Received 6 November 2021; revised 25 December 2021; accepted 11 January 2022. Date of publication 14 January 2022; date of current version 4 February 2022.

Digital Object Identifier 10.1109/OJCOMS.2022.3143098

Towards 6G-Enabled Internet of Vehicles: Security and Privacy

DIANA PAMELA MOYA OSORIO [1] (Member, IEEE), IJAZ AHMAD [2] (Member, IEEE), JOSÉ DAVID VEGA SÁNCHEZ [3] (Member, IEEE), ANDREI GURTOV [4] (Senior Member, IEEE), JOHAN SCHOLLIERS [2], MATTI KUTILA [2], AND PAWANI PORAMBAGE [1] (Member, IEEE)

[1]Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland

[2]VTT Technical Research Centre of Finland Ltd., 02150 Espoo, Finland

[3]Departamento de Electrónica, Telecomunicaciones y Redes de Información, Escuela Politécnica Nacional, Quito 170525, Ecuador

[4]Department of Computer and Information Science (IDA), Linköping University, 581 83 Linköping, Sweden

CORRESPONDING AUTHOR: D. P. MOYA OSORIO (e-mail: diana.moyaosorio@oulu.fi)

This work was supported in part by the Academy of Finland 6G Flagship under Grant 318927 and Project FAITH under Grant 334280; in part by the 5G-SAFEplus Celtic+ Project; in part by the Business Finland; and in part by the EU Project AirMOUR (Enabling Sustainable Airmobility in Urrban Contexts via Emergency and Medical Services) under Grant 101006601.

ABSTRACT The conceptualisation of the sixth generation of mobile wireless networks (6G) has already started with some potential disruptive technologies resonating as enablers for driving the emergence of a number of innovative applications. Particularly, 6G will be a prominent supporter for the evolution towards a truly Intelligent Transportation System and the realization of the Smart City concept by fulfilling the limitations of 5G, once vehicular networks are becoming highly dynamic and complex with stringent requirements on ultra-low latency, high reliability, and massive connections. More importantly, providing security and privacy to such critical systems should be a top priority as vulnerabilities can be catastrophic, thus there are huge concerns regarding data collected from sensors, people and their habits. In this paper, we provide a timely deliberation of the role that promissory 6G enabling technologies such as artificial intelligence, network softwarisation, network slicing, blockchain, edge computing, intelligent reflecting surfaces, backscatter communications, terahertz links, visible light communications, physical layer authentication, and cell-free massive multiple-input multiple-output (MIMO) will play on providing the expected level of security and privacy for the Internet of Vehicles.

INDEX TERMS 6G networks, Internet of Vehicles, privacy, security, vehicle-to-everything communications.

I. INTRODUCTION

THE INTERNET of Vehicles (IoV) has emerged as a new paradigm driven by the innovations in vehicular communications. In the IoV concept, vehicles are equipped with sensors, control and computing units, communication, storage, and learning capabilities, which allows the integration of smart vehicles with the Internet, transport infrastructure and other road users via vehicle-to-everything (V2X) communications [1], [2]. During long time, the only V2X solution was the dedicated short-range communication (DSRC), which is based on the IEEE 802.11.

In 2017, an advanced technology that relies on the capabilities of 4G, 5G and future 6G cellular networks was incorporated by the 3rd Generation Partnership Project (3GPP), the so-called cellular-enabled V2X or C-V2X, which can provide significantly higher system performance, higher spectral efficiency, higher range, reliability, and security, thus enabling higher levels of safety to more road users than alternative technologies. C-V2X employs two complementary transmission modes to enable a very broad range of driving safety features. These modes are the short-range direct communications (C-V2X Direct) and the long-range network communications (C-V2X Mobile Communications). C-V2X Direct comprises short-range communication between vehicles (V2V), between vehicles and infrastructure (V2I), and vehicles and pedestrians (V2P).

In the latter, C-V2X employs the conventional mobile network into the vehicle-to-network (V2N) communication to enable the vehicle to receive information about road conditions and traffic in the area, beyond the driver's line-of-sight (LoS) [3].

In this regard, IoV technologies are expected to address the main challenges of modern transportation, and, at the same time, being in line with the goals of a sustainable society. It is expected then, by 2025, connected cars could save 11,000 lives and lead to 260,000 fewer accidents, while avoiding 400,000 tonnes of CO2 emissions and saving 280 million hours of driving every year [3].

The evolution to IoV will rely on the efforts from different sectors including automobile, transportation, wireless communications and networking, robotics, as well as regulation organizations. In this sense, 6G plays a pivotal role on attaining the ambitious goals for IoV by satisfying the more rigorous key performance indicators (KPIs) that were partially fulfilled by 5G for vehicle communications. Indeed, it is expected that 5G use cases categories will evolve to Further enhanced Mobile Broadband (FeMBB), Mobile BroadBand and Low-Latency (MBBLL), ultra-massive Machine-Type Communication (umMTC), and massive Low-Latency Machine-Type communication (mLLMT) with extreme requirements such as data rates over 1 Tbps, end-to-end delays lower than 0.1 ms, network availability and reliability beyond 99.99999%, extreme connection density of over 10^7 devices/km^2, and spectrum efficiency over 5 times that of 5G while supporting extreme mobility [4]. Additionally, 6G is also targeting higher frequency bands (i.e., THz), thus allowing a more precise sensing and positioning resolution and enhanced beamforming directionality and data throughput. Indeed, 6G will be a self-learning intelligent network by leveraging artificial intelligence (AI) to deal with the expected complexity of networks and network management [5].

In this context, security and privacy are critical to ensure the expected resilience and reliability of future wireless networks, thus the investigation of these aspects from the very beginning of the conceptualisation of 6G is crucial in order to have a holistic picture of 6G security [6], [7]. Indeed, IoV applications bring new and challenging security and privacy threats towards drivers, passengers, and pedestrians, thus security defence systems and privacy protection mechanisms are critical to be investigated in order to provide initial guidelines towards secure and reliable IoV, and the role of 6G in this context is undoubtedly of paramount importance.

A. RELATED WORK

A survey on Long Term Evolution (LTE) and 5G technologies that support V2X is presented in [8]. This work summarizes the evolution towards 5G. Particularly, DSRC supporting communication in a short range among devices such as road-side units (RSUs), on-board units (OBUs) in vehicles, and pedestrian devices, had received a dedicated frequency range from the Federal Communications Commission in the United States in a move towards practical deployment. However, the challenges such as short range communication, large channel access delay and huge capital investments reinvigorated research for cellular network-based solutions. Therefore, the survey in [8] elaborates the efforts in LTE and 5G in this direction. The survey studies LTE V2X communication models, architectures, and operating scenarios as well as its challenges and possible solutions. Furthermore, it elucidates the technological enablers such as software-defined networking (SDN), multiple-input-multiple-output (MIMO), multi-access computing (MEC), slicing, etc., of 5G with regards to its facilitation of V2X, and sheds light on the challenges in 5G for V2X.

A detailed tutorial survey on access technologies for V2X is presented in [9]. The article provides the fundamental concepts and use-cases of vehicular networks, and then details the access technologies as enablers of V2X. Standard access technologies such as IEEE 802.11p, and cellular technologies such as LTE, LTE Advanced (LTE-A), 5G, and mix of different technologies termed as heterogeneous access technologies are discussed as the potential V2X access candidates. DSRC being the most widely researched and accepted technique still has to overcome several challenges including that of security, robustness and operational costs.

Automotive industry is focusing the effort to the hybrid communication where both short range and long range protocols are used for different applications. C-V2X Direct (PC5) is using 5.9 GHz channels (5855-5875 MHz and 5875-5925 MHz), which were originally allocated for IEEE802.11 based V2X. Today, the 5G Automotive Association (5GAA) is pushing co-existence of DSRC and C-V2X Direct in 5905-5925 MHz band, thus leaving 5875-5895 MHz to the future NR-V2X.

The article concludes that even though cellular technologies offer benefits compared to the other counterparts, struggles to provide low latency communication without direct Device-to-Device (D2D) communications.

Evolutionary technologies of V2X towards IoV are discussed in [1]. The article discusses the initial generation of V2X, i.e., DSRC, followed by a detailed overview of 802.11 V2X and cellular V2X standards. As emerging technological trends, the article focuses on the role of big data and cloud computing in terms of opportunities that these technologies provide, as well as the challenges laying ahead in its adoption. The main challenges in IoV big data, highlighted in the article, are related to data sourcing and transmission, whereas the challenges of cloud-based IoV are related to interoperability, trustworthiness, and resource allocation. A survey of technological evolution, standards and infrastructure of 5G for V2X communication to enable IoV is presented in [10]. The article sheds light on the evolution towards 5G from the perspectives of vehicular communications, and focuses on some of the latest technologies such as mmWave and SDN, and highlights the potential challenges. However, most

TABLE 1. Existing survey and literature review articles with main focus highlighted and compared to our article.

Publication year	Ref.	Focus	Limitations	Comparison with this work
2015	[11]	Pseudonym based privacy solutions for Vehicular Ad-hoc Networks (VANETs)	Limited to technologies that were used mostly before 5G	Our paper focuses on enabling technologies towards 6G-enabled IoV.
2018	[9]	A survey on access technologies for V2X	The focus is not on in-depth analysis of the security aspects	Our paper focuses on security and privacy aspects of C-V2X towards 6G-enabled IoV.
2019	[14]	V2X testing and verification techniques	Focused only on testing and verification techniques and LTE network	We focus on discussing security challenges and potentials of relevant enabling technologies towards 6G.
2020	[1]	Evolution from V2X to IoV in terms of emerging technologies	The scope is limited to the use of big data and cloud systems	Our scope is wider by considering our vision of key 6G enabling technologies and their challenges and potentials for security and privacy in IoV.
2020	[13]	A survey on cloud computing security for V2X	It is focused on one of the important enablers, i.e., cloud computing, thus limiting its scope	Our scope is wider by considering our vision of key 6G enabling technologies and their challenges and potentials for security and privacy in IoV.
2020	[15]	The applications of blockchain in IoVs towards Intelligent Transportation System (ITS)	The main focus is limited to blockchain and not the communication network	Our scope is wider by considering our vision of key 6G enabling technologies and their challenges and potentials for security and privacy in IoV.
2020	[10]	Technological evolution towards 5G for IoV	The main focus is on access technologies and lacks discussion on security aspects	Our focus is particularly security and privacy aspects of key 6G enabling technologies and their challenges and potentials for IoV.
2021	[8]	A survey on LTE and 5G technologies for V2X	Covers LTE and 5G for V2X, not the recent developments towards 6G, neither provides in details of the security landscape	Our focus is particularly security and privacy aspects of recent technologies of beyond 5G and 6G towards IoV.

of the focus is on radio technologies and does not provide insights into the security landscape.

Several surveys under the theme of V2X are published on specific topics such as security and privacy, integration of cloud-based systems, and technologies for improving latency, to name a few. For example, in [11], the author surveys the techniques for improving security and privacy of vehicular networks through pseudonym schemes. Different architectural design concepts for integrating cloud, edge, and fog-based systems for vehicular communications are surveyed in [12]. Once cloud-based systems are integrated into the vehicular networks, such as edge computing to meet the latency requirements, there is a possibility of exposing the network and nodes to security and privacy challenges. Therefore, security and privacy of connected vehicular cloud computing is discussed in [13]. Since V2X is still largely in the testing and experimenting phase, a survey on testing techniques for V2X is presented in [14]. The main focus is on testing techniques for communication using DSRC and LTE, whereas the technological shift is already happening beyond 5G. Blockchain is gaining traction in many applications in wireless networks, thus the role of blockchain in IoV is investigated in [15] mainly from the perspectives of management and security.

Table 1 describes existing survey and literature review articles relates to this work.

B. CONTRIBUTION AND ORGANIZATION

None of the existing survey articles cover the security of future IoV systems in detail. There is also a lack of studies on investigating the security challenges and potential solutions for IoV in the realm of the latest technological developments for 5G, such as massive MIMO, SDN, network function visualization (NFV), and edge computing, to name a few. Our article provides a detailed study on the security and privacy landscape of IoV from the perspectives of the novel technological developments that pave the path towards 6G. Since 5G has already been deployed and research on 6G has already begun, this article provides a timely deliberation on security of the IoV eco-system. In this sense, the following are the main contributions of this paper.

- We contextualize the IoV scenario by overviewing the evolution of V2X communications toward IoV, the use cases categories and their requirements by emphasizing on the aspects towards 6G-enabled V2X.
- We provide an overhaul on the security landscape for IoV in order to review the main security requirements and threats for IoV.
- We detail how potential 6G enabling technologies can be involved to enable a secure IoV ecosystem while describing promising state-of-the-art solutions. We also discuss some challenges ahead and potential research directions toward 6G-enabled IoV.
- We trace important aspects regarding privacy issues in IoV.

The rest of this tutorial is organized as follows (as shown in the high-level view in Fig. 1). In Section VI is presented the evolution from V2X towards IoV. Section III presents IoV use cases and requirements. The security landscape for IoV is shown in Section IV. Section V details the 6G key enabling

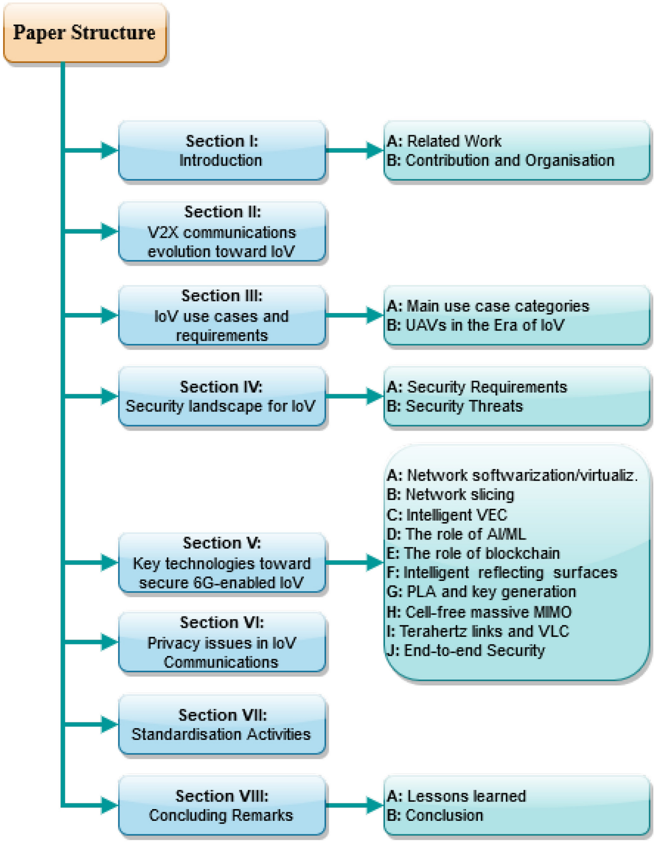

Paper Structure
Section I: Introduction
A: Related Work
B: Contribution and Organisation
Section II: V2X communications evolution toward IoV
Section III: IoV use cases and requirements
A: Main use case categories
B: UAVs in the Era of IoV
Section IV: Security landscape for IoV
A: Security Requirements
B: Security Threats
Section V: Key technologies toward secure 6G-enabled IoV
A: Network softwarization/virtualiz.
B: Network slicing
C: Intelligent VEC
D: The role of AI/ML
E: The role of blockchain
F: Intelligent reflecting surfaces
G: PLA and key generation
H: Cell-free massive MIMO
I: Terahertz links and VLC
J: End-to-end Security
Section VI: Privacy issues in IoV Communications
Section VII: Standardisation Activities
Section VIII: Concluding Remarks
A: Lessons learned
B: Conclusion

FIGURE 1. Paper Structure.

TABLE 2. Summary of acronyms.

Acronym	Definition
3GPP	3rd Generation Partnership Project
5GAA	5G Automotive Association
APIs	Application programming interfaces
AI	Artificial intelligence
XR	Augmented/mixed/virtual reality
AAA	Authentication, authorisation, and accounting
BC	Backscatter communication
BSM	Basic safety message
C-V2X	Cellular-enable vehicle-to-everything
COTS	Commercial off-the-shelf
CAM	Cooperative awareness message
CAM	Count-Min-Sketch
DENM	Decentralised environmental notification messages
DSRC	Dedicated short-range communication
DDoS	Distributed denial-of-service
D2D	Device-to-Device
ECUs	Electronic Control Units
ECTL	European Certificate Trusted List
ETSI	European Telecommunications Standards Institute
FL	Federated Learning
FeMBB	Further enhanced Mobile Broadband
FRMCS	Future Railway Mobile Communications System
GNSS	global navigation systems
HIP	Host Identity Protocol
ITS	Intelligent Transportation System
ITS	International Telecommunication Union
IETF	Internet Engineering Task Force
IoE	Internet of Everything
IoV	Internet of Vehicles
IRS	Intelligent reflecting surfaces
IVEC	Intelligent vehicular edge computing
IDS	Intrusion detection systems
IVI	In-vehicle-information
KPIs	Key performance indicators
LiDAR	Light Detection and Ranging
LoRa	Long Range
LTE	Long Term Evolution
mLLMT	Low-Latency Machine-Type communication
ML	Machine Learning
MBBLL	Mobile BroadBand and Low-Latency
MEC	Multi-access edge computing
MBMS	multimedia broadcast multicast service
MIMO	Multiple-input multiple-output
NFV	Network function virtualisation
NSI	Network slice instances
NR	New Radio
NOMA	Non-orthogonal multiple access
OBUs	On-board units
OWCs	optical wireless communications
OFDM	Orthogonal frequency division multiplexed
OBUs	Personally identifiable information
PSM	Personal safety message
PLA	Physical layer authentication
PLS	Physical layer security
PLK	Physical layer key
ProSe	Proximity services
PKI	Public key infrastructure
QoS	Quality-of-service
RATs	Radio access technologies
RFID	Radio-frequency identification
RSUs	Road-side units
SOP	Secrecy outage probability
SWPA	Secure wireless pilot authentication
SPAT	Signal phase and time
SAE	Society of Automotive Engineers
SDN	Software-defined networking
TLM	Trust List Manager
TTP	Trusted-third-party
umMTC	ultra-massive Machine-Type Communication
URLLC	Ultra-Reliable Low-Latency Communications
VLC	Visible Light Communication
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
V2I	Vehicle-to-infrastructure
V2N	Vehicle-to-network
V2P	Vehicle-to-pedestrian
VANETs	Vehicular Ad-hoc Networks
WLAN	Wireless Local Area Network

technologies that will impact security in IoV. Privacy issues are tackled in Section VI, while standardization activities are discussed in Section VII. Finally, concluding remarks are presented in Section VIII.

To assist the reader, a summary of acronyms used in this paper is given in Table 2.

II. V2X COMMUNICATIONS EVOLUTION TOWARD IOV

Over the past decade, the advent of wireless technologies has enabled the fast growth of vehicular communications, promising to radically change the transportation service standards for people worldwide. The early stage of wireless communications for automotive and ITS applications started with the DSRC era, which is based on multiple cooperating standards developed in the IEEE WiFi architecture. Since then, the DSRC technology was adopted as the core of V2X communications allocated on different reserved spectrum bands across the world for effective driving assistance, traffic safety, and ITS [1]. The DSRC development was standardized as an amendment to IEEE 802.11, namely IEEE 802.11p, focusing mainly on the simplicity distributed operation of the IEEE 802.11 MAC and PHY layers [16].

On the other hand, because IEEE 802.11p was optimized for Wireless Local Area Network (WLAN) with low mobility, it does not support neither dynamic network infrastructure nor high data rate transmission with high mobility [2]. At that time, the 3G cellular network was successfully operating; but, like the IEEE 802.11p-based DSRC, it could not meet the strict specifications required for V2X services. The IEEE 802.11bd standard was intended as an improved version of IEEE 802.11p to support high vehicular density, lower end-to-end latency, and noticeably increase the throughput offered by its predecessor [17].

3GPP launched C-V2X as an alternative technology to further enhance V2X technology. 3GPP Release 12/13 [18], [19] provides specifications for D2D proximity services (ProSe), where transmissions between two or more devices in proximity are supported over the sidelink interface without/with the help of a network infrastructure (i.e., eNodeB). Essentially, ProSe is similar to DSRC technology because they both use short-range communication; nevertheless, some differences emerge when inter-vehicle communication, high-speed scenarios, and information security come into play.

C-V2X roadmap begins with 3GPP Release 14 [20], where 4G-LTE is used to support V2X use cases, such as V2V, V2I, V2P, and V2N. Then, in Release 14, C-V2X provides data transport services for basic road safety applications such as cooperative awareness message (CAM), decentralized environmental notification messages (DENM), basic safety message (BSM), in-vehicle-information message (IVI), personal safety message (PSM), signal phase and time (SPAT) message and map message (MAP) [20].

3GPPP Release 15 [21] continues the evolution of C-V2X sidelink transmission underpinned by the first appearance of the 5G system. From an architectural perspective, Release 15 introduces key functionalities such as transmission diversity, carrier aggregation, and higher-order modulation (i.e., 64-QAM) to improve the throughput and reduce the maximum latency to 1-10 ms compared with the Release 14 counterpart (approx 20 ms) [21]. 3GPP Release 16 [22] constitutes the second stage of the 5G project, where the driving use cases encompassing advanced driving, truck platooning, remote driving, and extended sensors are the major contributions. To fulfill the stringent requirements for advanced V2X services and vehicle quality-of-service (QoS), Release 16 is based on the New Radio (NR) V2X architecture with the ability to enable the coexistence of NR and LTE sidelink transmissions and the opportunity to build cloud environments with computing resources for V2X services [22].

3GPP Release 17 [23] for V2X is oriented to offer enhancements to the specifications already working in Release 16. Specifically, Release 17 efforts will focus on the maturity of the NR radio-access technology, and the incorporation of NR-based multimedia broadcast multicast service (MBMS) to develop new use cases for V2X. Furthermore, taking advantage of the fact that wireless technologies will evolve in Release 17, V2X communications will surely benefit from NR MIMO systems, Ultra-Reliable Low-Latency Communications (URLLC), MEC, multi-radio dual connectivity, and many others [24].

3GPPP Release 18 is in its planning stage; future use cases are expected to be related not only to V2X but also to a variety of heterogeneous networks, devices, and vehicles communicating with each other. Moreover, Release 18 aims to introduce new use cases for Future Railway Mobile Communications System (FRMCS) within the Off-Network idea, just like virtual coupling data communications and complementary services (e.g., unicast/broadcast/multicast, and identification of devices and location). Moreover, exciting topics expected to be addressed in Release 18 include: 1) Railway Smart Station Services, i.e., passenger supporting tactile and multi-modality applications, real-time vehicular station operation and control, and business services, 2) vehicle-mounted relays to serve users within the vehicle or in the proximity to the vehicle, 3) machine learning (ML) models for identifying traffic features in automotive applications in order to enhance V2X performance in terms of data rate, reliability, security, latency, and coverage, and 4) accuracy of sidelink positioning (missing functionality in Release 17) in the context of autonomous vehicle applications [25].

Regarding a broader view of 3GPP-based V2X, the NR V2X development race is accelerating thanks to the joint efforts from standard organizations and industries. In this sense, the 5G Automotive Association (5GAA) formation has helped promote inter-operable solutions for C-V2X based on 5G and LTE research [26]. All technical findings of 5GAA, 3GPP, 5G-PPP, and IEEE 802.11 amendments have contributed to creating innovative solutions for the radio access technologies (RATs), system architecture, and privacy and security for IoV networks.

On the other hand, the forward-looking trend in which all smart things are connected via the Internet (i.e., IoT) leads to the inescapable development of the IoV. An unprecedented proliferation of new Internet of Everything (IoE) services is anticipated, taking IoV applications to unimaginable levels. Examples of such services range from holographic control 3D displays, immersive in-car infotainment, wireless brain-vehicle interfacing, traffic management through massive availability of small data, tactile and haptic communications, augmented/mixed/virtual reality (XR) to both flying vehicles and connected autonomous trucks, to name just a few [4]. All next-generation advanced V2X services will primarily require ultra-low latency, hyper-fast data rates, and visionary algorithms for personal data protection.

With the aforementioned in mind, it is very likely that 5G NR-based V2X networks will not mature enough for dazzling V2X services to be a reality, so its full potential will be realized with disruptive 6G wireless systems. Despite recent 6G research, the fundamental candidate technologies for 6G remain undefined. However, different from 5G era, 6G will not just go further on the exploration of new frequency bands or the use of evolving traditional technologies, but it will instead be a convergence of disruptive technologies [27]. Therefore, it is hard to imagine safer and more reliable next advanced V2X services without AI/MC and extensive use of RT; unique advantages 6G offers. Finally, the evolution of V2X communications toward IoV is summarized in Fig. 2.

III. IOV USE CASES AND REQUIREMENTS

To meet the expectations for IoV, V2X communications should comply with extremely stringent requirements, such as ultra low end-to-end latencies (< 5 ms), ultra high reliability ($\approx$99.999%), very high velocities (up to 150 km/h in average), high vehicle density (up to 500 vehicles/km^2 for highway and 1000 vehicles/km^2 for suburban environments), a maximum tolerable packet loss rate at the application layer of 10^{-5}, support of a wide range of V2X services,

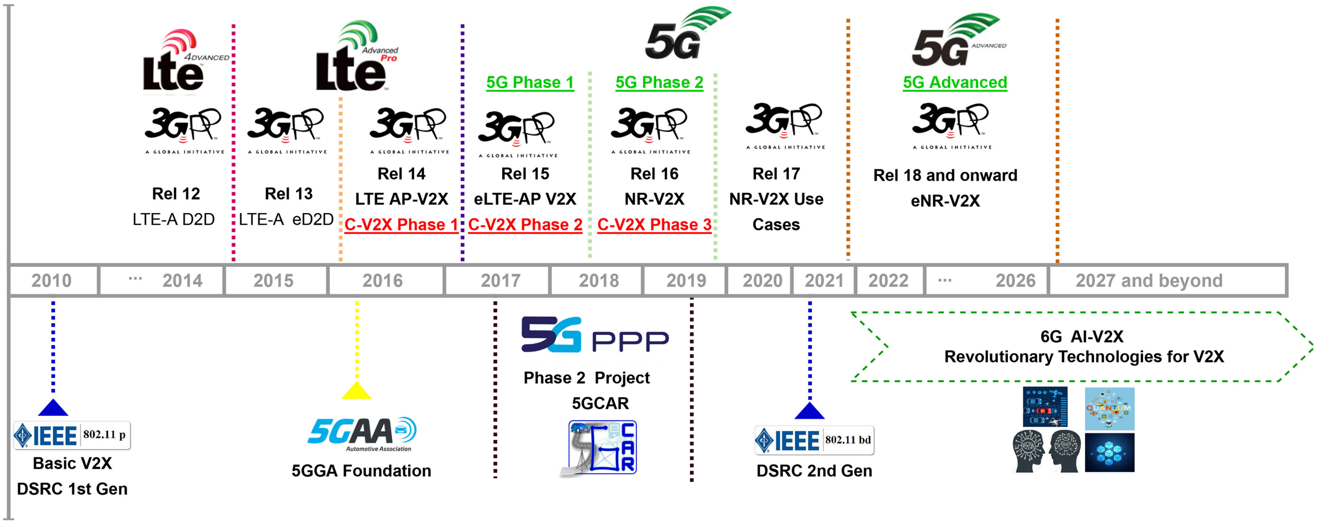
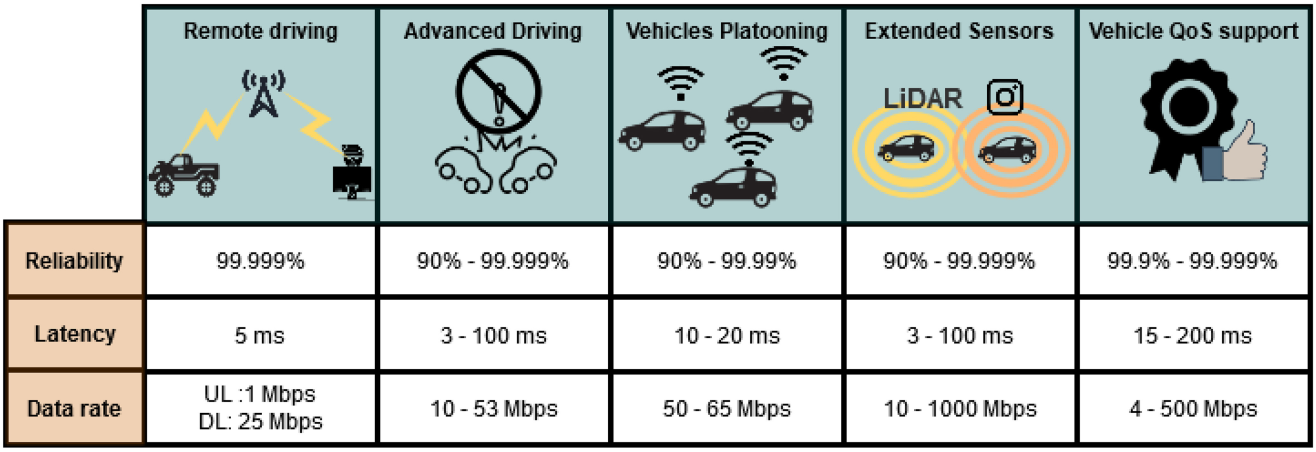


FIGURE 2. Evolution of V2X communications towards 6G-enabled IoV.



	Remote driving	Advanced Driving	Vehicles Platooning	Extended Sensors	Vehicle QoS support
Reliability	99.999%	90% - 99.999%	90% - 99.99%	90% - 99.999%	99.9% - 99.999%
Latency	5 ms	3 - 100 ms	10 - 20 ms	3 - 100 ms	15 - 200 ms
Data rate	UL :1 Mbps DL: 25 Mbps	10 - 53 Mbps	50 - 65 Mbps	10 - 1000 Mbps	4 - 500 Mbps

FIGURE 3. C-V2X use cases requirements (values take from 3GPP in its technical specification TS 22.186 of Release 16 [29]).

and advanced positioning (with accuracy of 30 cm and vulnerable road user accuracy of 10 cm) [28]. Under these requirements, a large number of use cases can be enabled and have been already proposed, although for most cases, less stringent requirements are adequate. In the following, we provide a high-level introduction of IoV use cases categories proposed by the 3GPP and their specific requirements, and we introduce the case of Unmanned Aerial Vehicles (UAVs) as special vehicles in the IoV.

A. MAIN USE CASE CATEGORIES

The 3GPP defined five use-case categories for C-V2X communications in its technical specification TS 22.186 of Release 16 [29]. These use case categories are described below and their specific requirements are presented in Fig. 3.

Remote driving: It contemplates that a remote driver or application is able to operate a remote vehicle when passengers cannot drive themselves or the remote vehicle is located in dangerous zones. It also considers driving based on cloud computing for predictable applications, e.g., public transportation.

Advanced driving: It covers the cases of semi-automated or fully-automated driving for longer inter-vehicle distance. By relying on the exchanging of data among vehicles or RSUs in the proximity, they are able to coordinate their trajectories or maneuvers, thus achieving safer traveling, collision avoidance, and enhanced traffic efficiency.

Vehicles platooning: Contemplates applications where vehicles are capable of dynamically assemble a group traveling together. For that purpose, there is a leading vehicle that sends periodic messages to the others to perform platoon operations. Through these operations, the distance among vehicles can be significantly reduced (in the order of sub second when distance is translated to time).

Extended sensors: This allows vehicles to improve their perception of the environment by overcoming the limitations of their sensors, as raw or processed data from sensors can be exchanged among RSUs, vehicles, devices of pedestrians, and V2X application servers.

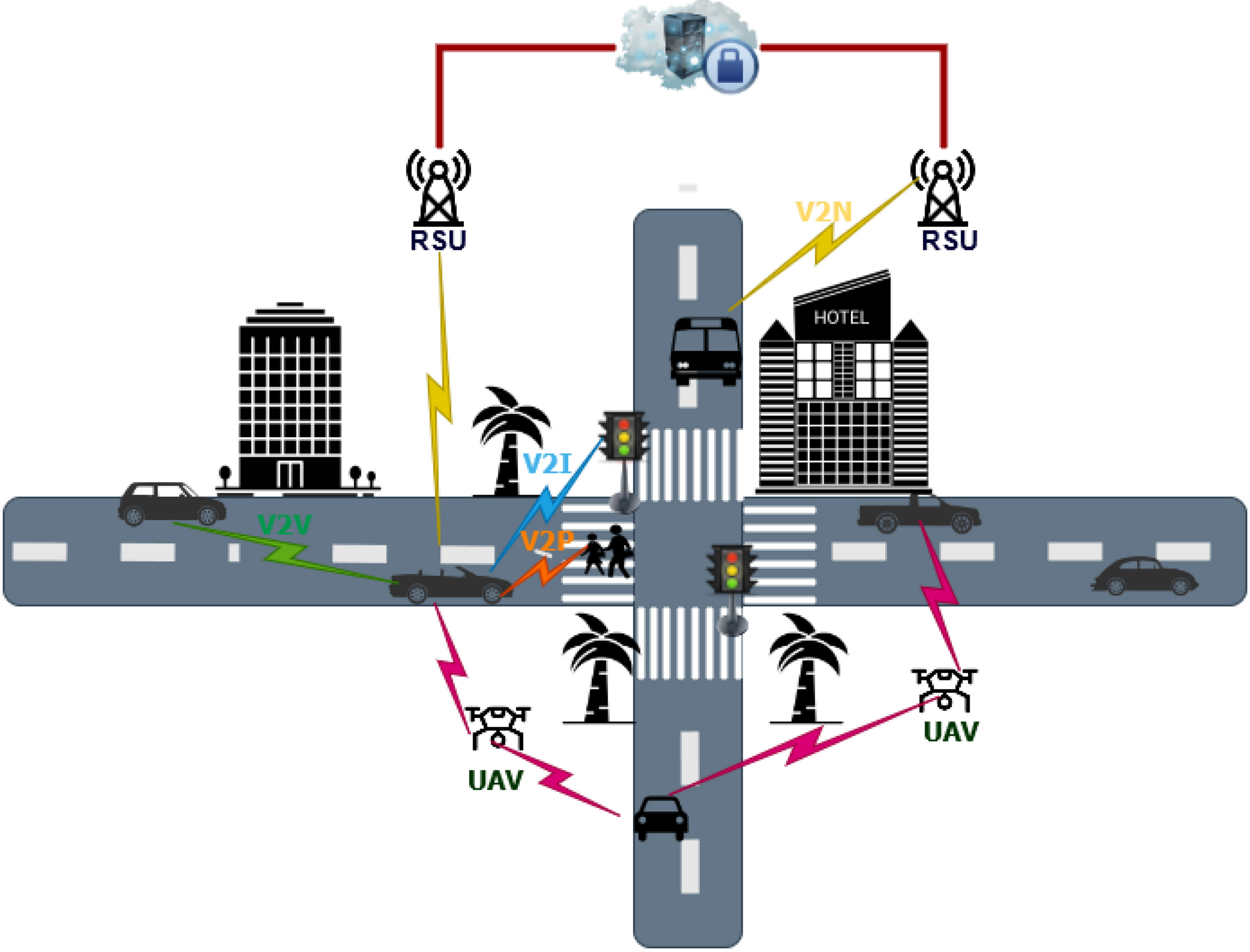


FIGURE 4. Illustration on types of V2X communications and UAV-assisted communication in IoV.

Vehicle QoS support: It allows an IoV application to be notified of possible changes on the QoS before a change occurs, thus the application can adjust to the conditions of 3GPP system. It is also possible for the 3GPP system to adapt the QoS according to the application's necessities.

B. UNMANNED AERIAL VEHICLES IN THE ERA OF IOV

UAVs, also known as drones, present a special class of vehicles for 6G. UAVs can be useful for item delivery, photography, search and rescue missions, and construction, etc. Also, in IoV, they can provide service to the ITS, as flying RSUs or relays, see for instance Fig. 4. Typically UAVs are remotely controlled by an operator within LoS, although advanced autonomous flying scenarios are being investigated. For those, reliable communication for a drone is critical. Beyond low-altitude UAVs connectivity, 6G can be also used via airborne relays to provide network, e.g., in disaster areas or difficult terrain. In addition, with proper antenna design, direct 6G connectivity can be provided for commercial aeroplanes flying at altitudes of 10 km and above [30].

UAVs offer some unique challenges to 6G. UAVs can fly at relatively high speed and change altitude, thus providing 3D mobility pattern. On the opposite, base stations are typically optimized for ground coverage. Thus, antenna tilt can cause loss of coverage for UAVs at some spots. Therefore, 6G network design should provide guaranteed signal for typical UAVs' flight altitudes of several hundred feet. When UAVs fly above a city, it can have direct line-of-sight with several base stations. On one hand, it enables high-speed links in millimeter wavebands or even optical band. On the other hand, it could cause severe interference. Advanced antenna techniques such as massive MIMO are needed to mitigate this issue.

Positioning for UAVs is important for safety to prevent collisions with buildings and trees. While global navigation systems (GNSS) provides accurate coordinates in many scenarios, flying in urban environment or indoors is challenging where the satellite signal is weak. For Beyond-Line-Of-Sight operations, just relying on GNSS for navigation is often inadequate. Therefore, additional mechanism such as camera-based place recognition is

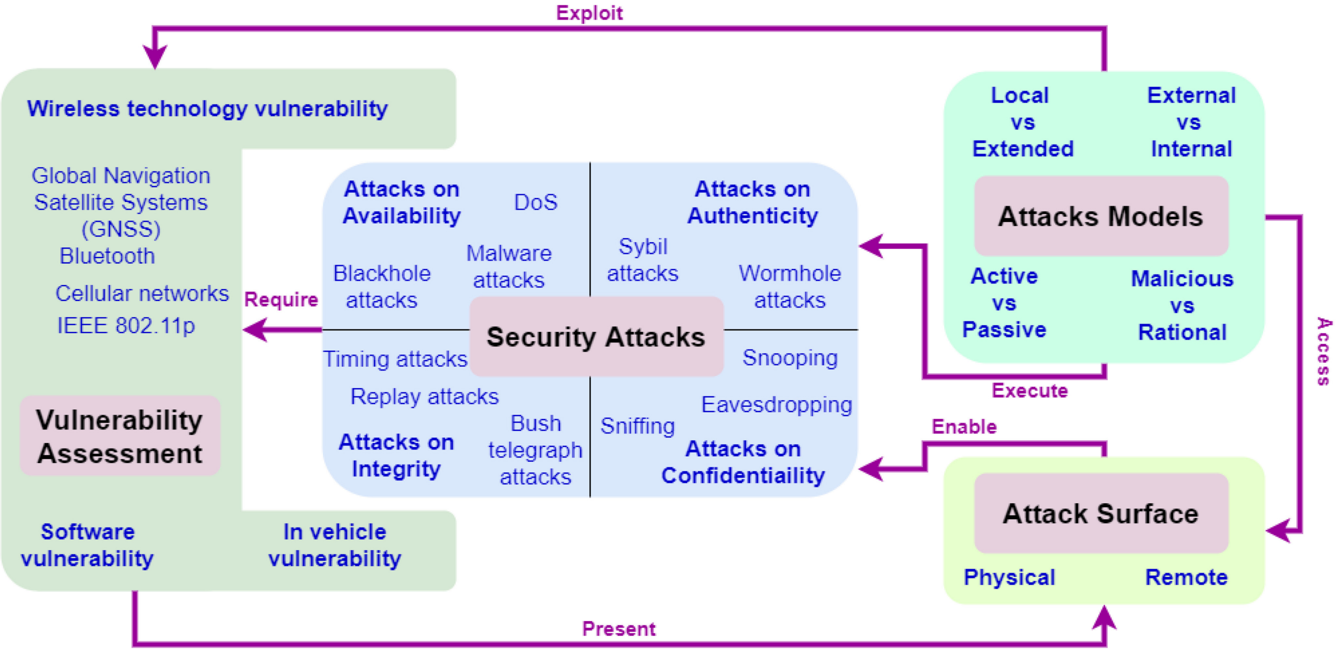


FIGURE 5. IoV Security Threat Taxonomy.

needed. 6G can provide complimentary positioning service with beamforming and triangularing from multiple base stations.

Remote identification for UAVs is a legal requirement nowadays in many countries, including USA and EU. Currently, UAVs broadcast its ID using WiFi or Bluethooth, which can be received, e.g., by Android application on an observer's smartphone. This has limited range and security considerations of possible ID spoofing. With 6G, a drone could store its cryptographic ID and credentials on a embedded SIM card. Furthermore, Internet connectivity via a cellular link also enables network-based ID which could be received by authorities remotely without requiring close proximity to the drone location.

In the following section, Section IV, we discuss the security landscape of IoV in detail.

IV. SECURITY LANDSCAPE FOR IOV

In this section, we provide an overview on the security threats that could hinder the benefits of IoV applications joint with the security requirements of V2X communications for the safe implementation of future IoV.

A. SECURITY THREATS

The fast evolving of IoV may also encounter advanced and more intelligent security attacks that can create serious issues to the entire transportation system and users [31]. In [32], authors provide an extensive survey on security landscape of intelligent transport systems. Similar to their explanation, the security threats related to IoV are becoming more and more critical as human lives can be placed at risk. As a summary, we present the security threat taxonomy in Figure 5. Basically, the attacker models will exploit the vulnerabilities in vehicular systems by accessing physical or remote attack surfaces to execute security attacks. The attacks may create on RSUs or other physical attack surfaces such as vehicular external interfaces OBUs via Electronic Control Units (ECUs) [33].

There can be different attacker models in an IoV system which may intrude from outside or be internal to the system. The local attackers may target only the close-by vehicular systems, whereas the extended attacks may perform attacks with a broader scope, which is irrespective of the locality. The active attackers may inject malicious packets to block the vehicular networks causing denial-of-service (DoS), sybil and blackhole attacks. For instance, with sybil attacks, by falsifying or stealing multiple identities of legitimate users, the attackers may control a fraction of the network. The passive attackers will monitor the network traffic and launch eavesdropping attacks to extract useful information to create future attacks. Malicious attackers may damage the network without considering the further consequences, whereas rational attackers target specific users who can be owner of a vehicle or the passengers.

Security vulnerabilities may occur in the vehicular system itself or with wireless technologies or raise software issues. Security attacks require to have vulnerabilities to be present through the attack surfaces to enable attacks. In IoV, there are many wireless technologies in use including bluetooth, IEEE 802.11p, cellular networks and GNSS. Other than this, in 6G, IoV may also incorporate novel wireless technologies such as visible light communication and quantum communication. Certainly, the security vulnerabilities related to such technologies may also create a direct impact on the IoV

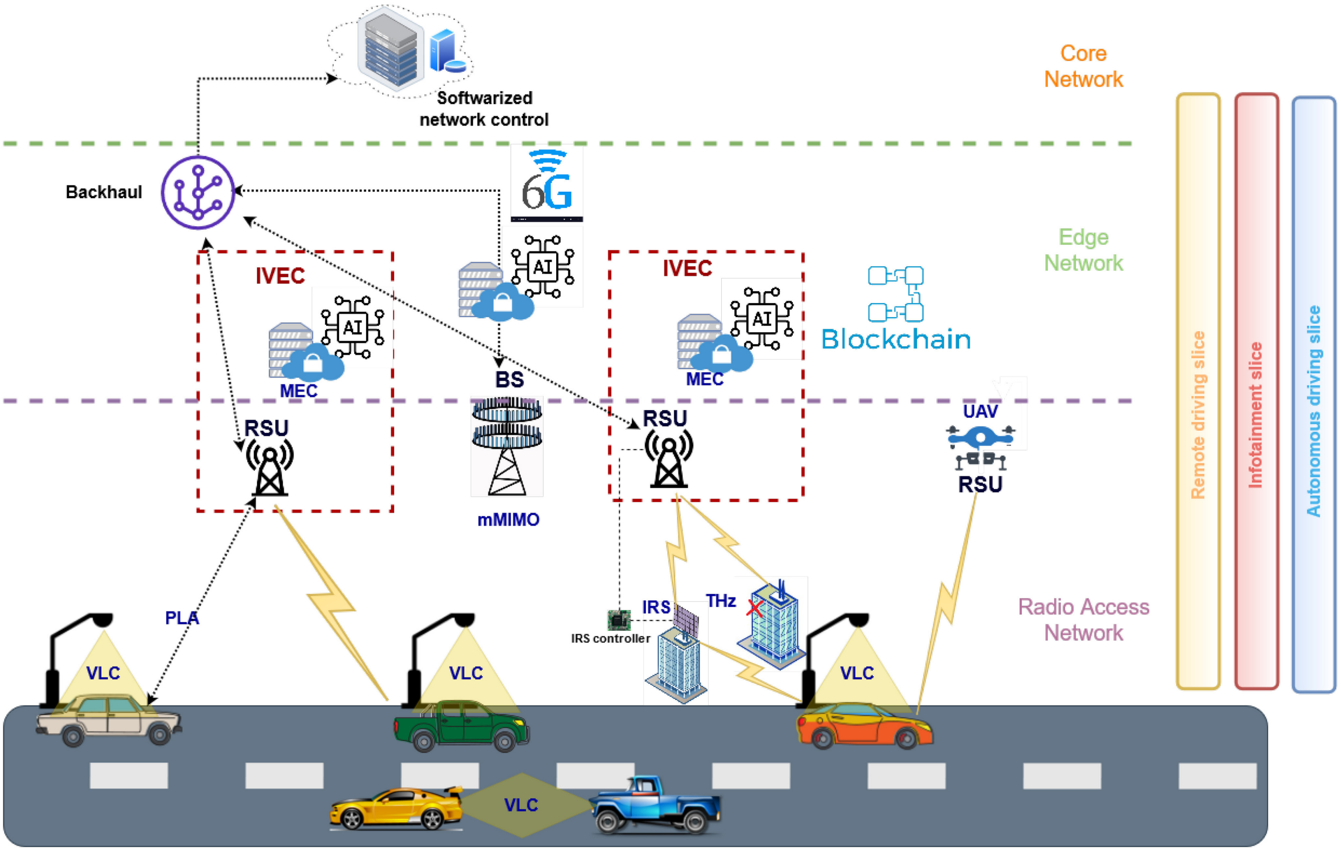


FIGURE 6. 6G-enabled Secure IoV: Interactions among different technologies.

security. In Figure 5, we highlight the most common types of security attacks that can occur in IoV with attacks on availability, authenticity, confidentiality, and integrity.

B. SECURITY REQUIREMENTS

The envisioned ubiquitous connectivity of vehicles in future IoV demands robust security mechanisms to prevent unauthorised access to vehicles and leakage of sensible information once the incidence and impact of security breaches is immense. At the same time, security protocols must be implemented with low communication overhead due to time constraint and low computation complexity, as well as the timeliness of authentication management should be ensured [34], [35]. According to the International Telecommunication Union (ITU) within its Telecommunication Standardization Sector (ITU-T) [36], the security requirements for V2X communication can be described as follows.

Confidentiality: It should not be possible for an unauthorised entity to reveal the messages among vehicles, between vehicles and infrastructure, vehicles and devices, and vehicles and pedestrians. Also, the unauthorised entity shouldn't be able to analyze the identification of a person through personally identifiable information (PII).

Integrity: Messages sent to or from entities in the V2X communication should be protected from unauthorised modification and deletion.

Availability: It should be possible for an entity on the V2X communication to send messages in real-time, thus low-overhead and lightweight security solutions are required.

Non-repudiation: It should not be possible for an entity to deny that it has already sent a message. This requirement can be implemented using digital signatures in vehicular communication system.

Authenticity: OBUs, RSUs, vehicles and nomadic devices should be able to provide proof of being an authorized owner of a legitimate identification. In group communications, the vehicle should be able to prove that is a legitimate member of the group. This requirement is called attribute authentication.

Accountability: It should be possible for an entity to detect and prevent any misbehavior of OBUs or vehicle sensors by checking their data.

Authorisation: It should be defined access control and authorisation for different entities.

V. KEY TECHNOLOGIES FOR SECURE 6G-ENABLED IOV

In the following, it is described 6G key technologies that we consider essential for safeguarding vehicular communications in IoV, which are also illustrated in Fig. 6.

A. NETWORK SOFTWARISATION/VIRTUALISATION

Network softwarisation, the philosophy behind taking network control functions out of the traffic forwarding elements and implementing it in software, has evolved the network landscape towards an agile, robust, and scalable one. Enabling network programmability with application programming interfaces (APIs) through splitting the network control and data planes, and logically centralizing the network control, SDN proved to be the most widely accepted technology enabling network softwarisation. NFV [37], separating applications and services from the hardware and enabling it to be deployed on commercial off-the-shelf (COTS) hardware, has enabled network service and function elasticity, improved innovation, and increased cost efficiency of network and service providers [38]. Therefore, network softwarisation and visualization are highly complementary to each other [39], and the technologies behind each, i.e., SDN and NFV, leverage on each other for full potential. Due to the overreaching importance of the concepts for IoV, software-defined IoV [40], [41] has been prevalent in research lately in this domain.

5G has already paved the way towards IoV with increased base stations densities along with novel access techniques, thus minimizing the chances of congestion, increasing reliability and decreasing latency. However, there still exist the challenges of security in 5G [42], that can be severe in the case of IoV for to apparent reasons. The first and foremost challenge is ensuring the availability (important security dimension recommended by ITU-T) of network/connectivity to a moving car, that can be ensure through the logically-centralized control frameworks provided by SDN to leverage multiple access technologies at the same time, as demonstrated in [43]. Once the network availability is ensured, the global network state and resource visibility provided by SDN can be used to monitor the network and detect anomalies, as evaluated through probabilistic data structures in [44]. The technique employ Count-Min-Sketch (CMS) to locate suspicious nodes from the incoming flow and use bloom filters to verify signatures of suspicious nodes.

Secure softwarized group communications in vehicular networks architecture has been proposed in [45]. The architecture enables secure and dynamic set-up of a group of vehicles where data integrity and confidentiality is ensured, as well as provide secure access and mobility management to the fleet traversing heterogeneous networks. Automated security orchestration and enforcement using NFV and SDN in UAV deployments is demonstrated in [46]. Virtual security functions, working as virtual firewalls, intrusion detection systems (IDS), proxies and authentication, authorisation, and accounting (AAA), are deployed in a MEC architecture developed for UAVs. These frameworks can be used to provide security in future IoVs, for instance in 6G, that will require such zero-touch systems.

Softwarisation and visualization have also their own security challenges, as discussed in [47], [48]. One of the main or pertinent challenges that is faced by both, i.e., DoS and distributed DoS attacks [49] on the centralized entities, such as controller of SDN and hypervisor in NFV platforms, which have pivotal roles in their respective domains. Due to their functions, the traffic towards these entities can be easily recognised, making these visible targets for security attacks, such as DoS, DDoS and other resource exhaustion attacks. Primary security approaches for such points of attraction for malicious actors include devolution of control plane functionalities, and hierarchical architectures with cascade failure-proof security techniques [47].

Network softwarisation, visualization, and cloudification in 5G are driving towards the automation of network and service management in the beyond 5G or 6G architecture, as the next paradigm shift. One good initiation network automation in future 6G networks is the proposed Zero-touch network and Service Management (ZSM) architecture by the European Telecommunication Standardization Institute (ETSI) [50]. The ZSM architecture is formed by modular characteristics using intent-based interfaces, closed-loop operation, and AI/ML techniques to empower full-automation of the intelligent management operations with AI-enabled self-configuration/self-optimisation/self-healing and self-organizing capabilities.

B. NETWORK SLICING

Network slicing is another promising technology in 5G which brings the benefits of providing customized services and logical networks over the shared physical and virtual networking infrastructure. A network slice is defined as a virtual entity that spans across all the networking segments including the core network, backhaul network and radio access network. Network slicing technology also has a close alliance with IoV to fulfil the requirements of ITS. Specially, these sliced network infrastructure will support the diverse use cases in IoV by fulfilling their specifications in terms of resource requirements, latency, security, and QoS [51]. Different network slices can be allocated for specific requirements in IoV, such as mLLMT network slice for automated driving services, FeMBB network slice for entertainment services in IoV, and umMTC network slice for handling large amounts of data in IoV.

Although, network slicing is introduced in 5G as a key enabling technology, its advanced variants will be introduced in the future 6G networks. The slicing technology will move from the connected things in 5G towards the connected intelligence in 6G with the full openness (e.g., deep slicing [52]). As discussed in [53], hyper-specialized slicing will be one such advancement that may allow separate software stacks in slices for different functional treatment of flows. In IoV related network slices, further dissection of RAN functions into modular micro-service may improve the flexibility in slice-specific RAN implementation. For instance, one can expect slice specializations for a video service slice for in-vehicle infotainment by incorporating specific video optimization micro-services. Moreover, the novelties and innovative advancements in orchestration, adaptation to different hardware platforms and service management should be considered in such hyper-specialized network slices in

6G. Furthermore, in the vehicular networks, intelligent slice selection algorithms can be also incorporated to allow flexible radio access network slicing, automated selection of edge caching, and content delivery.

There are many forms of security challenges in network slicing technology [54]. The security in network life cycle includes threats such impersonate attacks, identity theft attacks, DoS/DDoS attacks, data modification, and unauthorised access in the network slice instances (NSI). Inter-slice security considers the security issues between slices. One minor data leakage between slices may cause serious issues in data security and privacy violation matters. Therefore, strong slice isolation between NSIs is a key security requirement. Particularly, slice isolation should be considered in hypervisors, operating systems, network hardware, network operators, and APIs.

C. INTELLIGENT VEHICULAR EDGE COMPUTING

MEC has been included in 5G standardization in order to provide cloud-computing capabilities at the edge of the mobile network, within RAN and closer to mobile subscribers. This introduction was driven by the increasing demands on high-bandwidth and low-latency of 5G-based applications, introduction of new wireless technologies, and stringent requirements of QoS. Towards 6G, MEC provides a great number of opportunities while facing several challenges in terms of distributed resource management, reliability, mobility, network integration and application portability, coexistence of heterogeneous traffic, security and privacy [55]

Particularly, IoV applications will be part of a data-driven system with an extremely high amount of data being transferred over V2X communications. This unprecedented amount of data will overburden communication and computing infrastructures. At the same time, IoV applications are highly sensitive to latency by requiring to react to real-time traffic conditions, which urge for significant computing capabilities. In this regard, the service provided by cloud computing platforms will not be enough for the wide implementation of IoV, thus real-time processing and reliability can be compromised. In this context, vehicular edge computing (VEC), consisting of RSUs and MEC servers, has emerged to overcome the limitations of on-board computing and the excessive latency in cloud computing by delivering cloud services directly from the vehicular network edge. The processing of data at the edge can bring several advantages as saving in bandwidth use, security and privacy protection, low latency suitable for delay-sensitive safety applications, thus enabling new applications in IoV, such as driver identification, real-time traffic estimation, and public safety [56].

In the 6G era, the AI empowered VEC or Intelligent VEC (IVEC) will introduce the use of machine learning techniques and data analytics at edge devices in order to perform tasks with low latency, high energy efficiency, and reduced bandwidth consumption [57]. However, data in IoV applications could be in most cases privacy-sensitive; for instance, location and orientation, images of the interior of the vehicle captured by the on-board camera, measurements from the Light Detection and Ranging (LiDAR) and ultrasonic sensors are data that are useful to provide intelligent services and preventive alerts, but can also expose confidential information [58]. To prevent this, federated learning (FL), a decentralized learning algorithm, has been considered in AI-empowered VEC schemes for some privacy-sensitive tasks of IoV, once it allows vehicles to share only partial information. Indeed in [59], it is proposed an efficient and secure scheme based on deep Q-network and FL to share data in a collaborative manner in a vehicular edge network.

Moreover, IVEC can benefit from the use of blockchain for improving transparency in VEC resource management and allowing edge consumers to have a computation verification option, thus overcoming problems such as fake computation feedback and unfair resource allocation.

D. THE ROLE OF AI/ML

AI and ML have been increasingly finding their space as resource efficiency, reliability, and robustness are becoming more stringent in 5G networks, and the introduction of intelligent network operations have become imperative. The increasing user and service dependency on communication networks complicates even further the provisioning of new services within existing resources and its management. Thus, communication networks have embraced AI and ML to meet the growing and diverse requirements of future services [60]. 6G is expected to be highly heterogeneous, dynamic, and densely deployed, with stringent QoS requirements. Therefore, to deal with this complex network and realise a fully intelligent network orchestration and management, AI and ML will domain 6G in all phases, thus enabling a network with the capabilities of self-optimization, self-configuration, and self-healing [61].

Particularly, the IoV eco-system presents challenges in terms of meeting the requirements of timely service provisioning and ensuring security during movements. Due to its capability to predict real-time or even future service needs, machine learning will play a critical role on ensuring security of IoV. Therefore, there exist interesting research work in this direction.

In IoV, the BSM (or CAM) containing location, speed, acceleration, and direction information is broadcasted every 100 ms beyond the local sensors of a vehicle. Such information can be manipulated to affect road safety and efficiency, for instance through Sybil attacks [62]. An ML-based detection model for IoV to mitigate such attacks has been proposed in [63]. The proposed technique overcome the limitations in traditional approaches that are reactive in nature and are dependent on availability of predefined rules and human intervention. The data-centric technique proposed in [63] uses supervised learning techniques [64] integrated with plausibility checks to detect and classify misbehavior by using information collected from neighboring vehicles.

However, there still exist the challenges of data manipulation based vulnerabilities, for instance, foul data supplied by malicious nodes to fool ML models.

To mitigate challenges due to shortcomings arising from the availability and complexity of data for ML, transfer learning based approaches are proposed for intrusion detection schemes in IoV [65]. The main technique employed to alleviate the challenges associated with labeling and corruption of data is a localized update scheme that obtains pseudo labels of unlabeled data along with multiple rounds of transfer learning. The technique proposed in [65] also enables vehicles to train a model in an independent and local manner, thus responding to new attacks on one hand, and updating the IoV cloud to label new attack data and release a new detection model, on the other hand.

Along with all benefits, AI/ML will have its own challenges of security, latency, and resource requirements in critical communications, as discussed in [66], that require further investigation to be efficiently utilized in IoV. Moreover, AI/ML can have security challenges in the underlying communication infrastructure that enables vehicles to connect or share data [67]. Such security vulnerabilities can cause disruptions and unavailability of the communication infrastructure or become means for leakage of sensitive information in IoV. Moreover, authors in [68] demonstrate how ML models can be fooled to launch attacks against autonomous vehicles. The adversarial ML creates attacks that can be hardly detected by classical ML classifiers. Such security weaknesses and vulnerabilities require research work to first secure the ML techniques that are the main enablers of autonomy or self-decisions in IoVs.

Moreover, centralized AI/ML approaches present serious drawbacks that conflicts with the stringent requirements of IoV, namely high bandwidth usage, high latency, and privacy vulnerabilities as sensitive information can be leaked while transferring data to central locations. Therefore, FL has emerged as an interesting distributed approach that facilitates distributed collaborative learning, and it improves learning accuracy, communication efficiency and allows privacy preservation [69]. However, FL would not be enough to provide privacy-guarantee as model parameters exchanged between parties still can expose sensitive information, which can be exploited in some privacy attacks. Thus, privacy-preserving techniques should be further explored in the context of federated learning to protect sensitive information in IoV [70].

E. THE ROLE OF BLOCKCHAIN

Blockchain is a distributed ledger technology (DLT) that allows a platform to perform trusted tasks and transactions in an untrusted environment by dispensing a trusted entity [71]. In 5G and beyond, blockchain and similar DLTs represent the most important enablers to address various problems related to security, automation, interoperability, and resource management in a distributed and decentralized manner, thus enabling various services at the front-haul, edge and the core [72]. Towards 6G, blockchain will be critical to facilitate the evolution of these 5G services to comply with 6G requirements [6].

Particularly, blockchain can provide IoV applications of decentralization, security, non tampering, traceability, immutability, and automation. Integrating blockchain into the IoV offers security and prevention of data manipulations by its ability to guarantee the data immutability [15], [73], [74]. For instance, in [73], a blockchain-based approach is used for providing network security for a containerized edge computing platform for IoV, which allows vehicles to offload their tasks remotely. Then, transactions generated by distributed parties are tied up in blocks and annexed to the blockchain. Also, participants periodically verify the transactions in order to reward or punish the cooperative or malicious behavior of parties. Likewise, the authors in [74] considered the Ethereum platform to design an authentication protocol that demands minimum storage and low computational overhead while ensuring confidentiality, integrity, and privacy.

In the IoV, neighboring vehicles are usually strangers and untrustworthy due to the high mobility and variability, thus malicious vehicles can endanger traffic safety or efficiency of the ITS. In this regard, trust management systems are of paramount importance to enable an effective way to evaluate trustworthiness in the IoV nodes. However, centralized systems cannot always satisfy the rigorous QoS demands of IoV, thus decentralized solutions are attractive in order to allow trust management tasks being conducted in vehicles or RSUs, which may reduce interactions and satisfy QoS requirements. Thus, blockchain is an interesting solution as in a decentralized blockchain-based network, nodes are not required to trust other nodes, as each participating node can keep a copy of the ledger, then if the ledger of a member is corrupted, it will be rejected by the majority of the members in the network, thus facilitating trust establishment among nodes [75]. For instance, in [76] was proposed a blockchain-based trust management scheme using smart contracts at the edge, i.e., at the RSUs plane of IoV, where RSUs at the edge collaboratively maintain reliable and consistent vehicle trust values across the network. Also, in [77], a decentralized trusted data sharing management framework was proposed for edge computing-based IoV networks by relying on a consortium blockchain and smart contracts in order to provide secure data sharing environments among vehicles based on the generation of reputation ratings. Therein, an incentive mechanism was designed based on the vehicle's contribution that aims to encourage them to participate in trusted data sharing activities.

By considering that some vehicles can introduce false information in IoV applications in order to disrupt the traffic order, a blockchain-based vehicle trust management scheme is proposed in [78]. Therein, the validity of the sent message is evaluated through blockchain technology. According to vehicle's information score and a reward and punishment mechanism, the base station deducts the trust value of a vehicle that releases false information and rewards the trust value of a vehicle that releases correct information. Meanwhile, the BS releases accident-related blocks to ensure the safe transmission of information and reduce the waiting time of the vehicle, thus alleviating the traffic congestion.

F. INTELLIGENT REFLECTING SURFACES

In traditional wireless systems, the radio environment is usually assumed uncontrollable and often cannot be customized based on the propagation conditions. In the context of IoV, the most harmful wireless channel is undoubtedly the fast-fading (i.e., rapid fluctuations of the received signal's phase and amplitude over time), caused by the Doppler spread effect, which arises in response to the vehicle's high mobility [79]. As a result, the achievable data rate of V2X communications can be severely deteriorated, so that this is a primordial concern for IoV communications. 5G NR-based V2X releases are already working on including novel transmission schemes in order to reach robust data rates. Nevertheless, such techniques will face spectral efficiency issues while requiring intricate signal processing methods to be performed on the vehicle side [27].

Recently, a revolutionary technology named IRS has attracted full attention by its great potential to improve coverage, security, and spectral/energy-efficiency of upcoming wireless networks by controlling the propagation environment. An IRS is a man-made metasurface planar array comprising a larger number of nearly passive[1] reflecting antennas. Each element of IRS can be dynamically programmed through an external controller to tune the amplitude, phase, frequency, and even polarization of the impinging signals in order to overcome the hazardous effects of the wireless channel [80]. Based on this operation, IRS will likely allow physical layer security (PLS) finally flourish as a defence method for providing security to wireless networks by complementing cryptography-based algorithms.

In the current state-of-the-art, some IRS-based PLS techniques have been investigated to secure IoV applications. For instance, the PLS performance of the VANET IRS-relay model in terms of average secrecy capacity and secrecy outage probability was studied in [81], [82]. Later, a fair comparison of secrecy behavior between V2I IRS-aided communications and V2I traditional relying systems (e.g., decode-and-forward and amplify-and-forward schemes) was explored in [83]. Then, in [84], the authors explored the SOP of V2V systems employing sophisticated special functions such as Meijer-G and Fox-H. In such work, a quasi-static mobility vehicular scenario is considered; thus, there are no insights about high-speed V2X communications. Furthermore, in all aforementioned works, due to the complex nature of the IRS end-to-end channel, pivotal aspects into the IRS's channel characterization (e.g., spatial correlation, phase-shift noise, Doppler effect, electromagnetic interference) have not been sufficiently explored for securing IRS-assisted vehicular systems.

G. PHYSICAL LAYER AUTHENTICATION AND KEY GENERATION

Efficient and lightweight authentication methods are of paramount importance for avoiding spoofing and impersonation attacks, thus enabling the commercial deployment of IoV applications. Traditionally, V2X communications use authentication schemes that are based on public key infrastructure (PKI), which require the transmission of certificates and signatures for sending safety-related information. Those transmissions lead to huge signalling overheads in large-scale vehicle networks, which is specially critical under a traffic congestion scenario. Thus, reducing the overhead due to certificates and signatures is essential for more efficient V2X communication.

To circumvent this problem, physical layer authentication (PLA) emerge as a viable solution to provide secure communications with low latency and light signalling overhead, compatible with IoV applications, by relying on the unique channel properties or inherent attributes of communication devices to perform the authentication of vehicles [85], [86]. Based on this, [87] proposed a V2X PLA scheme that uses a Kalman filter to refine the iterative model and threshold model in the authentication mode. The solution in [87] can effectively carry out identity authentication in IoV, thus providing a high-security level with low overhead while reducing the consumption of communication resources for security purposes.

The researchers in [88] proposed a physical layer cover-free coding-based secure wireless pilot authentication (SWPA) protocol for multi-antenna orthogonal frequency division multiplexed (OFDM)-based communications to prevent data-origin authenticity attacks in IoV communications networks. This protocol encodes and conveys vehicle pilot signals into different sub-carrier activation patterns on the time-frequency domain by using a cover-free coding, which helps to ensure a successful separation of pilots. In [89], an adaptive PLA method is proposed by relying on a kernel-based machine learning technique to track multiple physical attributes in order to achieve a more robust and reliable authentication in dynamic time-varying scenarios.

On the other hand, physical layer key (PLK) generation, which exploits wireless channel reciprocity and randomness to generate secure keys, provides a feasible solution to protect IoV applications due to its lightweight, flexible, and dynamic implementation. In this sense, a PLK generation scheme is proposed in [90] for V2X communications based on Long Range (LoRa) protocol that utilizes the received signal strength indicator to generate secure keys. Therein, the authors proposed a multi-bit quantization algorithm with an improved cascade key agreement protocol in order to generate secure binary bit keys. From experiments in real outdoor scenarios, it was proved that the scheme achieved an improved key generation rate while avoiding information leakage during transmission.

Also, in [91] a PLK generation algorithm for IoV applications was proposed by considering a channel

[1] Passive means that IRS reflects radio waves upon it, without the need for energy-consuming RF chains (e.g., signal amplification process).

response quantization method that incorporates all V2X channel attributes that can contribute to variations on time, such as three-dimensional scattering and mobility of scatterers. The authors also propose an additional functionality, the perturbe-observe, that enables the adaptation of the algorithm for channel responses that are not reciprocal. The algorithm can successfully maximize the key bit generation rate, the secret-bit generation rate, and the key entropy, and, at the same time, the key bit mismatch rate is minimized.

H. CELL-FREE MASSIVE MIMO

The use of smaller cells (e.g., picocells and femtocells) is an efficient way to increase the next-generation network capacity, but, at the same time, this trend also leads to increasing inter-cell interference. Thus, for further network denazification, small cells may even reduce rather than increase the network capacity [92]. In this regard, the potential 6G-enabling network architectures are envisioned to overcome the shortcomings of 5G concerning the low service quality for users at the cell edges or experiencing hard inter-cell interference. One of the emerging 6G solutions to circunvent this issue is to utilize a fully decentralized massive MIMO scheme so-called cell-free massive MIMO (mMIMO).

Unlike traditional cell structures, cell-free mMIMO comprises a huge number of distributed access points (APs) that cooperate with each other to serve a much smaller number of users instead of creating autonomous centralized cells [92]. Specifically, each distributed AP is connected via a fronthaul link to a central processing unit (CPU), which is in charge for both the AP cooperation and the AP's baseband signal processing. The CPUs are connected either directly or via the core network. The user can be served in the same time-frequency resource by a subset of APs connected to different CPUs. This architecture leads to a user-centric cellular network approach that is able to solve the inter-cell interference concerns and QoS variations inherent of conventional cellular networks [93].

Owing to its promising features, cell-free mMIMO enables truly ubiquitous communications, where wireless applications (e.g., control of autonomous vehicles, high-rate navigation) will experience uniform data rate quality regardless of the user's location in the geographical coverage area, eliminating the well-known handover problem (i.e., no cell boundaries exist) [94].

On the other hand, to be in line with the vision of the future 6G era, the IoV needs to take advantage of key revolutionary technologies to ensure very high QoS in heterogeneous ecosystems. Thus, the outstanding cell-free mMIMO operating scheme facilitates the exploitation of advanced driving use cases by providing fast signal processing (due to the AP coordination) in high-speed scenarios with excellent coverage areas without cell edges or cells [95]. However, one of the most critical aspects of cell-free mMIMO-assisted V2X communications is related to information security. This fact is because IoV will be designed to support a plethora of driving applications that coexist in a wireless medium, which is sensitive to eavesdropping.

A deep-in inspection of cell-free mMIMO-related literature in V2X communications reveals that research activities on information security concerns on this direction have not yet started to date. Currently, as a first research stage, the secrecy performance on user-centric cell-free mMIMO networks for static or low-mobility mobile users has been investigated in [96], [97], [98]. As forward-looking research direction, AI is envisioned to alleviate security issues, congested spectrum, and high QoS requirements for 6G IoV applications.

I. TERAHERTZ LINKS AND VLC

Terahertz (THz) communications have emerged as an enabling technology to provide low-latency communication and extremely high throughput to 6G mobile networks, thus favoring the emergence of new applications in the context of IoV. Besides, THz transmissions present a high-resolution time-domain, which is crucial for allowing high-resolution sensing technology and ultra-accurate precision positioning services. These Thz features are important, for instance, in remote sensing and autonomous driving.

However, providing security at network and application layers becomes computationally expensive in THz wireless links that operate under rigorous energy and latency requirements. Even though the increased directionality of THz transmissions presents a more challenging environment for eavesdroppers, thus being considered more secure, there is still the chance for an eavesdropper of intercepting signals in line-of-sight transmissions. Therefore, PLS techniques, that exploit the physical properties of wireless channels to incorporate security features [99], [100], have been listed as an important solution for THz links [101], [102].

For instance, in [101], PLS is explored in sub-THz wireless links by relying on spatio-temporal array architectures, which allow enforcing spectral aliasing, loss of information, and constellation scrambling at undesired directions, thus mitigating eavesdropping attacks. Moreover, by considering that a potential eavesdropper can place passive objects in the beam in order to scatter some of the transmission towards a convenient direction to perform successful eavesdropping, the work in [101] have proposed a countermeasure for this eavesdropping technique relying on the characterization of the backscatter of the channel, which allows to detect some eavesdroppers. Therein, the authors highlighted the need for improved PLS techniques in THz wireless networks.

Alongside mobile communications based on RF, optical wireless communications (OWCs) will be extensively used in the timeframe of 6G. VLC is the most promising frequency spectrum because of the technological advancement and extensive use of light-emitting diodes (LEDs). The OWC in the visible spectrum (380 to 740 nanometers) is generally known as VLC. For short-range communication distances (up to a few meters), VLC technology offers unique advantages over its RF-based counterpart. Particularly, communication security and privacy are some of the major benefits of VLC as the transmissions cannot penetrate walls and other opaque obstructions, thus indoor applications are the main scope for VLC. However, the use of VLC in outdoor environments is attractive for IoV applications as many security attacks to vehicular networks based on omnidirectional RF communications can be mitigated by using VLC [103]. Indeed, hybrid RF/VLC schemes can provide of reliability and security to IoV applications [104].

J. BACKSCATTER COMMUNICATIONS

A typical backscatter communication (BC) system relies on a backscatter transmitter (also well-known as a tag), a legacy receiver, and a carrier emitter (e.g., radio-frequency-RF source). In that setup, the backscatter transmitter modulates and reflects the received signal from the emitter to neighboring receivers. For a smooth operation of BC, the legacy receiver should be designed in such a form that it can decode the modulated signal from the backscatter transmitter [105]. Based on the operation schemes, the backscatter network can be categorized into passive and semi-passive systems. In the former, the backscatter device works on the harvested energy from the incident RF signals, so the collected energy is used to activate the device. In the latter, the backscatter device is equipped with an internal power supply. This configuration generally makes it possible to improve the system's reliability compared to the passive counterpart strategy.

On the other hand, based on the architectures, BC can be classified into three major types, i.e., monostatic, bistatic, and ambient (see [105] for a nice discussion on this topic). Owing to the promising benefits of the BC in terms of energy efficiency, reliability, and security, a myriad of potential use cases have been identified. For instance, BC for healthcare networks (e.g., health motoring and emergency evaluation) [106], BC to energize IoT Devices [107], BC for enabling ultra-massive Connectivity in emerging wireless networks [108], BC for human activity recognition and transportation, [109], and secure multi-antenna radio-frequency identification (RFID) in IoT [110], to name a few.

Regarding emerging V2X networks, some challenges have to be overcome in the coming years for enabling secure backscatter-assisted IoV networks to be a reality. Specifically, fast time-varying channels, fast handover, and large penetration losses for wireless signals are pivotal aspects to be tackled on secure high-speed rails. Furthermore, it is necessary to incorporate learning capabilities in backscatter devices to evolve the BC-aided V2X in a secure platform of intelligent vehicles operating in a self-organizing way. These challenges of BC-assisted IoV have raised great interest recently.

In [111], the authors designed both the UAV's trajectory and the battery-less backscatter devices' scheduling for achieving a secure UAV-aided BC system in the existence of multiple eavesdroppers. A deep-in performance secrecy analysis was addressed in [112] for a BC between two smart cars in VANETs. Concerning learning-based resource allocation in BC-assisted V2X, in [113], the authors introduced a resource allocation and user association scheme for large-scale heterogeneous BC-aided V2X systems. In [114], the authors investigated the integration of ambient BC with Non-Orthogonal Multiple Access (NOMA) to support low-powered IoV in 6G transportation systems. Therein, a novel energy-efficient resource allocation for ambient BC-enabled NOMA IoV system under successive interference cancelation was proposed. Finally, motivated by BC's low-powered and spectral-efficient benefits, the authors in [115] investigated a NOMA-enabled backscatter-based V2X system. Therein, a novel scenario was proposed, where tags acting as ultra-low-powered safety sensors communicate with vehicles using the same spectrum resources.

K. END-TO-END SECURITY

End-to-end security, including data encryption and authentication, is ideal for providing confidentiality and privacy from the user's perspective. In principle, end-to-end security mechanisms are agnostic to the used link layer, such as 6G. At the network layer, end-to-end security can be provided by IPsec with the help of Host Identity Protocol (HIP) for the key exchange. At the transport layer, SSL-based protection is available for TCP as well as recently for UDP traffic with DTLS.

From 6G viewpoint, end-to-end security could complicate implementation of certain services. For example, caching, content adaptation, QoS, virus and intruder detection, as well as multicast services become problematic. Furthermore, legal call and data interception cannot be implemented within the operator's network and would require cooperation from the user device, such as a smartphone.

Finally, Table 3 summaries the 6G key technologies described above for secure IoV.

VI. PRIVACY ISSUES IN IOV COMMUNICATIONS

In addition to the security, privacy is yet another very important topic to discuss within IoV environments. One common privacy issue arising with V2X communication networks is due to the generation and collection of large amounts of data from peer vehicles and transmitting those data to the edge or central clouds [116]. Therefore, location and identity should be critically considered in such a way that an attacker cannot link the data with the users and For instance, digital number plates can be used by vehicles that are broadcast by a crowd service to read each others number plates with camera and share information about dangerously driven vehicles.

The key challenges in privacy preservation of 6G over 5G networks are due to the availability of smart agents with supercomputing powers and the exponential growth of gigantic networks with smart applications that connect things and humans [52]. Typically, when the information is shared among multiple vehicles, it should preserve data privacy. Particularly, with the realization of intelligent networks for

TABLE 3. Summary of 6G key technologies for secure IoV.

Key technology	Main security threats	Potential solutions
Network softwarisation	DoS attacks, denying availability and access, hijacking attacks	Distribution of control functions, strong authentication and authorisation procedures
Network slicing	DDoS attacks, side channel attacks, inject traffic into interfaces, network slice manager impersonate attacks	service oriented authentication, secure inter-slice communication, slice isolation, policy based security
IVEC	Confidentiality attacks, privacy leakages, fake computation feedback, DDoS attacks, spoofing attacks	FL-based schemes, blockchain-based mechanisms
AI/ML	Model and data corruption attacks, privacy challenges	Integrity verification techniques, localised and distributed AI/ML techniques
Blockchain	Consensus attacks, privacy leakages, sybil attacks, blockchain peer flooding attack	Private or consortium blockchain, trust/reputation management mechanisms, privacy-preserving schemes
IRS	Passive eavesdropping and active attacks at the physical layer level	Deep learning algorithms for IRS's channel estimation and passive beamforming design, friendly interference strategies and cooperative jamming schemes
PLA	Spoofing or replying attacks, impersonation and substitution attacks	Robust learning-based multi-attribute PLA schemes. Novel channel-based quantisation methods.
Cell-free mMIMO	Eavesdropping, origin authenticity, message integrity and privacy-preservation	FL approaches based on data availability and partition, and aggregation algorithms
THz and VLC	Eavesdropping, privacy attacks, jamming	Improved PLS techniques. Hybrid VLC/RF techniques
End-to-end Security	Key leakage, side-channel attacks, cryptoanalysis, quantum computing	Crypto agility, randomisation, post-quantum cryptography
BCs	Passive eavesdropping attacks at the physical layer level, and information leakage	Properly RFID protocol designs using learning algorithms subject to power limitations in the backscatters devices

IoV, the ethical decision making is very important for privacy sensitive data handling. Moreover, 6G networks may need more accurate and efficient privacy protection mechanisms with reduced communication overhead. This implies that 6G requires to ensure efficient knowledge sharing and privacy protection in high speed and highly dense networks. The well-known 5G technologies such as network slicing and blockchain can be further utilized to enhance privacy in V2X communication networks which are future intelligent transport systems in 6G [15]. Moreover, 6G will bring the automation of telco clouds that allow migrating workloads to the cloud with the shared infrastructure and may worsen the privacy threats in 5G. In addition to the perfect privacy enhancing technologies in technical terms, 6G need to have strong coordination with policies and laws.

FL is already getting a lot of attention as a promising tool for privacy enabled machine learning in many fields including IoV [117], [118]. FL based model training will allow protecting the privacy of training data locally in the vehicles. However, it is important to keep the uninterrupted and reliable communication links to support the continuous exchange of model parameters when FL is applied among IoV components. Zhou *et al.* present a two-layer FL model taking the advantage of distributed end-edge cloud architecture in 6G supported IoV [117]. Their proposed two-layer FL model is based on convolutional neural network that uses global and local context of vehicles and RSUs to perform heterogenous and hierarchical model selection and the aggregation at the cloud and edge levels.

Spacial crowdsourcing (SC) applications are widely applied in IoV scenarios to support traffic or road monitoring, real time navigation, maps, parking, and location based services. However, since the location is reported in SP tasks, there can be serious issues with location privacy. Using a trusted-third-party (TTP) to manage the location information is not a very pragmatic approach to cater different privacy demand of the users. In [119], the authors introduce a blockchain based decentralized location privacy-preserving SC for IoVs. They exploit circle-based location verification and homomorphic encryption to assure the confidentiality of the location policy with multi-level privacy preservation for workers' location.

The security level can be significantly enhanced with the introduction of strong authentication protocol for the users of V2X communication networks. In [120], vehicles are granted anonymous pseudo-identities to protect the conditional privacy of the vehicles. In IoV environments, the announcement messages are meant for transmitting data by the vehicles through wireless channels to announce their condition. When an attacker reveals those transmitting data with the vehicle identities, it may create serious security and privacy issues. In [121], the anonymity of vehicles is achieved by an identity-based group signature scheme which introduces a privacy-preserving announcement protocol. Other than privacy, their scheme has a blockchain-based trust management system for IoV.

VII. STANDARDIZATION ACTIVITIES

Standardization bodies and their workgroups involved in V2X include International Organization for Standardization (ISO) TC 204, European Committee for Standardization (CEN) TC 278, Society of Automotive Engineers (SAE)

V2X, ETSI, ITS, and Internet Engineering Task Force (IETF) IPWAVE. An overview of standardization with a focus on security aspects of V2X is given in [122].

ETSI ITS finished recently its first release of V2X standards for basic safety use cases, involving CAM, DENM, IVIM, SPAT and MAP messages, and started working on the second release involving more complex use cases including Cooperative Perception Message (CPM) and Manoeuvre Coordination Message (MCM). The European Commission has been active in stimulating research, standardization and deployment of V2X [123]. The EU Rolling Plan for standardization [124] identified as main security standardization aspects misbehavior detection and revocation of trust for ITS stations as well as standards for protocols and profiles for credential requests.

Regarding security and privacy, in Europe the European Commission has set up the European C-ITS Security Credential Management System EU (EU CCMS). The EU certificate policy is based on PKI, which is at its highest level composed of a set of root Certificate Authorities, whose certificates are included in an European Certificate Trusted List (ECTL), and managed by a Trust List Manager (TLM) [125]. Two types of certificates are exchanged with end-devices: an Enrolment Certificate, which is programmed into the end-device, and commonly changing Authorisation Tickets. In order to assure privacy of end-users, Authorisation Tickets and all other vehicle identifiers included in the V2X messages should change at regular time intervals. The EU CCMS went operational in 2020 and will be fully operational in 2023.

In ITS stations, which exchange V2X messages, A Hardware Secure Module (HMS) takes care of secure storage of credential data and provides cryptographic services. All ITS stations have to be certified according to a Common Criteria Protection Profile. At the moment of writing, protection profiles have been developed for the V2X HSM [126] and for a road works warning gateway [127]. Current protection profiles have been developed for ITS-G5 communications, and will have to take 6G requirements into account. Future potential developments include new and hybrid processing units, hardware acceleration and accelerated abstraction layer [128]. PKI solutions would also evolve to more decentralized architectures to maintain scalability [129].

Currently, ETSI V2X messages are signed at the GeoNet layer using IEEE1609.2. When transmitting V2X messages over IP, the sessions are also secured using TLS, which uses X.509 certificates [130]. Hence, in current specifications, messages sent over IP have 2 certificates. The new ISO/TS 21177 allows to secure sessions with only a single certificate, through the use of the amended TLS 1.3 with IEEE 1609.2 certificates (RFC8902) [131].

With respect to misbehavior detection, the ETSI report TR 103460 [132] investigates the needs for standardization. A Misbehavior Authority, dealing with detection of misbehavior, collection of data and mitigating actions will be key to misbehavior management, and is described in ETSI TS 102 940 [133].

VIII. CONCLUDING REMARKS

A. LESSONS LEARNED

In this paper, we reviewed aspects related to security and privacy on our vision for 6G-based IoV. Herein, we summaries the lessons learned by this review.

In regards to softwarisation, the emphasis is largely on networking functions. However, security-by-design, which is the most important requirement, needs softwarizing security functions along the networking functions with NFV. Such softwarisation will enable mobility of security functions. Therefore, an emphasis is needed on security function softwarisation that will leverage visualization of network resource to be dynamically deployed.

The introduction of network slicing in the 5G era will continuously evolve in the 6G domain to assure user and use case specific services and network/resource requirements. When the IoV in 6G era needs to enable the automation of network slicing technology it needs to tackle many security and privacy challenges with respect to time critical responsiveness and high sensitive data handling.

Even though distributed AI/ML has been heavily researched for V2X and IoV, security challenges arising from the deployment of AI/ML has received little attention. One of the most pertinent challenges, i.e., data corruption, can easily misguide the learning models. Yet little research is dedicated to data integrity verification. In a nutshell, most of the research is following the convention of using AI/ML for improving security, while AI/ML has also been demonstrated to be successful in corrupting or misguiding learning models.

With the dominant presence of AI/ML processes in 6G networks, relying on IVEC is of paramount importance to reduce latency and improving quality of service (QoS) in IoV applications. However, there are security aspects that should be addressed to provide protection for the growing number of vehicular edge networks, where a major risk falls on the privacy of the user's sensible information.

The integration of blockchain brings novel opportunities for, among other aspects, enhancing security and trust in IoV applications. However, there are some challenges ahead to be solved in order to have the whole benefit of this integration. For instance, scalability, latency, heterogeneity of data collected from IoV devices, storage burden, and energy efficiency are aspects that should be considered for the design of blockchain-based IoV solutions, as most of vehicular infrastructure is resource-constrained. Lightweight solutions should be developed for efficient blockchain-based IoV applications.

IRS technology is still immature and requires a lot of effort from researchers to harness the enormous potential of intelligent radio environments. Undoubtedly, various advanced V2X applications in the 6G era can be realized with the help of revolutionary IRS technology. However, some IRS

TABLE 4. **Research directions.**

Key technology	Research questions	Research directions
Network softwarisation	What is the potential of network softwarisation for improving IoV security?	The main potential lies in softwarizing network and security functions to enable mobility of such functions at run-time whenever the need arises. Further research is needed to investigate the possibility, challenges and benefits of security functions as software agents can be as mobile as the vehicles.
Network slicing	What are the possibilities of advancing network slicing technology in the IoV and ubiquitous intelligence with AI?	Integrate AI with the network slicing such as AI-assisted network slicing for management purposes and in the different phases of end-to-end network slice life cycle. Introduce AI-based techniques for slice instance construction, resource management, intelligent security management, and improve QoS in V2X communication [134].
IVEC	How to preserve privacy in IVEC?	Develop new privacy-preserving for content and context protection protocols for edge computation offload. For instance, novel architectures could be designed by leveraging on ontology to perform automatic processing without disclosing sensitive information at the edge [135].
AI/ML	How can AI/ML improve security of IoV and what security challenges can the use of AI/ML create?	Since existing AI/ML techniques are mostly centralised in nature, distributed AI/ML beyond the edge will be required for IoV. Vehicles carry on-board computers, so that AI is performed locally, thus synchronising AI/ML with the network requires further research. Furthermore, the potential security challenges arising from the use of AI/ML in IoV must be investigated, in contrast to the current tradition of using AI/ML to improve existing security techniques.
Blockchain	How to ensure that blockchain-based solutions are suitable for the resource and latency constrained scenarios of IoV?	More research is needed in order to use blockchain as a security solution in the IoV, where some nodes may present limited computing and storage capabilities. Also, investigating improvements on blockchain operation suitable for real-time applications is imperative as the validation of transactions can be a time-consuming task. Throughput, latency, security, and decentralisation of blockchains do not scale simultaneously with the number of nodes in the network, thus error correcting codes were introduced in sharded blockchain for boosting throughput and improving latency without compromising security and decentralisation [136]. Also, reducing the time for a block to propagate through the network deserves further exploration [137].
	How to enable scalable blockchain-based solutions?	In the IoV, vehicle density may vary in a drastic manner over time and location. Thus, to exploit the benefits of blockchain, scalable solutions should be investigated. For instance, changing the blockchain structure or sharding-based blockchain protocols can be further investigated [138].
IRS	How to transform fast to slow fading in high speed scenarios?	In high-speed scenarios, the vehicle's Doppler frequency results in a fast-fading between the source (e.g., BS) and the desired user. Taking into advantage the practical functionalities of the IRS to tackle the intrinsic drawbacks of wireless channels, the feasibility of mitigating the Doppler effect by adjusting the elements reflection phase is a unique and novel solution introduced from the IRS technology. From a PLS perspective, IRS can intentionally increase the Doppler effect (i.e., degrade the received signal) for unintended vehicles (eavesdroppers), yielding a more secure IoV [139], [140], [141].
	What is the impact of Electromagnetic Interference (EMI) over IRS performance?	Since the appearance of the IRS paradigm, a common practice in the vast literature of V2X IRS-aided communications is to neglect the EMI when analysing the secrecy performance. Specifically, EMI inevitably occurs by the presence of electromagnetic waves that reach the IRS from external natural, intentional, or non-intentional sources, yielding a negative impact on the security behavior. In fact, EMI on the IRS could be deliberately caused by active eavesdroppers in order to interfere with the properly tuning of phase shifts in the IRS elements, compromising the safety of V2X IRS-assisted communications [142].
	What is the impact of Spatial Correlation over IRS performance?	Inspection in prior literature of the IRS-related activities in secure V2X communications reveals that assuming independent and identically distributed (i.i.d) fading on IRS channels in a scattering environment is a common practice. However, it is an unrealistic scenario only justified for the sake of mathematical tractability. Based on this, the computation of the achievable secrecy performances over i.i.d. IRS channels in a lot of body of secure V2X research works are overrated. Hence, from a practical secrecy perspective, since an IRS will be implemented with a small inter-element IRS distance (e.g., $\lambda/4$ or $\lambda/5$) [143], [144], a spatial correlation across IRS channels must be considered for designing and implementing the next secure V2X IRS-aided communications.
	What is the effect of near and far-field propagation on IRS-aided V2X communications?	In the context of V2I IRS-aided communications, the near-field channel arises whenever the distance of the receiving vehicle is comparable with the IRS's dimensions. Indeed, if the number of reflecting elements is large and the vehicle approaches the IRS, it is eventually in the geometric near-field. In this sense, it is worth mentioning that the operation of V2I IRS-assisted in the near- or far-field is of paramount importance when quantifying the channel gain, which is linked to the end-to-end SNR. In the far-field V2I IRS setup, the average SNR scales as N^2 (being N the total number of elements at IRS), which seems a remarkable benefit. However, this power scaling law does not capture the near-field behaviour of the underlying scenario. An in-depth review of the literature shows that there are no V2I IRS-related works that have addressed the near-field propagation effect into the secrecy performance. Therefore, the research on this topic is open and non-trivial [145].
PLA	How to extend PLA solutions to end-to-end PLA?	Further investigation on the seamless integration of PLA into the existing, well-established cryptography primitives should be carried out. For instance, in [146], a cross-layer authentication framework is proposed, which does not impose any extra implementation overhead.
	How to improve the performance of PLA in dynamic and high mobility conditions of IoV scenarios?	PLA performance can be significantly affected by time-varying communication channels, thus adaptive schemes can be investigated relying on ML techniques in order to learn and use the complex time-varying environment to improve the reliability of PLA [89].

(Continued.)

signal processing challenges must be addressed to achieve ubiquitous, trustworthy, secure V2X communications. In this regard, the paradigm of IRS empowered by AI towards intelligent wireless environments is an open research direction that high-speed V2X communications can leverage to provide security at the physical layer level.

TABLE 4. ***(Continued)*** **Research directions.**

Key technology	Research questions	Research directions
Cell-free mMIMO	How to enhance the privacy of cell-free mMIMO-assisted V2X communications?	Based on AI-enabled intelligent 6G networks, FL will become a promising approach to boost highly secure cell-free mMIMO-aided V2X communications in IoV. Unlike the typical ML framework used in 5G systems, FL has the ability to process raw data collected by in-built vehicle sensors, traffic navigation, and vehicle localisation at the edge nodes instead of the cloud center (i.e., centralised infrastructure). This unique feature allows each mobile user train its own model using its own data while maintaining users' privacy. The core idea behind FL is decentralised learning, where the user data is never sent to a central server [147]. Based on this background, some works have investigated how to integrate FL into cell-free mMIMO [148], [149], [150]. However, it is worth mentioning that some key challenges (e.g., AI smartphones capabilities, sufficient data on the user to create a model) must be addressed to employ FL towards secure cell-free mMIMO-assisted V2X networks.
THz and VLC	How to design suitable schemes for more secure VLC-based outdoor vehicular applications?	More research is required for characterising the behaviour of VLC links in real-world driving scenarios. It is important to develop more realistic channel models and transmitter and receiver models, as well as verify adaptive techniques at the physical layer and receiver design to deal with the variations on the optical received power due to vehicle manoeuvres, mobility, and environmental and road conditions [103]. Also, hybrid RF/VLC schemes would render solutions that combine the benefits from both technologies for security enhancements [151].
	How to prevent eavesdropping when attackers are placed within the transmitter beam?	PLS techniques are attractive solutions for these cases. IRS-aided solutions can be used to design PLS schemes in THz systems. Also the multi-path propagation of THz communications can be exploited [152].
End-to-end Security	How to store keys reliably e.g. in IoT devices, provide sufficient crypto protection for light devices in post-quantum era?	Research on size-efficient post-quantum cryptography primitives, new security protocols that adapt to discover weaknesses. Efficient lightweight cryptography algorithms with perfect forward secrecy, protection against cryptoanalysis with ML and side-channel attacks. Standardization with IETF.
Quantum computing	What would be the role of quantum computing and post-quantum criptography in IoV?	Quantum computing presently relies on large stationary installations, and it is not expected to be an active part of IoV in the near future. However, it could be used to break traditional public-key cryptography based on large number factorization. Fortunately, new post-quantum algorithms are already available and being tested, e.g. for aviation [153]. Their additional overhead is manageable even in constrained environments.
BCs	How to improve the secure communication range on a Backscatter-assisted IoV?	IoV secure services usually demand a long communication range up to some kilometres. Although this requirement is challenging to nearly all wireless technologies, it is harder to achieve in backscatter networks. This is mainly because of the higher path-loss compared to conventional wireless communication. Therefore, it is of great importance to explore new technologies that assist the reflection of the waves from the backscatter transmitter to the receiver as well as new ways of transmitting the signal from the carrier emitter to the backscatter device in order to improve the coverage area.

Regarding authentication processes in IoV, physical layer techniques provide promising solutions with respect to latency and computational overhead, which are critical aspects in vehicular communications. However, further efforts are required to evolve these techniques to robust solutions that can be integrated into end-to-end authentication processes.

On the other hand, cellular network technology will likely support the strict QoS requirements (e.g., ultra-throughput, high- reliability, and energy efficiency) of the emerging V2X use cases. Nevertheless, conventional cell structures (i.e., smaller cells in each subsequent generation) will not be able to provide uniform QoS across all end-node locations that build the IoV ecosystem. To overcome this issue, cell-free mMIMO emerges as a promising solution to truly bring QoS to all IoV locations by leveraging innovative cellular architecture without cells or cell boundaries. Such a novel cellular architecture calls for a new class of security frameworks to ensure data privacy in V2X networks. In this sense, a new candidate for secure cell-free mMIMO-aided V2X networks is the recently developed FL, which introduces the concept of MEC to process data at the edge device instead of the centralized center. It is worth mentioning that some challenges (e.g., origin authenticity, computational capabilities at the end devices, enough local training data) need to be addressed for FL and cell-free architecture to converge successfully in the 6G era.

In general, directionality of wireless channels implies a more secure transmission as malicious agents would need a LoS condition to carry out successful eavesdropping or jamming attacks. Hence, THz links and VLC are considered resilient technologies to security attacks, thus being promising for IoV applications compared to sub-6 GHz RF communications. However, there is still some challenges on the road to gain the benefits of these technologies in 6G-based IoV, where improved physical layer techniques and transmitter and receiver designs should be investigated.

For the consolidation of ITS in the near future, more and more car manufacturers will supply sensors and communication interfaces to integrate mobile devices into modern vehicles. Such actuators/sensors can also facilitate the exchange of critical information for driving assistance systems. However, it is not enough for the information to achieve its desired target, but it is also necessary that data does not fall into the hands of unauthorised entities. Therefore, passive sensors and BC can be used for spy node/vehicle detection, thus the vehicle begins with the dissemination of critical information for driving assistance.

Apart from the immense technological development and higher degree of autonomy, IoV also generates many new privacy threats towards the passengers, drivers and pedestrians. Therefore, it is important to carefully identify the privacy risks that may occur and privacy protection mechanisms against various privacy breaches and cyber attacks at the design stage of the vehicular networks and systems.

Finally, Table 4 presents potential research directions for the technologies discussed in Section V.

B. CONCLUSION

This article provides a detailed overview of our vision for the future of V2X communications toward IoV, by focusing on the security and privacy aspects of the 6G-enabled IoV, and emphasizing the role of technological developments that pave the path towards 6G over the IoV security landscape. We first provide the roadmap of the technical evolution of V2X, the already defined use cases categories and their requirements. Then, we have discussed how key enabling technologies for 6G, such as network softwarisation, network slicing, blockchain, AI/ML, IRS, physical layer security, cell-free mMIMO, THz, and VLC can provide secure V2X communications. We finalise by discussing the leasons learned and providing important research directions for the development of those technologies towards a secure 6G-enabled IoV era.

REFERENCES

[1] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, Feb. 2020.

[2] D. Garcia-Roger, E. E. González, D. Martín-Sacristán, and J. F. Monserrat, "V2X support in 3GPP specifications: From 4G to 5G and beyond," *IEEE Access*, vol. 8, pp. 190946–190963, 2020.

[3] "Connecting vehicles today and in the 5G era with C-V2X," GSMA, London, U.K., Rep., 2019. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/08/Connecting-Vehicles-Today-and-in-the-5G-Era-with-C-V2X.pdf

[4] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[5] C. D. Alwis *et al.*, "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836–886, 2021.

[6] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[7] P. Porambage, G. Gur, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627.

[8] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and solutions for cellular based V2X communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 222–255, 1st Quart., 2021.

[9] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[10] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by Internet of Vehicles," *IEEE Access*, vol. 8, pp. 117593–117614, 2020.

[11] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[12] H. Wang *et al.*, "Architectural design alternatives based on cloud/edge/fog computing for connected vehicles," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2349–2377, 4th Quart., 2020.

[13] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

[14] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle-to-everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/2/334

[15] M. B. Mollah *et al.*, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[16] *IEEE Standard for Information Technology-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) Physical Layer (PHY) Specifications Amendment 6: Wireless Access Vehicular Environments*, IEEE Standards 802.11p-2010, 2010. [Online]. Available: https://standards.ieee.org/standard/802_11p-2010.html

[17] G. Naik, B. Choudhury, and J.-M. Park, "IEEE 802.11bd 5G NR V2X: Evolution of radio access technologies for V2X communications," *IEEE Access*, vol. 7, pp. 70169–70184, 2019.

[18] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 40–48, Apr. 2014.

[19] S.-Y. Lien, C.-C. Chien, G. S.-T. Liu, H.-L. Tsai, R. Li, and Y. J. Wang, "Enhanced LTE device-to-device proximity services," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 174–182, Dec. 2016.

[20] "Release 14 description, v14.0.0," 3GPP, Sophia Antipolis, France, Rep. TR 21.914-e00, 2018. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/21_series/21.914/

[21] "Release 15 description, v15.0.0," 3GPP, Sophia Antipolis, France, Rep. TR 21.915-f00, 2019. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/21_series/21.915/

[22] "Release 16 description, v16.0.1," 3GPP, Sophia Antipolis, France, Rep. TR 21.916-g01, 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/21_series/21.916/

[23] M. Harounabadi, D. M. Soleymani, S. Bhadauria, M. Leyh, and E. Roth-Mandutz, "V2X in 3GPP standardization: NR sidelink in release-16 and beyond," *IEEE Commun. Stand. Mag.*, vol. 5, no. 1, pp. 12–21, Mar. 2021.

[24] M. H. C. Garcia *et al.*, "A tutorial on 5G NR V2X communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1972–2026, 3rd Quart., 2021.

[25] "Advanced Plans for 5G." 3GPP. Jul. 2021. [Online]. Available: https://www.3gpp.org/news-events/2210-advanced_5g

[26] "The case for cellular V2X for safety and cooperative driving," 5GAA, Munich, Germany, White Paper, Nov. 2016. [Online]. Available: https://5gaa.org/wp-content/uploads/2017/10/5GAA-whitepaper-23-Nov-2016.pdf

[27] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," 2020, *arXiv:2012.07753*.

[28] *5GCAR Deliverable D2.1 5GCAR Scenarios, Use Cases, Requirements and KPIs*, document 5GCAR/D2.1, 5GPPP, Heidelberg, Germany, 2017, [Online]. Available: https://5gcar.eu/wp-content/uploads/2017/05/5GCAR_D2.1_v1.0.pdf

[29] *5G: Service Requirements for Enhanced V2X Scenarios, Version 16.2.0, Release 16*, 3GPP Standard TS 22.186, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122100_22199/122186/16.02.00_60/ts_122186v160200p.pdf

[30] M. Mozaffari, X. Lin, and S. Hayes, "Towards 6G with connected sky: UAVs and beyond," 2021, *arXiv:2103.01143*.

[31] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization, and research directions," *IEEE Netw.*, vol. 34, no. 5, pp. 306–314, Sep./Oct. 2020.

[32] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[33] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *EEE Trans. Intell. Veh.*, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[34] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015. [Online]. Available: https://www.mdpi.com/2079-9292/4/3/380

[35] "5G automotive vision," 5G-PPP, Heidelberg, Germany, Rep., 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf

[36] "Security guidelines for vehicle-to-everything (V2X) communication," Int. Telecommun. Union, Geneva, Switzerland, Rep. ITU-T X.1372, 2020. [Online]. Available: https://www.itu.int/rec/T-REC-X.1372-202003-I

[37] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[38] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[39] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[40] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, and S. X. Sherman, "Software defined Internet of Vehicles: Architecture, challenges and solutions," *J. Commun. Inf. Netw.*, vol. 1, no. 1, pp. 14–26, 2016.

[41] J. Chen *et al.*, "Service-oriented dynamic connection management for software-defined Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2826–2837, Oct. 2017.

[42] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[43] O. Sadio, I. Ngom, and C. Lishou, "Design and prototyping of a software defined vehicular networking," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 842–850, Jan. 2020.

[44] S. Garg, A. Singh, G. S. Aujla, S. Kaur, S. Batra, and N. Kumar, "A probabilistic data structures-based anomaly detection scheme for software-defined Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3557–3566, Jun. 2021.

[45] C. Lai, H. Zhou, N. Cheng, and X. S. Shen, "Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 40–49, Dec. 2017.

[46] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz, and A. Skarmeta, "Security orchestration and enforcement in NFV/SDN-aware UAV deployments," *IEEE Access*, vol. 8, pp. 131779–131795, 2020.

[47] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 4th Quart., 2015.

[48] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[49] A. J. Siddiqui and A. Boukerche, "On the impact of DDoS attacks on software-defined Internet-of-Vehicles control plane," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2018, pp. 1284–1289.

[50] *Zero-Touch Network and Service Management (ZSM): End-to-End Management and Orchestration of Network Slicing*, document ETSI GS ZSM 003, ETSI, Sophia Antipolis, France, 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/003/01.01.01_60/gs_ZSM003v010101p.pdf

[51] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3832–3840, Jun. 2021.

[52] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[53] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020.

[54] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[55] Q.-V. Pham *et al.*, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974–117017, 2020.

[56] J. Zhang and K. B. Letaief, "Mobile edge intelligence and computing for the Internet of Vehicles," *Proc. IEEE*, vol. 108, no. 2, pp. 246–261, Feb. 2020.

[57] J. Hu, C. Chen, L. Cai, M. R. Khosravi, Q. Pei, and S. Wan, "UAV-assisted vehicular edge computing for the 6G Internet of Vehicles: Architecture, intelligence, and challenges," *IEEE Commun. Stand. Mag.*, vol. 5, no. 2, pp. 12–18, Jun. 2021.

[58] Q. Xia, W. Ye, Z. Tao, J. Wu, and Q. Li, "A survey of federated learning for edge computing: Research problems and solutions," *High-Confidence Comput.*, vol. 1, no. 1, 2021, Art. no. 100008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266729522100009X

[59] X. Li, L. Cheng, C. Sun, K.-Y. Lam, X. Wang, and F. Li, "Federated-learning-empowered collaborative data sharing for vehicular edge networks," *IEEE Netw.*, vol. 35, no. 3, pp. 116–124, May/Jun. 2021.

[60] I. Ahmad *et al.*, "Machine learning meets communication networks: Current trends and future challenges," *IEEE Access*, vol. 8, pp. 223418–223460, 2020.

[61] J. Du, C. Jiang, J. Wang, Y. Ren, and M. Debbah, "Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 122–134, Dec. 2020.

[62] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.*, 2002, pp. 251–260.

[63] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4991–4999, Mar. 2021.

[64] S. B. Kotsiantis, "Supervised machine learning: A review of classification techniques," in *Proc. Emerg. Artif. Intell. Appl. Comput. Eng.*, vol. 160, 2007, pp. 3–24.

[65] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of Vehicles," *Inf. Sci.*, vol. 547, pp. 119–135, Feb. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025520305569

[66] I. Ahmad *et al.*, "The challenges of artificial intelligence in wireless networks for the Internet of Things: Exploring opportunities for growth," *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 16–29, Mar. 2021.

[67] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine learning threatens 5G security," *IEEE Access*, vol. 8, pp. 190822–190842, 2020.

[68] P. Sharma, D. Austin, and H. Liu, "Attacks on machine learning: Adversarial examples in connected and autonomous vehicles," in *Proc. IEEE Int. Symp. Technol. Homeland Security (HST)*, 2019, pp. 1–7.

[69] X. Zhou, W. Liang, J. She, Z. Yan, and K. I.-K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6G supported Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5308–5317, Jun. 2021.

[70] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective," 2021, *arXiv:2011.05411*.

[71] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[72] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, "A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities," *IEEE Access*, vol. 8, pp. 115876–115904, 2020.

[73] L. Cui *et al.*, "A blockchain-based containerized edge computing platform for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2395–2408, Feb. 2021.

[74] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, A. S. M. Kayes, and A. Zengin, "A blockchain-based authentication protocol for cooperative vehicular ad hoc network," *Sensors*, vol. 21, no. 4, p. 1273, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/4/1273

[75] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[76] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in Internet of Vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.

[77] M. Firdaus, S. Rahmadika, and K.-H. Rhee, "Decentralized trusted data sharing management on Internet of Vehicle edge computing (IoVEC) networks using consortium blockchain," *Sensors*, vol. 21, no. 7, p. 2410, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/7/2410

[78] H. Xiao, W. Zhang, W. Li, A. T. Chronopoulos, and Z. Zhang, "Joint clustering and blockchain for real-time information security transmission at the crossroads in C-V2X networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13926–13938, Sep. 2021.

[79] S.-W. Ko, H. Chae, K. Han, S. Lee, D.-W. Seo, and K. Huang, "V2X-based vehicular positioning: Opportunities, challenges, and future directions," *Wireless Commun.*, vol. 28, no. 2, pp. 144–151, Apr. 2021.

[80] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, May 2021.

[81] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, 2020, pp. 1–6.

[82] A. U. Makarfi *et al.*, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," 2020, *arXiv:2004.11288*.

[83] N. Mensi, D. B. Rawat, and E. Balti, "Physical layer security for V2I communications: Reflecting surfaces vs. relaying," 2020, *arXiv:2010.07216*.

[84] Y. Ai, F. A. P. de Figueiredo, L. Kong, M. Cheffena, S. Chatzinotas, and B. Ottersten, "Secure vehicular communications through reconfigurable intelligent surfaces," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7272–7276, Jul. 2021.

[85] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Inf. Netw.*, vol. 5, no. 3, pp. 237–264, 2020.

[86] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101437–101447, 2020.

[87] J. Wang, Y. Shao, Y. Wang, Y. Ge, and R. Yu, "Physical layer authentication based on nonlinear Kalman filter for V2X communication," *IEEE Access*, vol. 8, pp. 163746–163757, 2020.

[88] D. Xu, P. Ren, and J. A. Ritcey, "PHY-Layer cover-free coding for wireless pilot authentication in IoV communications: Protocol design and ultra-security proof," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 171–187, Feb. 2019.

[89] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[90] B. Han, S. Peng, C. Wu, X. Wang, and B. Wang, "LoRa-based physical layer key generation for secure V2V/V2I communications," *Sensors*, vol. 20, no. 3, p. 682, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/3/682

[91] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail, and C. Maple, "Adaptive and optimum secret key establishment for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2310–2321, Mar. 2021.

[92] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1834–1850, Mar. 2017.

[93] E. Nayebi, A. Ashikhmin, T. L. Marzetta, and H. Yang, "Cell-free massive MIMO systems," in *Proc. 49th Asilomar Conf. Signals Syst. Comput.*, 2015, pp. 695–699.

[94] O. T. Demir, E. Bjornson, and L. Sanguinetti, "Foundations of user centric cell-free massive MIMO," 2021, *arXiv:2108.02541*.

[95] B. Ai, A. F. Molisch, M. Rupp, and Z.-D. Zhong, "5G key technologies for smart railways," *Proc. IEEE*, vol. 108, no. 6, pp. 856–893, Jun. 2020.

[96] X. Zhang, T. Liang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in cell-free massive MIMO with RF impairments and low-resolution ADCs/DACs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8937–8949, Sep. 2021.

[97] X. Wang, Y. Gao, G. Zhang, and M. Guo, "Security performance analysis of cell-free massive MIMO over spatially correlated rayleigh fading channels with active spoofing attack," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2020, pp. 540–545.

[98] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, "Physical layer security in cell-free massive MIMO," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–7.

[99] D. P. M. Osorio, J. D. V. Sanchez, and H. Alves, *Physical-Layer Security for 5G and Beyond in 5G REF*, R. Tafazolli, C.-L. Wang, and P. Chatzimisios, Eds. Hoboken, NJ, USA: Wiley, 2019. [Online]. Available: https://doi.org/10.1002/9781119471509.w5GRef152

[100] J. D. V. Sanchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," *Ann. Telecommun.*, vol. 76, pp. 155–174, Jun. 2020.

[101] K. Sengupta, X. Lu, S. Venkatesh, and B. Tang, "Physically secure sub-THz wireless links," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2020, pp. 1–7.

[102] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 8, pp. 89–93, 2018.

[103] A. Memedi and F. Dressler, "Vehicular visible light communications: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 161–181, 1st Quart., 2021.

[104] S. Ucar, S. C. Ergen, and O. Ozkasap, "IEEE 802.11p and visible light hybrid communication based secure autonomous platoon," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8667–8681, Sep. 2018.

[105] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.

[106] F. Jameel, R. Duan, Z. Chang, A. Liljemark, T. Ristaniemi, and R. Jantti, "Applications of backscatter communications for healthcare networks," *IEEE Netw.*, vol. 33, no. 6, pp. 50–57, Nov./Dec. 2019.

[107] M. L. Memon, N. Saxena, A. Roy, S. Singh, and D. R. Shin, "Ambient backscatter communications to energize IoT devices," *IETE Tech. Rev.*, vol. 37, no. 2, pp. 196–210, 2020.

[108] S. J. Nawaz, S. K. Sharma, B. Mansoor, M. N. Patwary, and N. M. Khan, "Non-coherent and backscatter communications: Enabling ultra-massive connectivity in 6G wireless networks," *IEEE Access*, vol. 9, pp. 38144–38186, 2021.

[109] U. S. Toro, K. Wu, and V. C. M. Leung, "Backscatter wireless communications and sensing in green Internet of Things," *IEEE Trans. Green Commun. Netw.*, early access, Jul. 13, 2021, doi: 10.1109/TGCN.2021.3095792.

[110] Q. Yang, H.-M. Wang, Q. Yin, and A. L. Swindlehurst, "Exploiting randomized continuous wave in secure backscatter communications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3389–3403, Apr. 2020.

[111] J. Hu, X. Cai, and K. Yang, "Joint trajectory and scheduling design for UAV aided secure backscatter communications," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2168–2172, Dec. 2020.

[112] V. Hansini, N. E. Elizabeth, R. Hemapriya, and S. Kavitha, "Secured backscatter communication between smart cars in a vehicular ad-hoc network," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, 2016, pp. 1–4.

[113] W. U. Khan *et al.*, "Learning-based resource allocation for backscatter-aided vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 18, 2021, doi: 10.1109/TITS.2021.3126766.

[114] W. U. Khan, M. A. Javed, T. N. Nguyen, S. Khan, and B. M. Elhalawany, "Energy-efficient resource allocation for 6G backscatter-enabled NOMA IoV networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 21, 2021, doi: 10.1109/TITS.2021.3110942.

[115] W. U. Khan, F. Jameel, N. Kumar, R. Jäntti, and M. Guizani, "Backscatter-enabled efficient V2X communication with non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1724–1735, Feb. 2021.

[116] H. Bagheri *et al.*, "5G NR-V2X: Toward connected and cooperative autonomous driving," *IEEE Commun. Stand. Mag.*, vol. 5, no. 1, pp. 48–54, Mar. 2021.

[117] X. Zhou, W. Liang, J. She, Z. Yan, and K. I.-K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6G supported Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5308–5317, Jun. 2021.

[118] J. S. Ng *et al.*, "Joint auction-coalition formation framework for communication-efficient federated learning in UAV-enabled Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2326–2344, Apr. 2021.

[119] J. Zhang, F. Yang, Z. Ma, Z. Wang, X. Liu, and J. Ma, "A decentralized location privacy-preserving spatial crowdsourcing for Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2299–2313, Apr. 2021.

[120] S. A. A. Hakeem, M. A. Abd El-Gawad, and H. Kim, "A decentralized lightweight authentication and privacy protocol for vehicular networks," *IEEE Access*, vol. 7, pp. 119689–119705, 2019.

[121] Y. Zhao, Y. Wang, P. Wang, and H. Yu, "PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV," *IEEE Syst. J.*, early access, May 27, 2021. [Online]. Available: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2021 doi: 10.1109/JSYST.2021.3078797.

[122] T. Yoshizawa and B. Preneel, "Survey of security aspect of V2X standards and related issues," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2019, pp. 1–5.

[123] M. Botte, L. Pariota, L. D'Acierno, and G. N. Bifulco, "An overview of cooperative driving in the European union: Policies and practices," *Electronics*, vol. 8, no. 6, p. 616, 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/6/616

[124] "Rolling plan for ICT standardisation 2021," Eur. Comm., Luxembourg City, Luxembourg, Rep., 2021.

[125] "Certificate policy for deployment and operation of European cooperative intelligent transport systems (C-ITS), release 1.1," Eur. Comm., Luxembourg City, Luxembourg, Rep., 2018. [Online]. Available: https://ec.europa.eu/transport/sites/default/files/c-its_certificate_policy-v1.1.pdf

[126] "Protection profile V2X hardware security module," CAR 2 CAR Commun. Consortium, Braunschweig, Germany, Rep. 2056, 2019. [Online]. Available: https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.4.0/C2CCC_PP_2056_HSM.pdf

[127] "Protection profile for a road works warning gateway," Bundesanstalt Straßenwesen, Bergisch Gladbach, Germany, Rep. BSI-CC-PP-0106, 2019. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/pp0106b_pdf.pdf

[128] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6G era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021.

[129] T. Giannetsos and I. Krontiris, "Securing V2X communications for the future: Can PKI systems offer the answer?" in *Proc. 14th Int. Conf. Availability Rel. Security*, 2019, p. 95.

[130] "Intelligent transport systems (ITS); security; pre-standardization study on ITS facility layer security for C-ITS communication using cellular Uu interface, v1.1.1," Eur. Telecommun. Stand. Inst., Sophia Antipolis, France, Rep. ETSI TR 103 630, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103630/01.01.01_60/tr_103630v010101p.pdf

[131] "Tls authentication using intelligent transport system (ITS) certificates," Internet Eng. Task Force, RFC 8902, 2020. [Online]. Available: https://datatracker.ietf.org/doc/rfc8902/

[132] "Intelligent transport systems (ITS); security; pre-standardization study on misbehaviour detection; release 2, v2.1.1," Eur. Telecommun. Stand. Inst., Sophia Antipolis, France, Rep. ETSI TR 103 460, 2020.

[133] "Intelligent transport systems (ITS); security; its communications security architecture and security management; release 2, v2.1.1," Eur. Telecommun. Stand. Inst., Sophia Antipolis, France, Rep. ETSI TS 102 940, 2021.

[134] G. Dandachi, A. De Domenico, D. T. Hoang, and D. Niyato, "An artificial intelligence framework for slice deployment and orchestration in 5G networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 2, pp. 858–871, Jun. 2020.

[135] M. Gheisari, Q.-V. Pham, M. Alazab, X. Zhang, C. Fernández-Campusano, and G. Srivastava, "ECA: An edge computing architecture for privacy-preserving in IoT-based smart city," *IEEE Access*, vol. 7, pp. 155779–155786, 2019.

[136] Y. Wang, Y. Tian, X. Hei, L. Zhu, and W. Ji, "A novel IoV blockstreaming service awareness and trusted verification in 6G," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5197–5210, Jun. 2021.

[137] C. Santiago and C. Lee, "Accelerating message propagation in blockchain networks," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2020, pp. 157–160.

[138] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.

[139] E. Basar, "Reconfigurable intelligent surfaces for doppler effect and multipath fading mitigation," 2019, *arXiv:1912.04080*.

[140] Z. Huang, B. Zheng, and R. Zhang, "Transforming fading channel from fast to slow: IRS-assisted high-mobility communication," 2020, *arXiv:2011.03147*.

[141] K. Wang, C.-T. Lam, and B. K. Ng, "IRS-aided predictable high-mobility vehicular communication with doppler effect mitigation," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, 2021, pp. 1–6.

[142] A. D. J. Torres, L. Sanguinetti, and E. Björnson, "Electromagnetic interference in RIS-aided communications," 2020, *arXiv:2106.11107*.

[143] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.

[144] J. D. V. Sanchez, L. Urquiza-Aguiar, M. C. P. Paredes, and F. J. Lopez-Martinez, "Expectation-maximization learning for wireless channel modeling of reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 2051–2055, Sep. 2021.

[145] E. Björnson and L. Sanguinetti, "Power scaling laws and near-field behaviors of massive MIMO and intelligent reflecting surfaces," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1306–1324, 2020.

[146] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[147] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 46–51, Jun. 2020.

[148] T. T. Vu, D. T. Ngo, N. H. Tran, H. Q. Ngo, M. N. Dao, and R. H. Middleton, "Cell-free massive MIMO for wireless federated learning," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6377–6392, Oct. 2020.

[149] T. T. Vu, H. Q. Ngo, T. L. Marzetta, and M. Matthaiou, "How does cell-free massive MIMO support multiple federated learning groups?" 2021, *arXiv:2107.09577*.

[150] T. T. Vu, D. T. Ngo, H. Q. Ngo, M. N. Dao, N. H. Tran, and R. H. Middleton, "User selection approaches to mitigate the straggler effect for federated learning on cell-free massive MIMO networks," 2021, *arXiv:2009.02031*.

[151] I. W. G. da Silva, D. P. M. Osorio, E. E. B. Olivo, I. Ahmed, and M. Katz, "Secure hybrid RF/VLC under statistical queuing constraints," in *Proc. 17th Int. Symp. Wireless Commun. Syst. (ISWCS)*, 2021, pp. 1–6.

[152] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, 2019, pp. 865–872.

[153] N. Mäurer, T. Gräupl, C. Gentsch, and C. Schmitt, "Comparing different Diffie-Hellman key exchange flavors for LDACS," in *Proc. AIAA/IEEE 39th Digit. Avionics Syst. Conf. (DASC)*, 2020, pp. 1–10.

DIANA PAMELA MOYA OSORIO (Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering from Armed Forces University (ESPE), Sangolquí, Ecuador, in 2008, and the M.Sc. and D.Sc. degrees in electrical engineering with emphasis on telecommunications and telematics from the University of Campinas, Campinas, Brazil, in 2011 and 2015, respectively. Since 2015, she has been an Assistant Professor with the Department of Electrical Engineering, Federal University of São Carlos, São Carlos, Brazil. In 2020, she joined the 6GFlagship Program with Centre for Wireless Communications, University of Oulu, Finland, as Senior Research Fellow, and she is also an Adjunct Professor of Physical Layer Techniques for Security. Also, she has been a Postdoctoral Researcher for the Academy of Finland since 2020. Her research interests include wireless communications in general, 5G and 6G networks, and physical-layer security. She has served as a TPC and a reviewer for several journals and conferences.

IJAZ AHMAD (Member, IEEE) received the M.Sc. and Ph.D. degrees in wireless communications from the University of Oulu, Finland, in 2012 and 2018, respectively. He is currently working with the VTT Technical Research Centre of Finland, and is an Adjunct Professor with the University of Oulu. He has visited several institutions as a Visiting Scientists, such as Technical University of Vienna, Austria, in 2019, and Aalto University, Finland in 2018. He has more than 45 publications, including journals, conference papers, book chapters, a patent application, and published an edited book on the security of 5G, called *A Comprehensive Guide to 5G Security* (Wiley Inc.). His research interests include cybersecurity, security of 5G/6G, and the applications of machine learning in wireless networks. He is a recipient of several awards, including the Nokia Foundation, Tauno Tönning and Jorma Ollila grant awards, and the VTT Excellence Award for 2020. Furthermore, he has received two best paper awards in IEEE conferences.

JOSÉ DAVID VEGA SÁNCHEZ (Member, IEEE) received the B.Sc. degree in electrical and telecommunications engineering from the Escuela Politécnica del Ejército, Sangolquí, Ecuador, in 2013, and the M.Sc. degree in electrical engineering from the University of Campinas, Campinas, Brazil, in 2015. He is currently pursuing the Ph.D. degree in electrical engineering with Escuela Politécnica Nacional (EPN), Quito, Ecuador. He is a member of the Grupo de investigación en Redes Inalámbricas, which was awarded among the best research groups from EPN in 2019. His research interests include modeling, analysis, and simulation of wireless fading channels.

ANDREI GURTOV (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from the University of Helsinki, Finland, in 2000 and 2004, respectively. He is a Professor of Computer Science with Linköping University, Sweden. Previously, he was with the University of Oulu (three years) and Aalto University (six years) and visiting the International Computer Science Institute at Berkeley multiple times. He has coauthored over 200 publications, including four books, five IETF RFCs, six patents, over 60 journals, and 110 conference articles. He supervised 15 Ph.D. theses. His research interests are in network protocols, security of vehicular, airborne, industrial systems, mobile, wireless and IoT networks, and smartgrids. He is an ACM Distinguished Scientist, an IEEE ComSoc Distinguished Lecturer from 2016 to 2019, and the Chair of IEEE Sweden Section. He received best paper awards at IEEE CSCN'17 and IEEE Globecom'11, was the Co-Adviser of the best Doctoral Thesis in CS in Finland in 2017. He had served on numerous journal editorial boards and conference program committees, including IEEE INTERNET OF THINGS JOURNAL, *Sensors* (MDPI), IEEE ICNP, ACM MSWiM, and IFIP Networking. URL: http://gurtov.com

JOHAN SCHOLLIERS received the M.Sc. degree in 1986 and the Ph.D. degree in applied sciences from Katholieke Universiteit Leuven, Belgium, in 1993. Since 1993, he has been working with the VTT Technical Research Centre of Finland, since 2011 has been a Principal Scientist with the Automated Vehicles Team. His research interests are with cooperative intelligent transport systems, and evaluations of applications for vehicle safety. He is currently involved in several international projects related to 5G for automated vehicles, such as 5G-MOBIX, 5G-SAFEplus, and 5G-ROUTES.

MATTI KUTILA received the Master of Science degree in 2000 and completed his driver monitoring and neural networks related doctoral thesis in 2006. He is 46 years old and leads the Automated Vehicles Team with VTT. His career started in 1998, first as a Researcher and later as a Project Manager of the Automotive Industry Related Research and Development projects. He has prepared about 40 peer-reviewed scientific articles related to the connected and automated driving and holds five patent applications in the field. Recent years his expertise fields have been focused on automotive sensors, V2X technologies, sensor data fusion, artificial intelligence, and automated driving functions.

PAWANI PORAMBAGE (Member, IEEE) received the Doctoral degree from the Faculty of Information Technology and Electrical Engineering, University of Oulu, Finland, in 2018, where she is a Senior Researcher and an Adjunct Professor with the Centre for Wireless Communications. She has over ten years experience in security and privacy in different networks, including wireless sensor networks, telecommunication networks, and IoT. She is the Finnish National Coordinator for EU COST Action CA17124 and the Management Committee Member for IC1301 and CA16226. She was a Visiting Researcher with Nokia-Bell Labs, Finland, VUB, and the University of Zurich. She is currently involved in two EU projects, including INSPIRE-5Gplus and Hexa-X, and 6G Flagship supported by the Academy of Finland. She has coauthored more than 50 publications, including four book chapters.