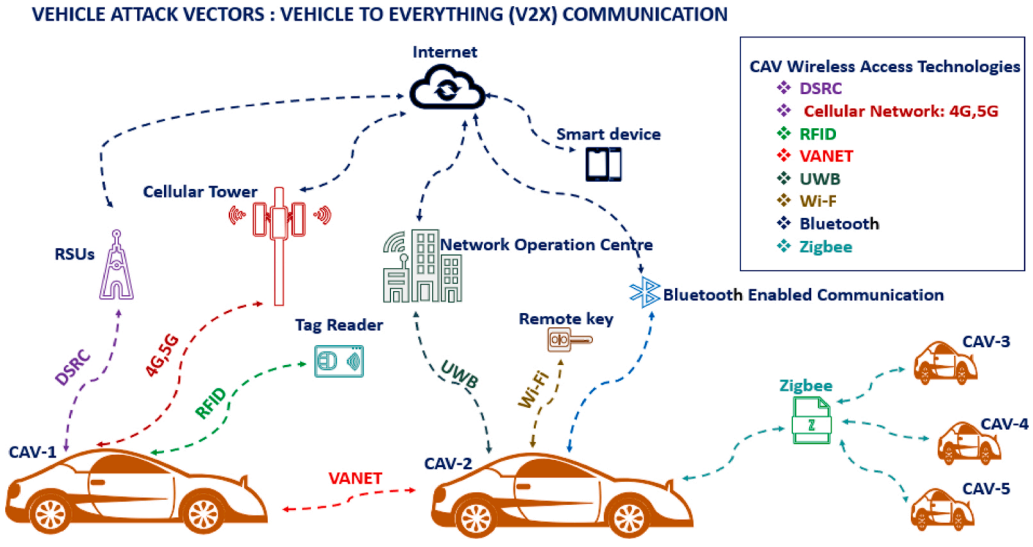

Fig. 6. Cyber-attack vectors in CAVs Vehicle to Everything (V2X) Communication (Source: Author's synthesis).

v) Wi-Fi, WiMAX: is also a potential contender for V2X communication referred to as IEEE 802.16, low-latency standard, secure, and all-IP core network support (Tanuja et al., 2015).
vi) Radio Frequency Identification (RFID): permits the identification of radio signals using VANET applications including public transport passes and traffic systems (Hennessy, 1916; Pawade et al., 2013; Vijaykumar and Elango, 2014; Al Zaabi et al., 2019; El-Rewini et al., 2019).
vii) Blue-tooth: is mostly used to connect smartphones with automotive infotainment and telematics systems for access to calls, music streaming, calendars, and car diagnostics units (Onishi et al., 2017).

3.1.3. *Orthodox CPS cybersecurity solutions are insufficient in CAVs*

Existing research suggests a number of cybersecurity approaches for the CAVs, most of which are based on CPSs security frameworks. However, these orthodox cybersecurity approaches cannot be used directly to counter cyber-attacks in the automotive industry; there is a need for robust hardware and easy-to-use applications. The reasons why these cybersecurity solutions are inadequate in CAVs are highlighted in Fig. 7. First, CAVs would remain in the field over a prolonged period relative to current IT networks, allowing white-hackers ample opportunities to identify flaws in the deployed vehicles. Second, current protection approaches are typically cost-effective and challenging to introduce in CAVs due to resource and technological constraints in the ECUs, as well as their sensitivity to stressful environments, such as low or high temperatures, vibrations, and electromagnetic interference (Scalas and Giacinto, 2019). Third, several ECUs are needed to carry out real-time activities that are often safety-critical. Furthermore, the presence of strict authentication constraints can lead to the extraction and misuse of various private details, i.e. identity surveillance, driving records, behavioural inferences, subscribed services, and mobility trends. Similarly, to protect intellectual property, vendors often supply (software) components without source code; it may be more challenging to change them to enhance security.

3.1.4. *Overview of cyber-attacks, their impact on the CAVs operation and mitigation techniques*

CAVs communication is vulnerable to two types of attacks; i) active: when communication is disrupted or replaced by fake messages, and ii) passive: when the intruder collects information for a potential malicious intent in a long-term timeframe. In contrast to passive attacks, active attacks are more challenging to protect but easier to detect. Table2 presents a summary of cyber-attacks, their impact on the CAVs in ITS, relevant mitigation techniques, communication layer details and recommendations for the future.

Voice Controllable Systems (VCS) are susceptible to hidden voice instructions that are ignored or unintelligible to humans. Depending on the target level, these threats may be categorised as inaudible voice commands (attacking the voice capture point) and audio-adversarial cases (attacking the speech recognition stage) (Zhou et al., 2019). For example, malicious voice commands encoded in the sound of online videos can sneakily control the vehicle as people watch these videos in the car (Zhou et al., 2019). A spoofing attack is when the intruder uses a false identity or sends out fake data (Linkov et al., 2019). This would impact on shared route management (platooning) of CAVs in two ways; i) pretend to be a (fake) neighbour CAV, or ii) send false information about a neighbour's CAV location. Man-in-the-middle attacks/passive attacks/relay attacks are where the adversary sends the original message to the CAV, updates it and sends a new message to the vehicle that causes an incorrect message switch between the CAVs communication (He et al., 2017). Eavesdropping, disclosure of information, and traffic-data analysis are the consequence of such assaults. The jamming attack is where radio signal noise interrupts the frequency of communication, intended to obstruct or hinder V2C communication (Parkinson et al., 2017). In Czerwinski et al. (2019), the author emphasises the impact of the radio power level of the ZigBee network module on the use of energy and performance in the CAVs communication under jamming conditions. A masquerade attack is an intrusion that uses a false identity, such as a network identity to obtain unauthorised access to the CAVs without valid access authentication. The authors in Choi et al. (2018a, 2018b) and Liu et al. (2017a, 2017b, 2017c) described two CAN vulnerabilities that allow masquerade attacks. An eavesdropping attack is known as a sniffing or snooping attack, is an incursion where white-hat hackers attempt to intercept information that CAVs send over a network. The black-hole attack is where the message is blocked without the CAV being aware of the missing message (Carsten et al., 2015). The impact of this attack is blocking communication to the target CAV, blocking or disabling the response of the receiver-CAV.

Similarly, in a replay attack, the perpetrators continually forward a valid frame to prevent the CAV from working in real-time Liu et al. (2017a, 2017b, 2017c). In bus-off attacks, intruder constantly sends bits both in the ID field and in other fields, which allows the ECU transmission error counter to be raised, if the value of the TEC is higher than 255, the resulting CAV-ECU would be shut down and will result in halting the CAV operation (Choi et al., 2018a, 2018b). Denial of Service (DoS) attacks happen when adversaries consistently send high priority messages that circumvent genuine low priority messages. DoS attacks may be used as a way of monitoring override attacks that enable attackers to gain control of the CAV (Carsten et al., 2015). In message spoofing attacks, intruders send unauthorised messages containing false information to interrupt vehicle communication (El-Rewini et al., 2019). Injection attacks happen when attackers are inserting unauthorised and harmful messages inside the in-vehicle network. In timing attacks, a deceptive CAV gets a notification, introduces a time delay, and then transfers the notification to other CAVs causing incorrect scheduling of instructions and fake road congestion. This intrusion may be catastrophic to transportation networks that rely on real-time applications (Sumra et al., 2011). Impersonation attacks are conducted by creating a CAV with a fake identity (Amirtahmasebi and Jalalinia, 2010). Impersonation is harmful to the integrity of the overall transportation network infrastructure and is especially destructive in the case of a crash, as the CAV under review is untraceable and misleading to other CAVs. The alteration/replay attack happens when an intruder utilises previously created frames to submit and interact with other nodes (CAVs), with or without modification causing incorrect location and speed value or wrong route adaption (Parno and Perrig, 2005).

Cyber-attacks don't often end in accidents, but they do cause broader oscillations (Cui et al., 2018). The slight attack is the case where the reported CAV data randomly deviate from the real data, and the deviations do not exceed the threshold-making the difference less noticeable. The authors in Li et al. (2018) indicated three findings; a) when one

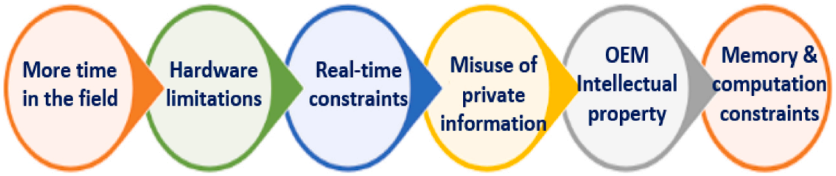

Fig. 7. Reasons why orthodox CPS cybersecurity solutions are inadequate in the CAVs. (Source: Authors' synthesis).

Table 2
Summary of cyber-attacks, its impact on the CAVs and mitigation techniques.

Attack Type	Communication System	Attack Vehicles	Attack Impact	Counterstrategies and Potential Mitigation Techniques	Communication Layer	Future Work
Hidden voice command/dolphin attack/commander song (Greenberg, 2015; Zhang et al., 2017; BMW-Group, 2018; Roy et al., 2018; Yuan et al., 2018; Zhou et al., 2019)	VCS, IV communication	BMW, GM, Chevy Impala	Infotainment malfunction, Vehicle driving control.	Pop-noise-based general defence strategy, audio turbulence and audio squeezing.	Network	Induction of Machine Learning (ML) and Deep Learning (DL) algorithms to combat such attacks.
Sibel/Spoofing/Botnet attacks (Wesson et al., 2011; Yu et al., 2013; Anouar et al., 2016; Solon, 2016; Van der Heijden et al., 2016; Muciaccia and Passaro, 2017; Nie et al., 2017; He and Chow, 2019)	GPS, IV communication	Tesla Model S P85, Model 75D, Jeep Cherokee	Incorrect location and speed value, wrong route adaption.	Speed-deviation such as acceptance range thresholds, Intrusion Detection System (IDS), correlating messages from neighbours. Using a reputation-based mechanism.	Network Transport	Blockchain is an evolving technology and has the potential to circumvent the security challenges of existing VANETs and can help to combat these cyber-attacks. Its scope and utilization in CAV communication are still in the early stages.
RF Jamming attacks (Azogu et al., 2013; Puñal et al., 2014; Parkinson et al., 2017; Lyamin et al., 2019)	Over-the-air communication, LiDAR, autonomous navigation		Performance of platooning, in-accurate communication, object detection failure.	ML-based jamming detection, anti-jamming technique for VANET metrics-directed security defence..Jamming DoS detection using data mining, intrusion, and network coding.	Physical Network	Need for fast-detection and fast-reacting anti-jamming mechanisms in CAV (non-static) networks. The implementation of various techniques such as artificial intelligence, mobile agent, game theory, consistency check, cross-, spatial retreat, and frequency hopping needs to be assessed in this context.
Slight/ Greyhole attacks (Miller and Valasek, 2015; Verma et al., 2015; Liu et al., 2017a,2017b,2017c; BMW-Group, 2018; Li et al., 2018)	V2V, V2C	2014 Jeep Cherokee, BMW Cars	Longitudinal safety, traffic congestion.	Cyber-attacks should be considered for the entire CAV fleet rather than for individual's CAV.	Physical Network	Designing of dynamic defence mechanisms for CAVs platooning-as an entity of integrated ITS.
Passive Attacks/ Man-in-the-middle attacks/Relay attacks (Francillon et al., 2011; Weiß, 2011; Gagandeep et al., 2012; Nissan, 2016; He et al., 2017; BMW-Group, 2018; TencentKeen-SecurityLab, 2019).	V2V, V2C	Tesla model S 75, Nissan leaf	Eavesdropping, disclosure of information, traffic-data analysis.	Encryption techniques using public keys in V2X communications.	Network Transport	Developing and configuration of CAVs communication networks to encrypt not only data but also information and electromagnetic shielding.
Replay /Playback attacks (He et al., 2017; TencentKeen-SecurityLab, 2019)	V2V, V2C	Tesla Model S 75	Impact on real-time CAV-operation.	Tagging each encrypted component with a session ID and a component number.	Network	Designing and induction of bio-metric identification systems, i. e. fingerprints, iris, speech, face, retinal recognition and hand morphology, for swift and effective identification purposes.
DoS/Message Delaying/ Blackhole attacks (Hasbullah and Ahmed, 2010; Hortelano et al., 2010; Raiyn, 2013; Bergin, 2015; He et al., 2017)	Automotive Bus System, Over-the-air communication		blocking communication to the target CAV, blocking or disabling the response of the receiver.	Cryptographic techniques such as MAC and digital signatures to secure information.	Physical Network	The CAV programme needs to be reviewed and tested regularly, protocols need to be constantly reinforced, induction of firewall set up, watchdogs and data-based malicious behaviour detection.
Modification/Injection attacks (Koscher et al., 2010; Weiß, 2011; Foster et al., 2015; He et al., 2017; Raiyn, 2018)	V2V, V2C	2009 Chevy Malibu	Modify messages e.g. GPS details on the communication channel.	Use of public keys as encryption: which uses biometric data for message authentication and secured communication-based on iris recognition.	Network Transport	Machine learning method to filter the data, analyse it, and cross-check it with other input parameters.
Timing-faking attacks (Sumra et al., 2011; Taylor et al., 2015; Cho and Shin, 2016)	Over-the-air communication		Incorrect judgements by the Road-Side Units (RSUs) directing	Timing-based CAN-Bus anomaly detectors.	Physical layer	Clock-based ECU fingerprinting,

(*continued on next page*)

Table 2 (*continued*)

Attack Type	Communication System	Attack Vehicles	Attack Impact	Counterstrategies and Potential Mitigation Techniques	Communication Layer	Future Work
			the CAVs to follow sub-optimal paths, i.e. high-traffic or crash paths.			fixed processing time algorithms.
Tunnelling attacks (Rawat et al., 2012; Zhang et al., 2014; Xu et al., 2018; Shrestha et al., 2019; Zhang et al., 2019).	V2V, V2C		Modification of packets, delaying communication.	Split Horizon DNS concept, cloud-based on-board malware defence manager.	Network Transport	Developing CAVs communication networks to encrypt not only data but also information and electromagnetic shielding.
Impersonation attacks (Amirtahmasebi and Jalalinia, 2010)	V2V, V2C		Vehicle under investigation becomes un-trackable.	Digital signatures without certificates.	Network	Designing a two-layer (cross-verification) approach for decision-making by the CAV. For example, one input from CAV-generated data and another input from Infrastructure-generated data.
Cyber-attacks on sensor networks (Rouf et al., 2010; TencentKeen-SecurityLab, 2019)	Autonomous navigation, IV communication	Tesla Model S 75	Providing inaccurate inputs to the CAV-ECUs, low network performance.	Used of encryption and cryptography techniques, updated firmware, and use of a VPNs.	Physical	Using a non-standard network and diagnostic ports. Developing a sensor tampering detector so that the functionality and sensitivity of the CAV-sensors can be checked and notified immediately.
Attacks on GPS (Spoofing and Jamming) (Rouf et al., 2010; Wesson et al., 2011; Lopez et al., 2019; TencentKeen-SecurityLab, 2019)	Autonomous navigation, IV communication		Incorrect location and speed value, wrong route adaption.	i) Cryptography: use of authentication and encryption procedures, and ii) Signal check: Utilizing distortions of correlation function in the receiver.	Physical	Improvements to the traditional firmware and applications running on the underlying ECUs.
Attacks on LiDAR (Petit et al., 2014, 2015; Shin et al., 2017)	Autonomous navigation, IV communication		Deception with toxic signs, failed pedestrian detection.	Reduced range of LiDAR connections, shortening pulsing time interval, and pulsing laser multiple times.	Physical	The impact of attacks may be mitigated by reducing the receiving angle. Using multiple LiDAR input as cross-verification.
Attacks on camera (Petit et al., 2014, 2015; Raiyn, 2018; Decisions, 2019; Lopez et al., 2019; TencentKeen-SecurityLab, 2019)	Traffic sign recognition, Lane obstacle detection,		Hide or remove traffic signal photos at key locations, avoid track identification.	Filtering options, using photochromic lenses.	Physical layer	Use of machine-readable road signs (e.g. UV QR overlay or PCM-modulated light signals).
Attacks on TPMS (Rouf et al., 2010)	IV communication		Proving inaccurate inputs to the ECUs, gaining entrance via exploitable inputs.	IDS with updated firmware, prevention of spoofed activation.	Physical	Development of the sensor-tampering detectors.
Attacks on RADAR (Yan et al., 2016)	IV communication	Tesla Model S	Failed adaptative cruise control, failed pedestrian detection.	ML-based jamming detection, anti-jamming strategy for VANET metrics-directed security defence.	Physical	Using multiple RADARs for cross-checking and validation of input data with robust and efficient models.
Attacks on Ultrasonic sensors (Zhang et al., 2017; Yuan et al., 2018; Zhou et al., 2019)	IV communication		Autonomous navigation, parking assistance	Pop-noise-based general defence strategy, audio turbulence and audio squeezing.	Physical	Development of the sensor-tampering detector, using multiple sensors, cross-validation of input data.

CAV is under slight cyber-attacks, it becomes riskier if the locations transmitted are targeted than the speeds, b) if multi-CAVs are under attack, the scenario of more CAVs under low severity attack is expected to be more hazardous than those of fewer CAVs under high-intensity attack, and c) the effect of slight cyber-attacks during the deceleration phase is more severe than the acceleration phase. In a spamming attack, the transmission latency in VANET is increased, causing a severe delay in V2X communication. During a tunnelling attack, two parts of the network are linked by an attacker using an external communication channel that may result from eavesdrop on V2C communication to halting of CAVs real-time operation. CAVs cameras are also vantage points for white-hat aggressors. For example, attackers can hide or

remove traffic signal photos at key locations or attach lines to the path to avoid track identification. Similarly, GPS signals are weak and susceptible to remote malicious intrusion. GPS jamming attacks are usually considered to be the deadliest attack, there is a high probability of an accident when the GPS of the CAV is under attack (Cui et al., 2018). Furthermore, the attack on LiDAR is an expansion of the replay attack, and the intention is to transmit the original signal from the LiDAR device of the target vehicle from another location to produce false echoes impacting autonomous navigation (Nayegandhi, 2007).

Existing research suggests different classification requirements for categorising CAVs cyber-attacks. For example, in Mejri et al. (2014), the authors classified CAVs cyber-attacks into five categories depending on the related cryptographic classification, i.e. attacks on authenticity, availability, confidentiality, non-repudiation, and data trust. The authors in Cui et al. (2019) divided cyber-attack on the vehicles into four types; availability, data integrity, authenticity, and privacy based on security requirements concerning the CAVs. In Amoozadeh et al. (2015), such attacks are graded into the network layer, application layer, privacy leakage attacks, and system-level. Likewise, in Wang et al. (2020) CAVs cyber-attacks are fragmented into the group of three; bogus messages, collusion attacks, and replay/delay based on; i) cyber-attacks characteristics, and ii) attacking principles.

The severity of cyber-attacks on the CAVs cannot be explicitly categorised in prior as critical or minor because it depends on; i) the degree of interruption that white-hat hackers want, ii) the privileges they have access to, and iii) the CAV-driving scenario, i.e., vehicle platooning etc. The classification of such attacks under different security performance evaluation metrics is shown in Fig. 8. Visualising the role of CAVs in ITS and its operational framework, cyber-attacks that impact the availability and authentication of CAVs are usually of extreme severity (Lopez et al., 2019; Möller and Haas, 2019). Attacks on the reliability, robustness and integrity are typical of mild magnitude. Similarly, attacks impacting confidentiality and trustworthiness can be graded as low severity.

3.1.5. Counterstrategies and potential mitigation techniques

CAVs will rely on both sensor data and mapping data for real-time operation. Sensor data is the one collected from sensors, i.e., LiDAR, RADAR, camera etc. Mapping data can be of two types; i) static-terrain details, and ii) dynamic-real-time updates from communication infrastructure (Liu et al., 2017a, 2017b, 2017c). For secure CAVs communication, stringent low-latency authentication techniques are required. CAVs and relevant service platforms should be authenticated by one another or by a reputable third-party. Biometrics authentication can be introduced, which is safe and reliable, i.e. passwords cannot be lost or forgotten (Raiyn, 2018).

Commonly used biometric authentication are fingerprints, iris, speech, face, retina recognition, and hand geometry to secure data CAVs communication. Similarly, encryption techniques using a public key may be used in V2X communications (Weiß, 2011). Cryptographic techniques such as MAC and digital signatures may secure information against spoofing and forgeries. Blockchain is an evolving technology and has the potential to circumvent the security challenges of existing VANETs and can facilitate to combat cyber-attacks. Its scope and utilization of in-vehicle communication are still in the early stages (Shrestha et al., 2019; Zhang et al., 2019). The computing resources required for the CAVs are significantly higher to support the processing of large quantities of sensors data. In effect, this includes improvements to the traditional firmware and applications running on the underlying ECUs (Lopez et al., 2019).

3.2. Physical/proximity access attacks

Physical access to the CAVs can provide hackers with a multitude of entry points, but physical attacks are generally not very flexible, hard to be untraceable, and difficult to treat frivolously. Adversaries may have access to autonomous vehicles by either physical access or proximity access. Similarly, the operation of CAVs can be halted by vehicle diagnostic ports or by illusion attacks, depicted in Fig. 9.

Potential unauthorised access attacks are categorised in i) obvious interference, and ii) sensor manipulation. Typically, sensors are the direct security risks to the CAVs, adversaries can; i) produce incorrect messages; ii) obstruct sensor data; or iii) intervene with autonomous driving by hacking into the CAV computing device (Liu et al., 2019). In Becher et al. (2006), the authors analysed various physical attacks against sensor node hardware, i.e. node captures, Joint Test Action Group (JTAG) attacks, bootstrap loader attacks, and external flash attacks, though, such kinds of assaults require specialised skills and costly hardware. Proximity attacks can be classified as inaudible voice commands and PKES. Inaudible voice commands required the physical presence of an attack device to transmit synthetic ultrasound signals. PKES is used to unlock the door or to start the engine simply by holding the key in its pocket vulnerable to relay attacks, with hardware available just under $100 (Choi et al., 2018a, 2018b). Similarly, an attacker will tamper with on-board sensors and other hardware to alter the perceived position, direction, and distance (Petit et al., 2015; Wang et al., 2020).

Physical inputs and outputs contained within a CAV include ports such as diagnostic port (OBD-II), USB port, infotainment interactions, EV charging, and other open ports. Exploiting these ports is normally more difficult for an attacker because they will generally require physical access to the vehicle but due to the availability of additional devices

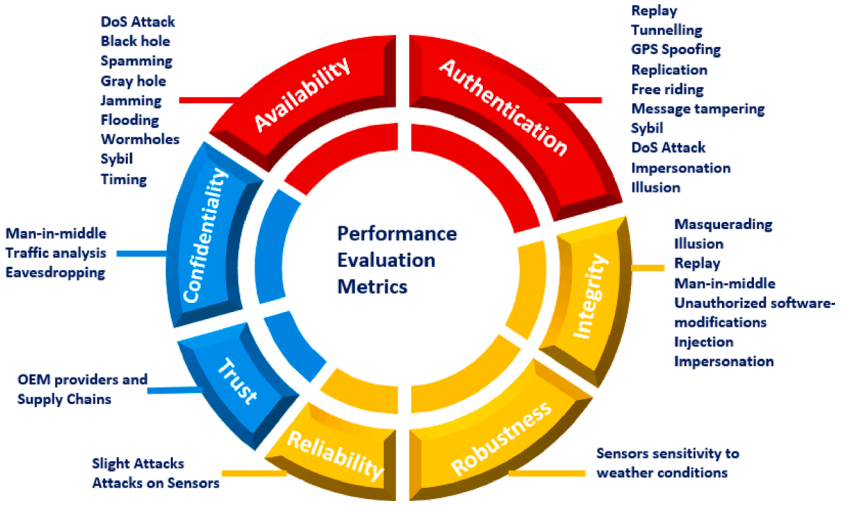

Fig. 8. CAVs cyber-attacks classification under security performance evaluation metrics (Source: Authors' synthesis).

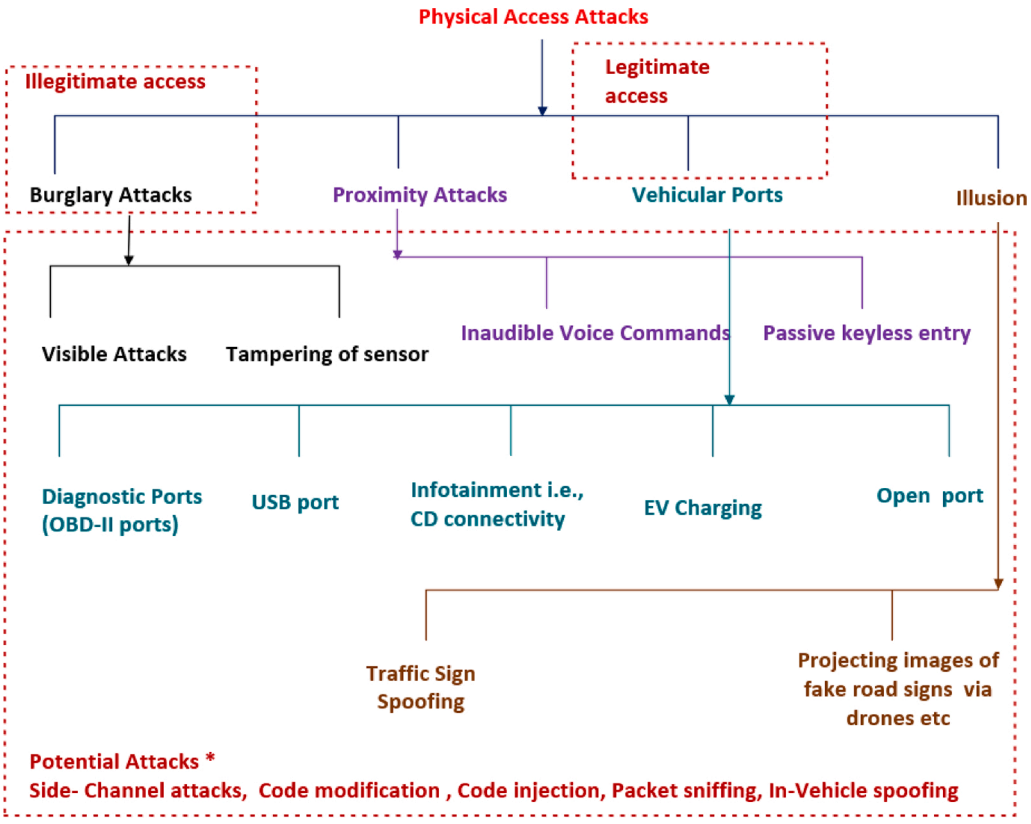

Fig. 9. Physical/proximity access attacks (Source: Authors' synthesis).

that connect to these ports, there are several ways in which attacks can be carried out through a remote link. The diagnostic port directly connects via CAN to multiple on-board computers; an intruder with physical access to the car can trigger attacks and compromise sensitive vehicle systems (Lopez et al., 2019). There is an opportunity for an attacker to reach the vehicle's internal network in the presence of the USB port. CAVs can also be targeted by placing an infected CD on a CD player that may execute malware automatically (Linkov et al., 2019). Entertainment systems and CAN bus networking to upgrade ECU software in CAVs could be the victim of hackers as well. CAVs can also be targeted when charging using an electrical adapter that attaches and records data. Furthermore, some cars have open ports where the intruder can quietly connect to the D-Bus without further authentication (Lopez et al., 2019). Moreover, illusion attacks could be in the forms of drones that projected pictures of fake machine-readable road signs (e.g. UV QR overlay or PCM-modulated light signals) for an instant, i.e., 100ms-too short for human sight, but long enough for autopilot sensors to be deceived (Gurion, 2019).

3.2.1. Defence strategies

Physical access to a CAV communication bus may be like root access to the system, so both physical and cyber risks must be addressed. However, as the priority for vehicle safety has increased in recent years, efforts are being made to prevent physical attacks. An external sensor tampering detection system is needed to track the sensitivity of the sensors on the CAVs. It's also effective to use vehicle alerts to detect and curtail proximity access attacks. A sound-based proximity-detection method, pop-noise-based general defence strategy, audio turbulence and audio squeezing can prevent relay attacks on PKES systems and combat inaudible voice commands (Greenberg, 2015; Zhang et al., 2017; BMW-Group, 2018; Roy et al., 2018; Tang et al., 2018; Yuan et al., 2018; Zhou et al., 2019). In Markham and Chernoguzov (2017), the authors proposed a role-oriented access control scheme to tackle vulnerabilities caused through diagnostic ports, i.e., any commercial OBD-II device would be certified by the OEM and would supply the vehicle with X.509 certificate and a public key to show its identity, and access will be granted accordingly with the relevant privileges. Uncertified gadgets would only be allowed to read the bus, while a licenced mechanic scanning tool would have both the read and write permissions. Similarly, cyber protection techniques will be used to counter information security risks. In addition, simple physical access points to a CAV, such as the OBD-II port, can be moved to a non-standard position. Furthermore, mitigation techniques for the threats to EV charging unit are; i) incorporation of secure encryption in the controller boards of EV charging unit, i.e., for both board-to-board communication and flash memory, ii) tampering alarm induction and activation for any breach, and iii) using secure coding standards.

3.3. CAVs supply chain

CAVs consist of complex digital systems and subsystems developed by several geographically distributed vendors. The increasing complexity of the software system and the dynamically interconnected IT subsystems have paved the way for the advent of new vendors within the CAVs supply chain. New entrants offer services, especially in the field of engineering and design, rather than physical products (Morris and Madzudzo, 2018). Two main issues concerning the supply chain of CAVs are as follows:

1 Cybersecurity is deemed a secondary task in most automotive business models. It offers minimal incentives for monetization and value generation within a highly profit-driven operating framework. Potential suppliers in this supply chain can incorporate confidential information and obtain access to assets produced by the other players. At the same time, the manufacturer would want to secure the product from other players in the supply chain. Such security

leaks could result in the malfunctioning of CAVs or the espionage of users and even access to OEM confidential information as well.

2 Device manufacturers build systems and components based on the technical requirements and performance criteria given by the automotive OEMs, but often product manufacturers make design choices without OEM input. The relationship between the limitations of technology information and the inefficiency of many cybersecurity techniques results in an overuse of intuition, a dependence on static and generic knowledge, and a lack of governance of cyber presence (Julisch, 2013).

The prerequisite commitment of CAVs OEMs/vendors/suppliers to impartial security testing will be very beneficial. Similarly, log files must be preserved and secured for a given period of time for all CAVs operations including physical access and anti-malware updates etc. In addition, OEMs/vendors/suppliers must fulfil audit requests and initiatives such as incident response, penetration testing and vulnerability scanning etc.

3.4. Human factor in the safety of CAVs and use of the criminological theory

CAVs cybersecurity is an evolving field of traffic safety. Since human weakness is the most likely explanation for a successful cyber-attack, psychologists and human-factor researchers can augment cybersecurity in CAVs by exploring how to reduce the risk of a successful attack. A major consultancy firm expressed it as "*Cybersecurity is not only about technology but rather about psychology and sociology. It's convenient for developers to think that the most appropriate approach is the one with the most blinking lights, but in the field of cybersecurity, it's mostly people's actions that decide the result (PWC, 2014)*".

Similarly, mixed traffic flow would be very normal in the near future, and the driver's reaction to the lead vehicle relies on their conditional perception of CAV technology rather than on the real driving behaviour. This suggests that in the immediate future, classic car-following behaviour in pure human vehicle traffic will need to be revised to model mixed traffic, based on the CAVs characteristics and layout (Zhao et al., 2020). Only the penetration of 100 per cent CAVs will contribute to the maximum protection (Sinha et al., 2020). The main human factors that need to be investigated in the effective mass adoption of CAVs and to minimise the risk of human-related failures are discussed below (Linkov et al., 2019):

Characteristics of people prone to cybersecurity failures–people vary in their ability to accurately identify cybersecurity risks. The research conducted in Katerina and Nicolaos (2018) found that 23 % of people correctly manage fewer than half of the cybersecurity scenarios, and only 4% are able to handle more than 90 % of situations. Internet users are likely to be more aggressive towards cybersecurity if they are more extraverted, less attentive, and addicted to the internet (Hadlington, 2017). Those who use computers more frequently for non-work purposes have little understanding of internet security. Anxious people are less effective in identifying cyber-threats (Welk et al., 2015). Generally, men have more knowledge about cybersecurity than women (Anwar et al., 2017). Risky cybersecurity attitude is related to the over-trust of automated technology (Noy et al., 2018). Similarly, older drivers and female drivers benefit maximally from the CAV communication facilities compared with the young drivers (Ali et al., 2020a, 2020b; Sharma et al., 2020). Nevertheless, the features of individuals with riskier conduct towards cyber-CAVs are still unclear.

Human behaviour–during cyber-attacks is an integral part of research to inform people about cyber threats in the CAVs. The level of multitasking that the driver indulges in can have an impact on the effectiveness of the response to cybersecurity breaches. Based on a study in this area, when CAV drivers have to respond to unusual incidents, they have a wide range of response times and their ability to react varies (Brandts et al., 2016; Dixit et al., 2016; Dogan et al., 2017). Similarly, due to ubiquitous CAVs communication and prior information availability about anticipated incidents, for example, informing in advance about pedestrians approaching from the pavement would make it safer for drivers to be more willing to give way and retain a higher margin of safety (Ali et al., 2020a,2020b).

Motivations and characteristics of attackers–Knowledge of attackers' intentions and behaviours can help to deter potential CAVs attacks. In King et al. (2018), the authors found that attackers may be characterised by low socioeconomic status, socialisation towards law-breaking behaviour, hyperactivity, and dark triad personality traits. Such characteristics can help to establish methods for the identification of attackers (Holt et al., 2010; King et al., 2018).

Criminological theory for mitigating and preventing cybersecurity threats–the authors in Kennedy et al. (2019) proposed criminological theory, i.e., Routine Activity Theory (RAT) for mitigating and preventing cybersecurity threats. Based on the discussion and in-depth literature review, the authors evaluated the use of RAT as a suitable framework for preventing and mitigating cybersecurity risks.

3.5. Regulatory laws and policy framework

Cities need to start planning for this modern mode of travel, which is evolving rationally. Regulatory bodies need to develop, review plans and policies for the anticipated development of CAVs and implement the measures necessary to ensure an efficient and sustainable transport network. Various factors of regulatory laws and policy framework need to be considered, such as data confidentiality and privacy, short-term economic considerations, operational safety, public acceptance, legal and ethical issues (Seuwou et al., 2020). In Taeihagh and Lim (2019), the authors studied and analysed government approaches taken globally in response to CAVs advancement. Based on their analysis, in most situations, state policymakers have resisted strict legislation to encourage innovation in the CAVs, relying only on the formation of committees or focused groups for further exploration. The implications are lack of clarification as to whether CAV passengers, CAV OEMs or other third parties are to be held liable in an accident. Another main concern is the obligations of service providing operators, which requires the mandate for operators to store CAVs related personal data inside a country and its availability to the overseas business partners (He, 2018). Although, China, Singapore and the US have adopted cybersecurity regulations, that are not distinct to the CAVs (Taeihagh and Lim, 2019). Australia and Germany are also becoming conscious of the threats involved with the CAV's cybersecurity, while the UK has plans to utilise cybersecurity hazards as an incentive to boost the competitive ability of the country (Cabinet Office, 2016; Lim and Taeihagh, 2018). CAVs and connected infrastructure require a continuous surveillance system to alert the relevant operation centre immediately about any data or vehicle breaches, including unauthorised access, control or operation (Hodge et al., 2019).

3.6. Integrated management framework for CAVs cybersecurity

This section underlines the importance of addressing safety and security standards for the roll-out and operation of CAVs in an integrated manner. CAVs telematics network would be the most appropriate example. The key components of the telematics are; i) subscriber identification module (SIM) cards, ii) input/output controllers, iii) engine interfaces, iv) accelerometers, and v) GPS receivers. Telematics is typically connected to external fleet operating systems of third parties, such as communications infrastructure and service database (Hodge et al., 2019). This establishes an external link to one or more CAV in a fleet. Since telematics connects with vehicles to gather data from the CAN and other communication systems; vulnerabilities in the CAV sensing capability may arise if the external network or physical telematics interface is compromised (Li et al., 2019; Wang et al., 2019a,2019b). Although, a potential approach will be to give a unique cryptographical key to each

telematics unit; however, to make it pragmatic, an integrated management co-operation framework is required.

Developments involved in the implementation of the CAVs are occurring primarily in the automotive, electronics and telecommunications industries. Value-creation of networks and closing information gaps between stakeholders are essential as well as the development of a shared vision for the entire value chain. Another concern is that most of the established processes are quality-oriented, with only a few safety-oriented, and no security-oriented. Moreover, there is no complete mapping of these standards. Therefore, it is of utmost importance to have an integration mechanism to ensure acceptable levels of cybersecurity risks.

4. Research gaps and future directions

Due to the high degree of non-linearity and variation of CAV cyber systems, risks cannot be asserted or calculated in conventional risk theory terms. Most publicised work is reactive, and vulnerabilities are typically undiscovered by white-hat hackers, hobbyists, and researchers. Cybersecurity challenges are on the rise, and cybercriminals are penetrating quickly. In this section, we spotlight a few promising areas which need further investigation.

4.1. Robust defensive techniques to identify, deter, and prevent CAVs cyber-attacks

V2C communication will be crucial for the successful operation of CAVs, but at the same time, it will be vulnerable to cyber-attacks on various interfaces and will require a robust ML and DL algorithms to identify, deter, and prevent cyber threats (Liang et al., 2018; Ye et al., 2018). While the essential elements are not modelling or algorithms, they are the abundance of data. A recent study reported that a CAV would have to travel up to hundreds of billions of miles across several scenarios to ensure statistical reliability relative to human drivers (Kalra and Paddock, 2016). Two main areas for further improvement of the attack surface analysis are; i) the integration of the system analysis, and ii) the understanding of rapidly evolving threats in various environments and scenarios.

The vulnerability of vehicle infotainment systems using the internet is an open field for in-depth research and review. The safety of V2C communication has not been investigated in detail and, unfortunately, security is not currently viewed by the automotive industry as a priority for V2C development. Because V2C technology is in its infancy, it would be appropriate for researchers to concentrate on strategies for testing the security of vehicle communication systems. CAVs safety is endangered if safety is compromised at any level. The task, though, is to ensure protection at all stack stages (Wang et al., 2019a,2019b). Therefore, the drafting of industrial safety authorization standards will be very beneficial in this regard (Liu et al., 2019).

Furthermore, we visualised the aggregate degree of keyword frequency in VOSviewer application for around 40 research articles (of the last 5 years), specifically related to the CAVs cyber safety, depicted in Fig. 10. Using VOSviewer app, users can visualise the main topics or thematic clusters, the interrelationships between the topics and the occurrence of those fields of study through infographics (Shaharudin et al., 2019). Visualising for the seven metrics of security performance assessment in Fig. 10, it is apparent that some of the popular thematic clusters have been “security”, “attack”, “communication”, “data”, “information” and “networks”. Small cluster on availability, reliability, robustness, and confidentiality in CAVs cyber-attacks assessment are observed suggesting relatively lesser work in this area. Nevertheless, cyber-attacks which fall under the categories of integrity, reliability and trustworthiness needs further rigorous analysis, assessment, and development of counter-mitigation strategies. A formal, systemized, dynamic, and multi-layered (cross-verification) approach to address these metrics based cyber-attacks will boost the CAVs safety.

4.2. Combating Physical/Proximity access attacks

Security and safety are processes, system designers need to stay up to date with the advances in attacks on the CAV-embedded system. First, an illusion attack or deceiving with a false traffic signal is an open field for study so that CAVs can operate smoothly without slowing down or limiting overall efficiency, especially at the intersections and multi-lane roads (Ali et al., 2019). Efficient detection mechanisms and algorithms are required to differentiate between genuine and fake or counterfeit

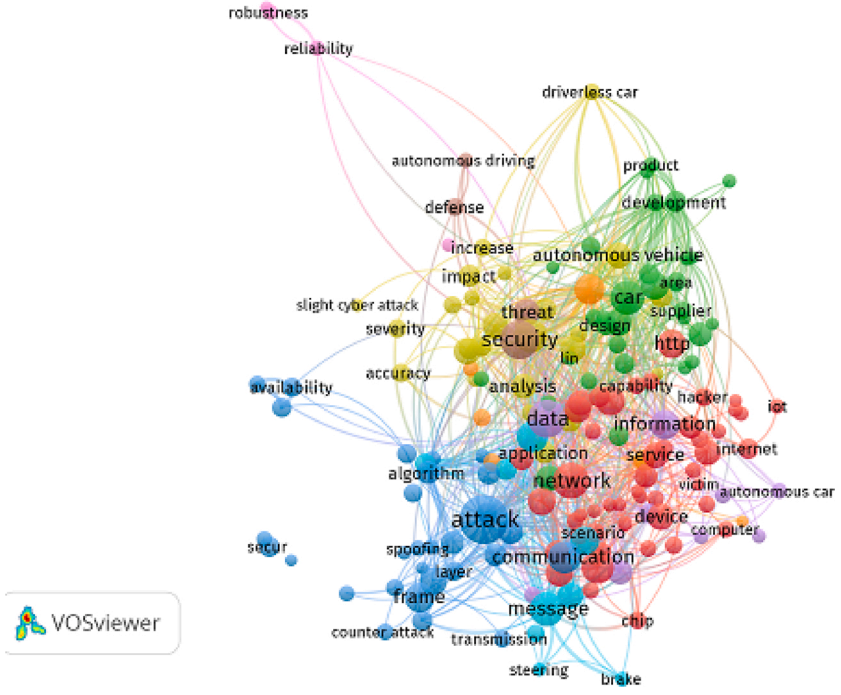

Fig. 10. Network visualization of keywords theme occurrences.

signs. Machine-readable road signs (e.g. UV QR overlay or PCM-light signals) with electronic signatures would make it secure in this context. Second, sensor tampering detectors required in-depth study and analysis, i.e., functionality and sensitivity of CAV-sensors need to be verified and notified instantaneously prior to CAV start-up. Development of anti-tampering devices in such a way that the physical access to the device does not opt for partial or full CAV network access. Besides, the safety assessment of the EV during charging is another area for further study, considering the aspects of grid protection, the safety of charging facilities, and security of communication.

4.3. Combating adversarial ML attacks on CAVs

ML and AI strategies are central ingredients in the success of several primary CAV functions. Nevertheless, ML/AI systems are susceptible to subtle adversarial perturbations that are deliberately designed. These perturbations could occur in voice (audio), vision (image), text and networking. The current defence mechanisms are ineffective in tracking and countering these perturbations. It has been observed that these defence mechanisms are only successful for a particular form of attack and fails for more vigorous or unknown assaults. It is therefore vital to establish new ML/AI protection strategies that are successful and productive, especially the auto-navigation framework of CAVs and preserving privacy as well.

4.4. CAVs infotainment system: ubiquitous connectivity

Infotainment systems in vehicles present the greatest potential of attacks on vehicle networks. OEM telematics service providers allow multiple infotainment systems to reach and communicate with the Internet, leading to vulnerabilities in CAV interconnections (Li et al., 2019). CAV infotainment systems compile and show details on the current state of various functionalities; however, infotainment device communication setup varies from supplier to vendor, model to model, and year to year (Hodge et al., 2019). Therefore, designing and countering specific attacks and generalising them is more challenging. This necessitates for the design of low latency two-fold mechanism; i) ensuring infotainment systems operate on a segregated communication network (other than the operational and safety network), i.e., ceasing IV bridged communication, and ii) configuring stringent user's access and augmenting digital signatures for mobile apps connected to the CAVs.

4.5. CAVs supply chain trust provisioning schemes

There is no existing mechanism for a formal engagement between road operators and suppliers, i.e. OEMs, data aggregators and suppliers to discuss the possibilities for addressing supply chain vulnerabilities; all present encounters are on an ad-hoc basis. Tech companies such as Google and Apple have made their claims on the driving markets of CAVs. Nonetheless, no one can win if security issues weaken consumer trust in CAVs. To alleviate these concerns, manufacturers need to integrate security into every part of their designs.

Trust provisioning schemes-The automotive industry is developing confidence-provisioning systems to tackle this issue at the architectural level; the notion is that assets are received from different stakeholders through a common, unified trust model. The trust model is usually established by the component manufacturer, which enables different stakeholders to inject assets at different stages. Blockchain security techniques and powerful AI approaches will make it easier to confront these difficulties. Each CAV and any outside communicator need to have a specific digital signature. Nevertheless, it is always the OEMs who are accountable for the reliability, quality, and safety of cars brandishing their logo.

4.6. Analysis of human behaviour concerning the safety of CAVs

Human factor researchers aim to recognise the most susceptible individuals in the CAVs cybersecurity, identify the types of scenarios they are struggling with, and develop tailored educational materials. Similarly, the drop in driving skills due to the use of CAVs and its relation to cybersecurity skills is also worth researching (Gkartzonikas and Gkritza, 2019; Linkov et al., 2019). Human-factor experts are conscious that improvements to CAVs cybersecurity may not necessarily maximise traffic safety. In Macher et al. (2017), the authors describe a scenario in which the steering wheel is blocked in a risky condition. This is safe from a cybersecurity point of view because the intruder cannot alter the direction of the steering wheel. However, it is not safe from a traffic perspective because the driver cannot react appropriately when the steering wheel is blocked. Investigators should consider these types of situations, i.e. where cybersecurity threats might be overestimated. Research on human behaviour concerning CAVs cybersecurity will be more appropriate in the future when people use CAVs regularly. Dedicated CAVs lanes are yet another future approach, but their impact on traffic safety and efficiency is still to be explored while taking into account two key factors; i) driver behaviour adaptation, and ii) manual and automated transitions in operational control (Rad et al., 2020).

4.7. Legal readiness in terms of policy, regulation, and liability of the CAVs

It has been witnessed that focusing solely on the market players for the production and distribution of CAVs is an ineffective solution in resolving the increasing death and accident tolls on our highways (Geels and Penna, 2015; Taeihagh and Lim, 2019). Strong legislation is therefore required that sets minimum vehicle safety performance before being exposed to cyber-attacks, i.e., hijacks and user privacy concerns. Similarly, where an incident happens that involves damage, such as the most recent one in Tesla, the liability needs to be clearly described that governs the legislation. (Boudette, 2017). Legal readiness in terms of policy and regulation, liability, privacy, and cybersecurity context will facilitate the untroubled roll-out of CAVs (Rosique et al., 2019). At the same time, state initiatives for the user acceptance, i.e. consumer acceptance, marketing and advertising, and affordable cost of CAVs will boost up these efforts. Finally, the legislation of relevant acts and rules will ensure smooth traffic and safety in terms of travel behaviour, transport supply, land use, economy, governance, and environment.

4.8. Integrated management framework for CAVs cybersecurity

Current state-of-the-art policy solutions do not provide a realistic mechanism to achieve the adaptability necessary for the complex, competitive, and diverse conditions under which CAVs operate. The journey to this destination is not easy since 84% of OEM employees and their vendors are concerned that cybersecurity measures are not keeping up with emerging technologies (Scalas and Giacinto, 2019). A recent study conducted by Austroads highlights that automotive manufacturers, data aggregators, vendors, and road operators are all interested in exploring techniques to realise value from crowdsourced and fleet-sourced CAVs-data for asset management purposes (Infrastructure-Australia, 2017). Providing a coordinated approach to CAV cybersecurity development would avoid duplication and sharing of the lessons learned could accelerate the learning process. This co-creation would adopt a shared problem-solving approach involving both the road operators (as customers) and suppliers such as automotive manufacturers, equipment manufacturers, data aggregators and data processors.

5. Conclusion

Connected and autonomous vehicles can see their environment,

evaluate the optimum route, and travel without human involvement for the entire journey. Nonetheless, there are challenges to the complete adoption of the CAV technology, and cybersecurity is one of them. In this review paper, we presented the CAV communication framework in an immersive way with a graphical flow chart to provide a concise picture of all the interfaces of CAV cyber-attacks in the ITS. We addressed the ineffectiveness of the orthodox CPS cybersecurity approaches for the CAVs. The summary of cyber-attacks on the CAVs, the respective CAV communication system, its impact and the corresponding mitigation strategies are presented. Besides, we identified the potential avenues that need to be addressed for the successful and timely battle against cyber-attacks. Moreover, each focused area is supported with research gaps and future direction which would facilitate CAV academics, application creators and decision-makers in defining and creating a comprehensive CAV-cybersecurity framework.

CRediT authorship contribution statement

Shah Khalid Khan: Investigation, Data curation, Methodology, Writing - original draft. **Nirajan Shiwakoti:** Conceptualization, Supervision, Writing - review & editing. **Peter Stasinopoulos:** Supervision, Writing - review & editing. **Yilun Chen:** Writing - review & editing.

Declaration of Competing Interest

The authors report no declarations of interest.

Acknowledgements

The authors would also like to acknowledge the Australian Government, Department of Industry, Innovation and Science for the financial support received for this study through the Automotive Engineering Graduate Program (GRANT NO: AEGP000050). The views expressed by the authors do not necessarily reflect those of the funding agency. The authors would also like to acknowledge three anonymous reviewers whose feedback have helped us to improve the paper.

References

Al Zaabi, A.O., Yeun, C.Y., Damiani, E., 2019. Autonomous vehicle security: conceptual model. 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific). IEEE 1–5.

Ali, Y., Haque, M.M., Zheng, Z., Washington, S., Yildirimoglu, M., 2019. A hazard-based duration model to quantify the impact of connected driving environment on safety during mandatory lane-changing. Transp. Res. Part C Emerg. Technol. 106, 113–131.

Ali, Y., Sharma, A., Haque, M.M., Zheng, Z., Saifuzzaman, M., 2020a. The impact of the connected environment on driving behavior and safety: a driving simulator study. Accid. Anal. Prev. 144, 105643.

Ali, Y., Zheng, Z., Haque, M.M., Yildirimoglu, M., Washington, S., 2020b. Understanding the discretionary lane-changing behaviour in the connected environment. Accid. Anal. Prev. 137, 105463.

Amirtahmasebi, K., Jalalinia, S.R., 2010. Vehicular networks-Security, Vulnerabilities and Countermeasures. http://publications.lib.chalmers.se/records/fulltext/123778.pdf.

Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H.M., Rowe, J., Levitt, K., 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. Ieee Commun. Mag. 53 (6), 126–132.

Anouar, B., Mohammed, B., Abderrahim, G., Mohammed, B., 2016. Vehicular navigation spoofing detection based on V2I calibration. 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt). IEEE 847–849.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Comput. Human Behav. 69, 437–443.

Azogu, I.K., Ferreira, M.T., Larcom, J.A., Liu, H., 2013. A new anti-jamming strategy for VANET metrics-directed security defense. 2013 IEEE Globecom Workshops (GC Wkshps). IEEE 1344–1349.

Becher, A., Benenson, Z., Dornseif, M., 2006. Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp. 104–118.

Behere, S., Torngren, M., 2015. A functional architecture for autonomous driving. 2015 First International Workshop on Automotive Software Architecture (WASA). IEEE 3–10.

Bergin, D.L., 2015. Cyber-attack and defense simulation framework. J. Def. Model. Simul. Appl. Methodol. Technol. 12 (4), 383–392.

BMW-Group, 2018. Experimental Security Assessment of BMW Cars: A Summary Report. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf.

Boudette, N.E., 2017. Tesla's Self-driving System Cleared in Deadly Crash. The New York Times 19. https://www.nytimes.com/2017/2001/2019/business/tesla-model-s-autopilot-fatal-crash.html.

Brandts, J., Rott, C., Solà, C., 2016. Not just like starting over-Leadership and revivification of cooperation in groups. Exp. Econ. 19 (4), 792–818.

Cabinet Office, 2016. National Security and Intelligence, HM Treasury, and the Rt Hon Philip Hammond MP. National cyber security strategy, pp. 2016–2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Carsten, P., Andel, T.R., Yampolskiy, M., McDonald, J.T., 2015. In-vehicle networks: attacks, vulnerabilities, and proposed solutions. Proceedings of the 10th Annual Cyber and Information Security Research Conference 1–8.

Cho, K.-T., Shin, K.G., 2016. Fingerprinting electronic control units for vehicle intrusion detection. 25th {USENIX} Security Symposium ({USENIX} Security 16) 911–927.

Choi, W., Joo, K., Jo, H.J., Park, M.C., Lee, D.H., Security, 2018a. Voltageids: low-level communication characteristics for automotive intrusion detection system. IEEE Trans. Inf. Forensics Secur. 13 (8), 2114–2129.

Choi, W., Seo, M., Lee, D.H., 2018b. Sound-proximity: 2-factor authentication against relay attack on passive keyless entry and start system. J. Adv. Transp. 2018.

Cui, L., Hu, J., Park, B.B., Bujanovic, P., 2018. Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: assessing cooperative adaptive cruise control under cyber attack. Transp. Res. Part C Emerg. Technol. 97, 1–22.

Cui, J., Liew, L.S., Sabaliauskaite, G., Zhou, F., 2019. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Netw. 90, 101823.

Czerwinski, D., Nowak, J., Przylucki, S., 2019. An impact of jamming Signal on the energy efficiency of ZigBee network elements. International Conference on Computer Networks 62–75.

Decisions, T., 2019. Outdated Firmware Could Be Putting IP Camera Security at Risk. https://www.technologydecisions.com.au/content/security/news/outdated-firmware-could-be-putting-ip-camera-security-at-risk-994422321.

Dey, K.C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., Martin, J., 2016. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. Transp. Res. Part C Emerg. Technol. 68, 168–184.

Dixit, V.V., Chand, S., Nair, D., 2016. Autonomous vehicles: disengagements, accidents and reaction times. PLoS One 11 (12), e0168054.

Dogan, E., Rahal, M.-C., Deborne, R., Delhomme, P., Kemeny, A., Perrin, J., 2017. Transition of control in a partially automated vehicle: effects of anticipation and non-driving-related task involvement. Transp. Res. Part F Traffic Psychol. Behav. 46, 205–215.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P., 2019. Cybersecurity challenges in vehicular communications. Veh. Commun., 100214

Foster, I., Prudhomme, A., Koscher, K., Savage, S., 2015. Fast and Vulnerable: a Story of Telematic Failures, 9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15).

Francillon, A., Danev, B., Capkun, S., 2011. Relay attacks on passive keyless entry and start systems in modern cars. Proceedings of the Network and Distributed System Security Symposium (NDSS),Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

Gagandeep, A., Kumar, P., Technology, A., 2012. Analysis of different security attacks in MANETs on protocol stack A-review. Int. J. Eng. 1 (5), 269–275.

Geels, F.W., Penna, C.C., 2015. Societal problems and industry reorientation: elaborating the Dialectic Issue LifeCycle (DILC) model and a case study of car safety in the USA (1900–1995). Res. Policy 44 (1), 67–82.

Gehrig, S.K., Stein, F.J., 1999. Dead reckoning and cartography using stereo vision for an autonomous car. In: Proceedings 1999 IEEE/RSJ International Conference on Intelligent Robots and Systems. Human and Environment Friendly Robots with High Intelligence and Emotional Quotients (Cat. No. 99CH36289). IEEE, pp. 1507–1512.

Gkartzonikas, C., Gkritza, K., 2019. What have we learned? A review of stated preference and choice studies on autonomous vehicles. Transp. Res. Part C Emerg. Technol. 98, 323–337.

Greenberg, A., 2015. GM took 5 Years to fix a full-takeover hack in millions of Onstar cars. Wired 10 (September), 1059-1028.

Gurion, B., 2019. Autonomous Vehicles Fooled by Drones That Project Too-quick-for-humans Road-signs. https://boingboing.net/2019/2007/2006/flickering-car-ghosts.html.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3 (7), e00346.

Hasbullah, H.S., Ahmed, Irshad, 2010. Denial of service (dos) attack and its possible solutions in VANET. Int. J. Electron. Commun. Eng. 4 (5), 813–817.

He, H., 2018. Cybersecurity Law Causing "mass Concerns" Among Foreign Firms in China. South China Morning Post. https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china.

He, B.Y., Chow, J.Y., 2019. Optimal privacy control for transport network data sharing. Transp. Res. Part C Emerg. Technol.

He, Q., Meng, X., Qu, R., 2017. Survey on cyber security of CAV. In: 2017 Forum on Cooperative Positioning and Service (CPGPS). IEEE, pp. 351–354.

Hennessy, A.P., 1916. Implementation of Physical Layer Security of an Ultra-wideband Transceiver (Doctoral Dissertation, Engineering).

Hodge, C., Hauck, K., Gupta, S., Bennett, J.C., 2019. Vehicle Cybersecurity Threats and Mitigation Approaches, in: National Renewable Energy Lab.(NREL), G., CO (United States) (Ed.).
Holt, T.J., Burruss, G.W., Bossler, A.M., 2010. Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. J. Crime Justice 33 (2), 31–61.
Hortelano, J., Ruiz, J.C., Manzoni, P., 2010. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. 2010 IEEE International Conference on Communications Workshops. IEEE 1–5.
Infrastructure-Australia, 2017. Automated Vehicles Do We Know Which Road to Take? https://infrastructure.org.au/wp-content/uploads/2017/2009/AV-paper-FINAL.pdf.
Julisch, K., 2013. Understanding and overcoming cyber security anti-patterns. Comput. Netw. 57 (10), 2206–2211.
Kalra, N., Paddock, S.M., 2016. Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? Transp. Res. Part A Policy Pract. 94, 182–193.
Katerina, T., Nicolaos, P., 2018. Mouse behavioral patterns and keystroke dynamics in End-User Development: What can they tell us about users' behavioral attributes? Comput. Human Behav. 83, 288–305.
Kennedy, J., Holt, T., Cheng, B., 2019. Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. J. Crime Justice 1–14.
Khan, S.K., Farasat, M., Naseem, U., Ali, F., 2020. Performance evaluation of next-generation wireless (5G) UAV relay. Wirel. Pers. Commun. 1–16.
King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B., Sample, C., 2018. Characterizing and measuring maliciousness for cybersecurity risk assessment. Front. Psychol. 9, 39.
Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., 2010. Experimental security analysis of a modern automobile. 2010 IEEE Symposium on Security and Privacy. IEEE 447–462.
Krishnapriya, V., Sikha, M., Nandakumar, R., Kidav, J.U., 2012. Hardware efficiency comparison of IP cores for CAN & LIN protocols. In: 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12). IEEE, pp. 1–3.
Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, S., Kolter, J.Z., Langer, D., Pink, O., Pratt, V., 2011. Towards fully autonomous driving: systems and algorithms. In: 2011 IEEE Intelligent Vehicles Symposium (IV). IEEE, pp. 163–168.
Li, Y., Tu, Y., Fan, Q., Dong, C., Wang, W., 2018. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. Accid. Anal. Prev. 121, 148–156.
Li, Y., Luo, Q., Liu, J., Guo, H., Kato, N., 2019. TSP security in intelligent and connected vehicles: challenges and solutions. IEEE Wirel. Commun. 26 (3), 125–131.
Liang, L., Ye, H., Li, G.Y., 2018. Toward intelligent vehicular networks: a machine learning framework. IEEE Internet Things J. 6 (1), 124–135.
Lim, H.S.M., Taeihagh, A., 2018. Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. Energies 11 (5), 1062.
Linkov, V., Zámečník, P., Havlíčková, D., Pai, C.-W., 2019. Human factors in the cybersecurity of autonomous vehicles: trends in current research. Front. Psychol. 10, 995.
Liu, J., Ma, D., Weimerskirch, A., Zhu, H., 2017a. A functional co-design towards safe and secure vehicle platooning. Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security 81–90.
Liu, J., Zhang, S., Sun, W., Shi, Y., 2017b. In-vehicle network attacks and countermeasures: challenges and future directions. IEEE Netw. 31 (5), 50–58.
Liu, S., Tang, J., Wang, C., Wang, Q., Gaudiot, J.-L., 2017c. A unified cloud platform for autonomous driving. Computer 50 (12), 42–49.
Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y., Shi, W., 2019. Edge computing for autonomous driving: opportunities and challenges. Proc. IEEE 107 (8), 1697–1716.
Liu, L., Wu, B., Shi, W., 2020. A Comparison of Communication Mechanisms in Vehicular Edge Computing, 3rd {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 20).
Lopez, A., Malawade, A.V., Al Faruque, M.A., Boddupalli, S., Ray, S., 2019. Security of Emergent Automotive Systems: A Tutorial Introduction and Perspectives on Practice. IEEE Des. Test 36 (6), 10–38.
Lyamin, N., Kleyko, D., Delooz, Q., Vinel, A., 2019. Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining. IEEE Commun. Lett. 23 (3), 442–445.
Macher, G., Armengaud, Eric, Messnarz, Richard, Riel, Andreas, Brenner, Eugen, Kreiner, Christian, 2017. Integrated safety and security development in the automotive domain. SAE Technical Papers 2017 (March).
Markham, T.R., Chernoguzov, A., 2017. A balanced approach for securing the OBD-II port. SAE Int. J. Passenger Cars-Electr. Electr. Syst. 10 (2017-01–1662), 390–399.
Mejri, M.N., Ben-Othman, J., Hamdi, M., 2014. Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. 1 (2), 53–66.
Miller, C., Valasek, C., 2015. Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015, 91.
Möller, D.P., Haas, R.E., 2019. Guide to Automotive Connectivity and Cybersecurity. Springer.
Morris, D., Madzudzo, G., 2018. Cybersecurity and the auto industry: the growing challenges presented by connected cars. Int. J. Automot. Technol. Manag. 18 (2), 105–118.
Muciaccia, T., Passaro, V.M.N., 2017. Future scenarios for software-defined metro and access networks and software-defined photonics. Photonics 4 (1), 1.
Muhammad, M., Safdar, G.A., 2018. Survey on existing authentication issues for cellular-assisted V2X communication. Veh. Commun. 12, 50–65.
Nayegandhi, A., 2007. LIDAR Technology Overview. ETI – US Geological Survey, Florida integrated Science Center, St. Petersburg, FL 33701. 17. http://www.ce.siue.edu/faculty/hzhou/Highway%20Inventory%20Refereces/Nayegandhi_Lidar_Technology_Overview.pdf.
Nie, S., Liu, L., Du, Y., 2017. Free-fall: hacking tesla from wireless to can bus. Briefing, Black Hat USA 1–16.
Nissan, 2016. Hacker Takes Control of Nissan Electric Vehicle From Other Side of the World Through Leaf App. https://www.ibtimes.co.uk/hacker-takes-control-nissan-electric-vehicle-other-side-world-through-leaf-app-1545808.
Noy, I.Y., Shinar, D., Horrey, W.J., 2018. Automated driving: safety blind spots. Saf. Sci. 102, 68–78.
Onishi, H., Wu, K., Yoshida, K., Kato, T., 2017. Approaches for vehicle cyber-security in the US. Int. J. Automot. Eng. Technol. 8 (1), 1–6.
Parkinson, S., Ward, P., Wilson, K., Miller, J., 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. 18 (11), 2898–2915.
Parno, B., Perrig, A., 2005. Challenges in Securing Vehicular Networks, Workshop on Hot Topics in Networks (HotNets-IV). Maryland, USA, pp. 1–6.
Pawade, S., Shah, S., Tijare, D., 2013. Zigbee based intelligent driver assistance system. Int. J. Eng. Res. Appl. 3, 1463–1468.
Petit, J., Feiri, M., Kargl, F., 2014. Revisiting attacker model for smart vehicles. In: 2014 IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC 2014). IEEE, pp. 1–5.
Petit, J., Stottelaar, B., Feiri, M., 2015. Remote attacks on automated vehicles sensors: experiments on camera and lidar. Black Hat Europe 11, 2015.
Puñal, O., Aktaş, I., Schnelke, C.-J., Abidin, G., Wehrle, K., Gross, J., 2014. Machine learning-based jamming detection for IEEE 802.11: design and experimental evaluation. In: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. IEEE, pp. 1–10.
Rad, S.R., Farah, H., Taale, H., van Arem, B., Hoogendoorn, S.P., 2020. Design and operation of dedicated lanes for connected and automated vehicles on motorways: a conceptual framework and research agenda. Transp. Res. Part C Emerg. Technol. 117, 102664.
Raiyn, J., 2013. Handoff self-management based on SNR in mobile communication networks. Int. J. Wirel. Mob. Comput. 6 (1), 39–48.
Raiyn, J., 2018. Data and cyber security in autonomous vehicle networks. Transp. Telecommun. 19 (4), 325–334.
Rawat, A., Sharma, S., Sushil, R., 2012. VANET: security attacks and its possible solutions. J. Inf. Oper. Manag. 3 (1), 301.
Rosique, F., Navarro, P.J., Fernández, C., Padilla, A., 2019. A systematic review of perception system and simulators for autonomous vehicles research. Sensors 19 (3), 648.
Rouf, I., Miller, R.D., Mustafa, H.A., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., Seskar, I., 2010. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, USENIX Security Symposium.
Roy, N., Shen, S., Hassanieh, H., Choudhury, R.R., 2018. Inaudible voice commands: the long-range attack and defense. 15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18) 547–560.
SAE-International, 2018. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-road Motor Vehicles.
Scalas, M., Giacinto, G., 2019. Automotive cybersecurity: foundations for next-generation vehicles. In: 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS). IEEE, pp. 1–6.
Seuwou, P., Banissi, E., Ubakanma, G., 2020. The future of mobility with connected and Autonomous vehicles in smart cities. Digital Twin Technologies and Smart Cities. Springer, pp. 37–52.
Shaharudin, M.S., Fernando, Y., Jabbour, C.J.C., Sroufe, R., Jasmi, M.F.A., 2019. Past, present, and future low carbon supply chain management: a content review using social network analysis. J. Clean. Prod. 218, 629–643.
Sharma, A., Zheng, Z., Kim, J., Bhaskar, A., Haque, M., 2020. Is an informed driver a better decision maker? A grouped random parameters with heterogeneity-in-means approach to investigate the impact of the connected environment on driving behaviour in safety-critical situations. Anal. Methods Accid. Res., 100127
Shin, H., Kim, D., Kwon, Y., Kim, Y., 2017. Illusion and dazzle: adversarial optical channel exploits against lidars for automotive applications. International Conference on Cryptographic Hardware and Embedded Systems 445–467.
Shrestha, R., Bajracharya, R., Shrestha, A.P., Nam, S.Y., 2019. A new type of blockchain for secure message exchange in VANET. Digit. Commun. Netw.
Sinha, A., Chand, S., Wijayaratna, K.P., Virdi, N., Dixit, V., 2020. Comprehensive safety assessment in mixed fleets with connected and automated vehicles: a crash severity and rate evaluation of conventional vehicles. Accid. Anal. Prev. 142, 105567.
Solon, O., 2016. Team of hackers take remote control of Tesla Model S from 12 miles away. The Guardian 20.
Stasinopoulos, P., Shiwakoti, N., Beining, M., 2020. Use-stage life cycle greenhouse gas emissions of the transition to an autonomous vehicle fleet: A System Dynamics approach. Journal of Cleaner Production 278, 123447.
Sumra, I.A., Ab Manan, J.-L., Hasbullah, H., 2011. Timing attack in vehicular network. In: Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), Corfu Island. Greece, pp. 151–155.
Taeihagh, A., Lim, H.S.M., 2019. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transp. Rev. 39 (1), 103–128.
Tang, J., Liu, S., Yu, B., Shi, W., 2018. Pi-edge: a low-power edge computing system for real-time autonomous driving services. arXiv preprint arXiv 04978.
Tanuja, K., Sushma, T., Bharathi, M., Arun, K., 2015. A survey on VANET technologies..

Taylor, A., Japkowicz, N., Leblanc, S., 2015. Frequency-based anomaly detection for the automotive CAN bus, 2015 World Congress on Industrial Control Systems Security (WCICSS). IEEE 45–49.
TencentKeen-SecurityLab, 2019. Experimental Security Research of Tesla Autopilot. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf(Ed.).
Van der Heijden, R.W., Kargl, F., Abu-Sharkh, O.M., 2016. Enhanced position verification for VANETs using subjective logic. In: 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). IEEE, pp. 1–7.
Verma, S., Mallick, B., Verma, P., 2015. Impact of gray hole attack in VANET. In: 2015 1st International Conference on Next Generation Computing Technologies (NGCT). IEEE, pp. 127–130.
Vijaykumar, V., Elango, S., 2014. Hardware implementation of tag-reader mutual authentication protocol for RFID systems. Integration 47 (1), 123–129.
Wang, J., Shao, Y., Ge, Y., Yu, R., 2019a. A survey of vehicle to everything (V2X) testing. Sensors 19 (2), 334.
Wang, Y., Liu, L., Zhang, X., Shi, W., 2019b. HydraOne: An Indoor Experimental Research and Education Platform for CAVs, 2nd {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 19).
Wang, P., Wu, X., He, X., 2020. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. Transp. Res. Part C Emerg. Technol. 115, 102625.
Weiß, C., 2011. V2X communication in Europe–from research projects towards standardization and field testing of vehicle communication technology. Comput. Netw. 55 (14), 3103–3119.
Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E., Mayhorn, C.B., 2015. Will the "Phisher-Men" Reel you in?: assessing individual differences in a phishing detection task. Int. J. Cyber Behav. Psychol. Learn. 5 (4), 1–17.
Wesson, K.D., Shepard, D.P., Bhatti, J.A., Humphreys, T.E., 2011. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. Radionavigation Laboratory Conference Proceedings.
West, D.M., 2016. Moving Forward: Self-driving Vehicles in China, Europe, Japan, Korea, and the United States. Center for Technology Innovation at Brookings, Washington, DC, USA.
Xu, C., Liu, H., Li, P., Wang, P., 2018. A remote attestation security model based on privacy-preserving blockchain for V2X. IEEE Access 6, 67809–67818.
Yan, C., Xu, W., Liu, J., 2016. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. DEF CON 24.
Ye, H., Liang, L., Li, G.Y., Kim, J., Lu, L., Wu, M., 2018. Machine learning for vehicular networks: recent advances and application examples. IEEE Veh. Technol. Mag. 13 (2), 94–101.
Yu, B., Xu, C.-Z., Xiao, B., 2013. Detecting sybil attacks in VANETs. J. Parallel Distrib. Comput. 73 (6), 746–756.
Yuan, X., Chen, Y., Zhao, Y., Long, Y., Liu, X., Chen, K., Zhang, S., Huang, H., Wang, X., Gunter, C.A., 2018. Commandersong: a Systematic Approach for Practical Adversarial Voice Recognition, 27th {USENIX} Security Symposium ({USENIX} Security 18), pp. 49–64.
Zhang, T., Antunes, H., Aggarwal, S., 2014. Defending connected vehicles against malware: challenges and a solution framework. IEEE Internet Things J. 1 (1), 10–21.
Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., Xu, W., 2017. Dolphinattack: inaudible voice commands. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 103–117.
Zhang, R., Xue, R., Liu, L., 2019. Security and privacy on blockchain. ACM Comput. Surv. 52 (3), 1–34.
Zhao, X., Wang, Z., Xu, Z., Wang, Y., Li, X., Qu, X., 2020. Field experiments on longitudinal characteristics of human driver behavior following an autonomous vehicle. Transp. Res. Part C Emerg. Technol. 114, 205–224.
Zhou, M., Qin, Z., Lin, X., Hu, S., Wang, Q., Ren, K., 2019. Hidden voice commands: attacks and defenses on the vcs of autonomous driving cars. IEEE Wirel. Commun. 26 (5), 128–133.