WIRELESS WORLD
RESEARCH FORUM®

OUTLOOK

Visions and research directions for the Wireless World

Connected Vehicles

March 2021, No 25 V2

WWRF VIP WG CONNECTED VEHICLES

White Paper

Connected Vehicles: The Role of Emerging Standards, Security and Privacy, and Machine Learning

Editor:

SESHADRI MOHAN, CHAIR CONNECTED VEHICLES WORKING GROUP
PROFESSOR, SYSTEMS ENGINEERING DEPARTMENT
UA LITTLE ROCK, AR 72204, USA

Project website address: www.wwrf.ch

This publication is partly based on work performed in the framework of the WWRF. It represents the views of the authors(s) and not necessarily those of the WWRF.

EXECUTIVE SUMMARY

The Internet of Vehicles (IoV) is an emerging technology that provides secure vehicle-to-vehicle (V2V) communication and safety for drivers and their passengers. It stands at the confluence of many evolving disciplines, including:

evolving wireless technologies, V2X standards, the Internet of Things (IoT) consisting of a multitude of sensors that are housed in a vehicle, on the roadside, and in the devices worn by pedestrians, the radio technology along with the protocols that can establish an ad-hoc vehicular network, the cloud technology, the field of Big Data, and machine intelligence tools.

WWRF is presenting this white paper inspired by the developments that have taken place in recent years in standards organizations such as IEEE and 3GPP and industry consortia efforts as well as current research in academia. This white paper provides insights into the state-of-the-art regarding 3GPP C-V2X as well as security and privacy of ETSI ITS, IEEE DSRC WAVE, 3GPP C-V2X. The White Paper further discusses spectrum allocation worldwide for ITS applications and connected vehicles. A section is devoted to a discussion on providing connected vehicles communication over a heterogonous set of wireless access technologies as it is imperative that the connectivity of vehicles be maintained even when the vehicles are out of coverage and/or the need to maintain vehicular connectivity as a vehicle traverses multiple wireless access technology for access to V2X applications. The White Paper carries a discussion of ongoing research in academia concerning the use of Cloud technology for V2X applications, blockchain technology for imparting security and privacy in the connected vehicles environment and the applicability of AI/machine learning to advanced spectrum management and spectrum sharing. It is anticipated that AI/machine learning techniques will be increasingly applied to improve traffic management, impart security and privacy, and to intelligently deliver V2X applications to vehicular users in the connected vehicles environment.

This Outlook is an updated version of Outlook 25 with a new section added on “The Role of Artificial Intelligence and Machine Learning in the Evolution of Connected Vehicles” with additional references. All the references of individual sections of Outlook 25 are consolidated at the end of the present Outlook.

Contributors

Seshadri Mohan
Systems Engineering, University of Arkansas at Little Rock, 2801 S University Ave, LITTLE ROCK, 72204, AR, United States.

Nigel Jefferies Huawei, UK

Osvaldo Gonsa
Dept. of Wireless Signals Technologies, Corporate S&T, Continental Teves Ag & Co. oHG.

G David González
Dept. of Wireless Signals Technologies, Corporate S&T, Continental Teves Ag & Co. oHG.

Andreas Andrae
Dept. of Wireless Signals Technologies, Corporate S&T, Continental Teves Ag & Co. oHG.

G C Deepak
Kingston University, London, UK

Ashok Chandra
Former Wireless Adviser to the Government of India, Ministry of Communications, New Delhi, India

Purnima Lala Mehta
IILM College of Engineering and Technology, Greater Noida, India

Marcus Wong
FutureWei Technologies, Bridgewater, NJ, USA

Rajen Akalu
Ontario Tech University, Oshawa, Canada

Sachin Sharma
Computer Science, Graphic Era University, Dehradun, Utharakhand, India
Ricard Vilalta CTTC, Spain

Contents

1 Introduction

The field of connected vehicles stands at the confluence of three evolving disciplines – the Internet of Things (IoT), emerging standards for connectivity of vehicles, and AI/machine learning. The number of connected IoT devices is expected to grow from 9.5 billion devices in 2019 to 21.5 billion devices in 2025 [1]. More optimistic estimates project the number of IoT devices in 2025 to be 41.5 billion connected devices [2]. Consequently, applications of IoT devices have rapidly expanded to integrate intelligent sensing and processing along with smart applications of the technology into various fields such as smart homes, smart appliances, enterprises, smart transportation including connected vehicles, smart cities, agriculture, energy, security, healthcare, shopping, location-based services including tracking and other similar fields. The exponential growth of IoT is transforming the quality of living of human beings around the globe.

Fueling the growth in the evolution of vehicles towards total automation is the development of novel sensors, 3D cameras, lidars and radars, and their ability to connect to the Internet and upload the data to a cloud. The sensors of an autonomous vehicle collect anywhere from 1.4 TB to 19 TB of data per hour [3]. Whether or not the vehicles are autonomous, one of the key features of connected vehicles is that they are able to share data between themselves in real-time. For example, the scene of an accident or road work encountered by a vehicle can be immediately shared with vehicles it is connected to. Thus, vehicles may learn about accidents or road work well in advance so as to enable them to make smart decisions and establish alternate routes to their destinations. This document will help in understanding the role that emerging standards, 5G and beyond and machine learning play in the realm of connected vehicles.

Facilitating the connectivity of vehicles is the development of standards in various standards organizations. They are aimed at ensuring communication takes place between various entities in a connected vehicles network - Communications Technologies – vehicle-to-vehicle (V2V), vehicle- to-infrastructure (V2I), infrastructure-to-vehicle (I2V), vehicle-to-pedestrian (V2P), and vehicle-to-nomadic devices (V2ND). Examples of such communications are:

- V2V - to inform each other of their arrival at an intersection; an advanced example is V2V communication is for vehicle platooning;
- V2I and I2V for communications between vehicles and traffic signals;
- V2P for communications with a pedestrian who may be crossing the road at an intersection and instruct the vehicle to stop; and

- V2ND, also referred to as V2N and V2D is for communications between vehicle and in-vehicle device, for example, for emergency braking.

Standards can target both long range and short range communications. Long range communication usually may have relaxed latency constraints whereas short range communication may impose stringent latency constraints. Short range communication standards have been variously called as ITS-G5 (in Europe), Wireless Access in Vehicular Environments (WAVE), Dedicated Short Range Communication (DSRC in North America) or IEEE 802.11p. 3GPP has been developing standards for communication between vehicles. Release 14 has prescribed Long Term Evolution (LTE) V2X and Release 15 5G V2X. Obviously, the intent is to facilitate the vision of connected vehicles with the help of widely deployed cellular technology and meet the bandwidth and latency constraints. The document will address the standards' development for connected vehicles and their performance.

The vast amount of raw data collected must be mined for it to become useful in ensuring traffic safety by means such as intelligent rerouting of traffic or distribution of information on roadwork activities or accidents. Machine learning is a mechanism that has become extremely powerful in extracting meaningful data. A number machine learning algorithms exist and can be broadly classified under unsupervised, supervised, and reinforcement learning algorithms. A number of algorithms exist under each category. This document will address the impact of machine learning and their applications such as spectrum management to connected vehicles with several use cases.

Section 2 provides an overview of 3GPP's C-V2X standard, specifically Releases 14, 15, and 16. The releases are about both LTE-based C-V2X (Rel. 14 and 15) and 5G C-V2X (Rel.16). This Section also discuss several use cases and their requirements such as latency, reliability, message size, message frequency, range, speed, etc., as detailed in the releases. C-V2X caters to use cases while network coverage is available but also when the coverage is unavailable. Besides a discussion of both LTE-based and 5G-based C-V2X, the section also includes information concerning the stake holders, the timeline, and use cases.

Section 3 discusses the need to provide V2X connectivity with a range of heterogeneous radio access technologies. It is possible vehicles may encounter a situation when the established radio access technology such as DSRC, or while traveling a mountainous terrain or countryside, access to a cellular network may not be available, in which case other technologies such as low power wide area network (LPWAN), multi-hop D2D, cognitive radio, unmanned aerial vehicles (UAVs) communication and Wi-Fi network could be the viable options for critical data transmission and reception.

Section 4 provides an introduction to spectrum allocation for various Intelligent Transportation System (ITS) applications, including applications for connected vehicles. Specifically, the section discusses ITU-Radio communications (R) concerning the allocation and management of frequency spectrum to the three regions of the world.

Section 5 elaborates on security of European Telecommunications Standards Institute ITS (ETSI ITS), IEEE DSRC WAVE, 3GPP C-V2X and privacy issues. Sections 6 and 7 dwell on ongoing research and approaches to offering security, privacy, and trust using technologies such as cloud, blockchain, and AI/machine learning techniques.

Section 8 offers some conclusions and summarizes the contributions the authors have strived to bring forth to the readers.

2 Relevant Standards

2.1 Cellular-based vehicular communications: The 3GPP's C-V2X standard

The 3rd Generation Partnership Project (3GPP) initiated studies on required enhancements of the Long Term Evolution (LTE) system to support vehicular communications in the fourth quarter of 2015. Since then, normative efforts have been placed over three 3GPP Releases (14, 15, and 16) within the three major Technical Specification Groups of the 3GPP: Radio Access Network (RAN), Core Network and Terminals (CT), and Service and System Aspects (SA). Hereafter, Rel. 14 and 15 refer to 4G (LTE) Cellular Vehicle-to- Everything (C-V2X), while Rel. 16 refers to 5G C-V2X. Naturally, the intention was to leverage the widely deployed mobile broadband infrastructure to provide the automotive industry with means to realize the vision of connected cars, and more recently, autonomous driving. In this section, an overview of C-V2X functionality of the 3GPP's 4G technology is provided, as well as a short outlook on 3GPP's 5G C-V2X.

Fundamentally, vehicle-to-everything communications imply transmitting/receiving information from/to (at least) one vehicle, infrastructure entity, or vulnerable road user. Hence, V2X communications can broadly be grouped into two categories: 1) V2V- direct communications among vehicles, V2I - road side units, V2P - vulnerable road users without using cellular network infrastructure, and V2ND - vehicle to devices or sensors that pedestrians may carry, and 2) communications between vehicles and (static) network infrastructure. In order to support these different types of V2X communications, C-V2X technology exploits two basic communication interfaces: Uu (evolved cellular interface) and PC5 (also referred to as side-link) as shown in Fig. 1.

Communication through the Uu interface employs the conventional cellular link in downlink, from network infrastructure (e.g., base station) to User Equipment (UE) or vehicular-mounted UE, and in uplink, from UE to network infrastructure. The PC5 interface allows for direct communication between peers, i.e., vehicles and other road users. In Rel. 14 and 15 side-link transmissions employ the same frequency resources and waveform (Discrete Fourier Transform (DFT) and Orthogonal Frequency Division Multiplexing (OFDM)) as the LTE uplink. This type of communication evolved from the Device-to- Device (D2D) framework (Proximity Services) standardized in the Rel. 12 and 13.

Uu-based communication requires network coverage, i.e., the UE is in the

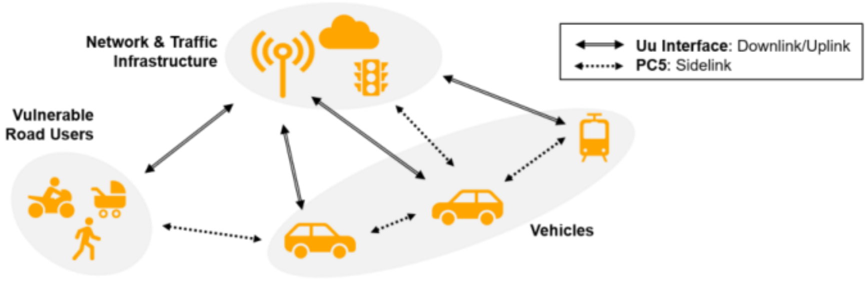

Network & Traffic Infrastructure
Vulnerable Road Users
Vehicles
Uu Interface: Downlink/Uplink
PC5: Sidelink

Fig. 1 Communication Types supported by C-V2X

radio range of a base station, and in this circumstance, the base station man ages the radio resources to be used by the UEs. PC5-based communication is possible with or without network coverage, which is a very important feature of C-V2X. In case of network coverage, the base station can take control of resource allocation and/or scheduling on the PC5 interface (mode 3). When the UE is out of network coverage, it will autonomously select the radio resources to be used from a pre-configured set (mode 4). It is worth noting that C-V2X can operate without provisioning of a Universal Subscriber Identity Module (USIM). To enable USIM-less communication, automobile Original Equipment Manufacturers (OEMs) will pre-configure vehicular-mounted UE with the required radio-related parameters (e.g., resources to be used, resource allocation schemes, synchronization sources, etc.) and to perform authorization for certain V2X services. Thus, PC5-based USIM-less communication allows C-V2X to support critical safety services when network coverage is unavailable or if the vehicle does not have an active cellular subscription. These parameters can also be securely updated, if needed, by the OEM. C-V2X employs three main sources of synchronism (synchronization signals): base stations, UE, and Global Navigation Satellite System (GNSS). Naturally, synchronization signals from the base stations are the preferred approach in-coverage, while synchronization signals from UE and GNSS are alternatives for out-of-coverage operation.

In terms of core network architecture, two new elements exist in the core network to support V2X services: the V2X Control Function and the V2X Application Server. These two elements interplay with the rest of network elements and UE to provide authorization/configuration to V2X services and timely modification/termination of existing connections through standardized interfaces and procedures at different levels of the protocol stack. The C-V2X architecture is fundamentally the same for releases 14 and 15.

From SA perspective, Rel. 14 [4, 5] C-V2X focused on defining (basic safety/non-safety) use-cases, requirements (latency, reliability, message size, message frequency, range, speed), and design principles, such as the need for operation in and out of network coverage, interworking between UEs of different network operators, flexibility (prioritization, range, distribution area, etc.), capacity (high density of UE), energy efficiency, and positioning accuracy. Rel. 15 [6, 7] saw a more detailed description of use cases including vehicle platooning, advanced driving, extended sensors, remote driving, and other general aspects. Obviously, more ambitious performance requirements were accordingly defined, for instance, improved positioning accuracy (0.1m), very high density (4k+ cars/km2), and UE-enabled relaying for access and discovery.

Summarizing from RAN perspective, Rel. 14 enhancements were predominantly introduced to handle high relative vehicle speeds (Doppler shift) up to 500kmph, time synchronization outside base station coverage, solutions to enhance latency, capacity and reliability, such as congestion control for operation in high traffic load, as well as sensing and traffic management for different V2X services. C-V2X Rel. 15 aims at complementing Rel. 14 C-V2X in a backward compatible manner. The major enhancements introduced in Rel. 15 include further latency reductions, carrier aggregation in the side-link, higher order modulations (64-QAM), transmit diversity, and short Transmission Time Interval (TTI), among others.

The current discussion on 5G C-V2X (based on New Radio, NR [8]) focuses on the following major areas: side-link design, evaluation of Uu interface for advanced V2X use cases, Uu-based side-link resource allocation/configuration, and several scenarios and schemes for coexistence (between LTE and NR C-V2X). To provide an outlook on 5G C-V2X from the RAN point of view, some important agreements (only few selected ones) made by the time of this writing are highlighted below:

- Three different types of transmissions will be supported for the side-link: unicast, groupcast, and broadcast.
- Enhancements could include, among others, channel feedback, channel state information acquisition, power control schemes, link adaptation, and multi-antenna transmission schemes.
- Consideration of the bandwidth part concept introduced for NR.
- Flexible time-frequency multiplexing of data and control channels.
- Variety of Uu-based resource allocation approaches, including dynamic resource allocation, activation/deactivation (e.g., semi-persistent scheduling), and (pre-)configured.
- Potential use of different subcarrier spacings and cyclic prefix, but only one at a time.
- In Rel. 16, at least CP-OFDM will be supported for the side-link.
- A more accurate, and perhaps proactive, QoS management for C-V2X, based on the framework defined for NR, could be adopted.

In addition, 3GPP's evaluation methodology has also been substantially revised to account for more realistic assumptions regarding automotive use cases (e.g., traffic models, deployments scenarios, number of antennas, channel models, etc.) [9]. As a general note, it is important to mention that 5G C-V2X will benefit from the advanced features of NR's physical layer.

2.2 C-V2X Timeline

Fig. 2 shows an approximate timeline of the C-V2X standardization. The evolution of LTE-based V2X continues towards NR C-V2X and it holistically represents the very first, yet reliable and advanced, C-V2X system. NR-based V2X will leverage not only the lessons from the development and deployment of LTE-V2X, but also the advanced features of 5G, thus providing an ideal ecosystem to develop V2X services.

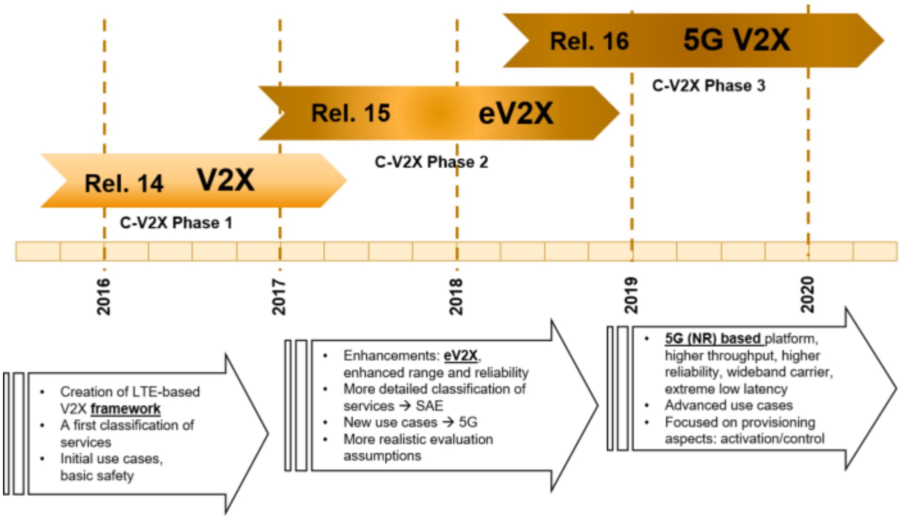

Rel. 16
5G V2X
C-V2X Phase 3
Rel. 15
eV2X
C-V2X Phase 2
Rel. 14
V2X
C-V2X Phase 1
2016
2017
2018
2019
2020
• Creation of LTE-based V2X framework
• A first classification of services
• Initial use cases, basic safety
• Enhancements: eV2X, enhanced range and reliability
• More detailed classification of services → SAE
• New use cases → 5G
• More realistic evaluation assumptions
• 5G (NR) based platform, higher throughput, higher reliability, wideband carrier, extreme low latency
• Advanced use cases
• Focused on provisioning aspects: activation/control

Fig. 2 Approximate Timeline for 3GPP's C-V2X Standardization

Finally, it is important to mention that NR C-V2X has a clear complimentary nature with respect to LTE C-V2X, i.e., NR C-V2X will complement LTE C-V2X by supporting the most advanced use cases, and, as indicated before, coexistence between them is a very important agenda item.

2.2.1 Stakeholders of C-V2X Ecosystem

As the creation of a whole new C-V2X ecosystem is an international approach, various stakeholders are involved, as illustrated in Fig. 3 below:

Of course, the automotive industry is in the lead of defining use cases and corresponding requirements for new C-V2X services. However, technology development groups, such as IEEE or 3GPP, have to account for worldwide and local regulation (e.g., radio spectrum) as well as existing regional standards (e.g., Asia, Europe, US) when specifying dedicated solutions.

One important organization that aims at paving the way for C-V2X applications is the 5G Automotive Association (5GAA). Since its creation in September 2016, the 5GAA acts as a global, cross-industry organization of

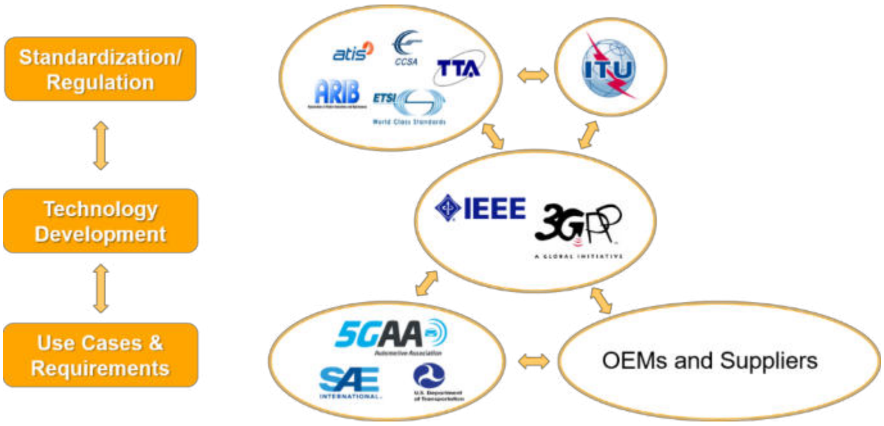


Fig. 3 Stakeholders of C-V2X

companies from the automotive and ICT industries, whose members jointly develop end-to-end solutions for future mobility and transportation services. 5GAA works towards defining requirements for advanced and new V2X use cases and tries to leverage its liaisons with standards developing organizations to promote technical standardization of C-V2X solutions.

According to the 5GAA methodology, relevant use cases and assumptions are thoroughly analyzed including user story, actors, road environment and roadside infrastructure, use case goals, constraints, event flow, service-level Key Performance Indicators (KPIs), as well as information requirements. Further, appropriate service-level metrics are derived and interpreted from a net- work point of view in order to align with 3GPP's network-level KPIs. For example, specific requirements resulting from a use case analysis comprise detailed information on communication range, information requested/generated, service-level latency, service-level reliability, vehicle sensor information (e.g., velocity, jerk, etc.), vehicle density, and positioning accuracy.

2.2.2 Roadmap and Evolution of C-V2X Use Cases

Originally, the technology behind Rel. 14 C-V2X has targeted a well-defined set of use cases for automotive safety, known as Day 1 and Day 1.5 use cases [10]. The initial release of C-V2X will target the basic safety use cases which already exist today as described in the Fig. 4 below. These use cases require direct, broadcast-based communications but with short latency and good reliability. The so-called Day 1.5 use cases, such as information on fueling and charging stations for alternative fuel vehicles, vulnerable road user protection, on street parking management and information, off-street parking information, require more complex approaches than direct peer-to-peer communication and are out of scope of this discussion.

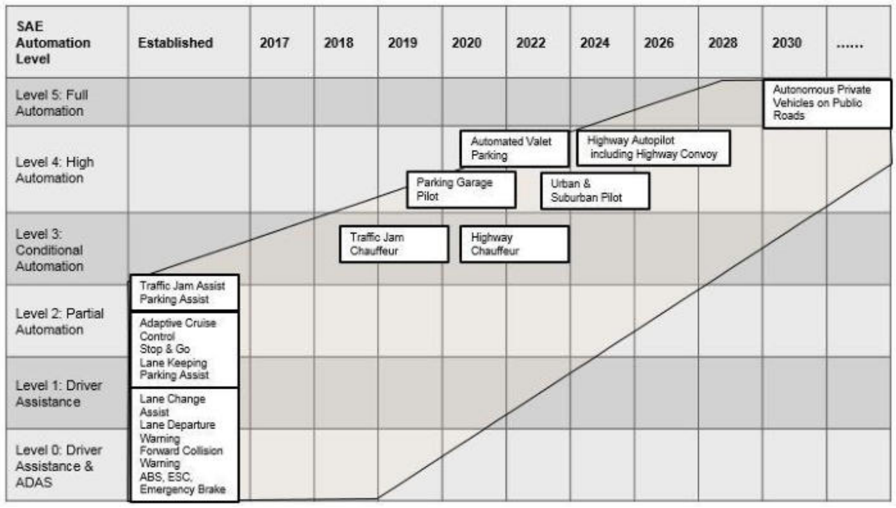

SAE Automation Level
Established
2017
2018
2019
2020
2022
2024
2026
2028
2030
......
Level 5: Full Automation
Level 4: High Automation
Level 3: Conditional Automation
Level 2: Partial Automation
Level 1: Driver Assistance
Level 0: Driver Assistance & ADAS
Autonomous Private Vehicles on Public Roads
Automated Valet Parking
Highway Autopilot including Highway Convoy
Parking Garage Pilot
Urban & Suburban Pilot
Traffic Jam Chauffeur
Highway Chauffeur
Traffic Jam Assist Parking Assist
Adaptive Cruise Control Stop & Go Lane Keeping Parking Assist
Lane Change Assist Lane Departure Warning Forward Collision Warning ABS, ESC, Emergency Brake

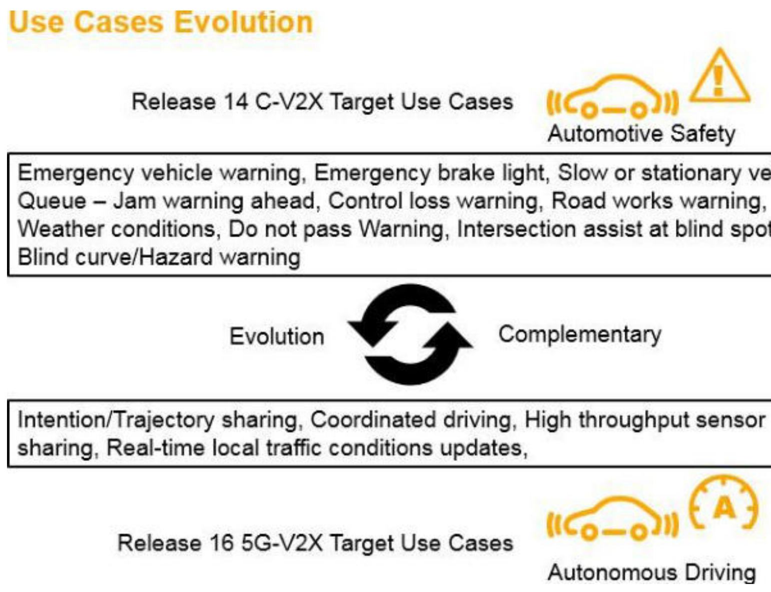
Fig. 4 Automated Driving Use Cases Deployment Path for Passenger Cars [11]

Subsequent releases of C-V2X (namely Rel. 15 and Rel. 16 NR V2X) will support the same basic use cases and more challenging and futuristic ones that require even lower latency, higher reliability, or higher bandwidth.

When we consider the available functionality in the previous releases of LTE and the way they evolved, the LTE standard in 3GPP Rel. 13 was not capable of meeting the low-latency and high-speed requirements of safety critical V2V applications. It could only support automotive applications that were not safety relevant and that relied on V2N communication. Only those applications that were oriented towards improved driving efficiency and comfort and that did not impose stringent latency requirements could be supported. Further, vehicles with poor or no cellular network coverage were not be able to communicate with each other.

As described in the previous section, Rel. 14 C-V2X supports low latency and reliable exchange of messages among vehicles and the infrastructure to enhance safety and efficiency. With the advancement of the technology, it is expected that this direct communication is just the start of a path towards supporting use cases for autonomous driving. This evolution will require additional V2X communication capabilities, such as those defined for the 5G standard and beyond, which are enhanced mobile broadband, extreme low latency, high reliability, and longer range. Continuous evolution and developments in V2X technologies are needed to meet new requirements and the new use cases that will emerge [12].

Currently, 3GPP is working on specifying 5G NR-based V2X. As also shown in Fig. 5, we must emphasize that 5G radio access enhancements will enable advanced use cases for data exchange and will not duplicate the Rel. 14 V2X functionality as illustrated in Fig. 2. By doing this, 5G-based V2X services can be added and complement the foundational capabilities of LTE



Use Cases Evolution

Release 14 C-V2X Target Use Cases

Automotive Safety

Emergency vehicle warning, Emergency brake light, Slow or stationary vehicle, Queue – Jam warning ahead, Control loss warning, Road works warning, Weather conditions, Do not pass Warning, Intersection assist at blind spots Blind curve/Hazard warning

Evolution

Complementary

Intention/Trajectory sharing, Coordinated driving, High throughput sensor sharing, Real-time local traffic conditions updates,

Release 16 5G-V2X Target Use Cases

Autonomous Driving

Fig. 5 Evolution of Automotive Use Cases with C-V2X

V2X. 5G NR V2X is expected to be future-proof and backwards compatible with LTE V2X as per design [13].

The authors consider that the path for LTE-based vehicular communications is clear: LTE-based C-V2X will continue to deliver cellular V2X direct communications and provide ubiquitous coverage as 5G technologies are designed and deployed. As new technology features are incorporated, these will be able to offer additional value or new services beyond those of basic safety.

3 Heterogeneous Connectivity and Requirements of CV

The automobile and information technology industries have been entirely independent industries, which, in recent years, are rapidly converging due to the rapid development in wireless technologies, e.g., LTE-A, 5G and beyond. This results a new domain of Internet-of-Vehicles (IoV) which broadly consists of V2V and V2I communications [14]. When the vehicles exchange data, e.g., traffic, road conditions, weather forecast etc. with each other or with the fixed infrastructure, it can dramatically improve the road safety and efficiency of the transportation systems.

Various wireless network standards have been proposed to enable IoV communication. For instance, DSRC in the USA and C-ITS in Europe are under active research and testing phase, which are based on the highly anticipated technology; IEEE 802.11p standards [15]. This is also one of the several standards for connected vehicles which is almost ready for the deployment in a real scenario. However, the proposed new protocols will have to go through a lot of testing, field trials and further standardization by stakeholders before commercial deployment. This is due to the fact that, unlike the cellular communications for voice and data, there is absolutely no room for any security compromise in IoV networks due to the nature of the applications. Therefore, network connectivity, reliability and robustness against any security threat are the key parameters to achieve the IoV goals in practice.

The success of IoV network deployment directly depends on the network coverage and quality of service (QoS) of the wireless channel, which include the end-to-end latency, jitter, received signal power etc. Therefore, vehicle's radio unit should be able to connect multiple radio access technologies (RATs) to achieve the always-on connectivity. Such a heterogeneous network requirements can be achieved by mounting each vehicle with multi-RATs transceivers. In such cases, when the vehicle losses the DSRC/C-ITS connection, it can reroute the critical information through the cellular network, e.g., NB-IoT, which is a dedicated cellular technology for IoT applications. In many segments of the road, especially, motorways and countryside, the cellular radio signal is too weak which makes it not possible to communicate with other vehicles or road side infrastructure. In such a case, for instance, low power wide area network (LPWAN), multi-hop D2D, cognitive radio, unmanned aerial vehicles (UAVs) communication and Wi-Fi network could be the viable options for critical data transmission and reception.

3.1 Heterogeneous Radio Access Technologies – A Comparison

There are two broadly categories of use cases in the IoV networks, i.e., safety-related and non-safety-related. The V2V communication is highly safety-related use case because there are likely to have packet collisions if there is no 100% reliability of the network. The cellular unicast network, e.g., LTE, cannot handle the huge amount of data from V2V terminals. Moreover, cellular network is an expensive option to install throughout the roadsides. The higher end-to-end delay occurs during the handover process which is also not suitable for IoV communications. The higher mobility of vehicles will have short coherence time which makes channel estimation task very complex if IoV works under cellular network. For safety-related V2V communications, 802.11p, which works on 75~MHz of bandwidth in the 5.9~GHz region, is more suitable due to the improved network reliability. Moreover, the accurate channel characterization among the vehicles is equally important for the reliable connectivity to transmit accurate and real-time information [16].

The deployment cost for 802.11p is also relatively lower because it can be easily deployed on the roadside infrastructure, such as lampposts. The allocated band for 802.11p is also worldwide available to use for IoV. It can achieve 10 Mbps throughput within the range of 500 m and an average roundtrip delay 10ms. The first major problem is that it has relatively short coverage range. Secondly, network congestion occurs in the dense network scenario in the urban area. However, the inter-vehicle distance is significantly lower than the coverage range of DSRC/C-ITS, it is likely to be the ideal technology for the safety-related V2V communications scenario. Due to the short inter-vehicle distance, the V2V communication delay is significantly reduced and 10 Mbps throughput is sufficient to transmit any safety-related data to the neighbor vehicles.

On the other hand, the V2I communication needs a higher transmission range, however, the delay constraint can be, to some extent, relaxed. If we use the 802.11p based DSRC/C-ITS standards for V2I communication, a large number of base stations are needed to cover the driving routes. In addition, a robust handover mechanism is needed due to higher mobility of the vehicles. As an alternative solution to this problem, long-range wide area network (LoRaWAN) can be used for non-safety related V2I communications. Such a heterogeneous IoV network provides improved network reliability and coverage to achieve the safe driving conditions.

The IoT protocols, such as, LoRa and SigFox network, operates on 868 MHz in Europe and 915 MHz in the USA which provides up to 10 km coverage distance. It consumes very low power and the transmitted information can be decoded even when the received power is very low. It is highly scalable and capable of listening to different channels simultaneously. Particularly in IoV network, it can broadcast critical messages to a large number of vehicular Long Range (LoRa) terminals to minimize road congestion or accidents, which makes it a strong candidate for V2I communications.

Here, LoRa is less likely suitable for V2V communication because it needs optimal transmit power control technique to avoid the interference or packet loss. When the transmission range is higher, a LoRa transmitter covers longer road distance. In cases there are many vehicles on the road, the majority of them will have to retransmit the packets several times. This worsens the energy efficiency and significantly increases the packet loss. Due to the short coverage area of 802.11p, the interference issue can be solved to improve the V2V throughput and end-to-end delay. Therefore, 802.11p is more suitable for safety-related V2V communication than the LoRa network case.

On the other hand, the significant end-to-end delay associated with the LoRaWAN and SigFox makes them unsuitable for IoV network, especially, for the safety-related information transmission. Moreover, such IoT technologies were not primarily designed for high mobility user devices, such as, the vehicular communication. Therefore, substantial improvement is needed on the physical and MAC layers of LoRaWAN/SigFox to implement in IoV network. One of the ways to improve the latency is to use the concept of cognitive radio spectrum sensing technique. The channel quality can be measured by using, for example, the energy detection method. The better the channels, the higher the received energy can be by the vehicles. Moreover, if there is a packet collision, the channels can be reallocated up to the maximum number of times, which can be fixed by the operator as a system defined parameter.

However, in any proposed solution, there is always a tradeoff among latency, throughput and coverage of the network. A further research will be needed to provide heterogeneous connectivity by means of available radio technologies to achieve the robust IoV network applications.

4 Spectrum Issues

4.1 Background

The unprecedented explosive growth in human population and the technological growth the world over during the last four to five decades has resulted in ever increasing vehicles (may be two, three and four wheelers; trains; planes; ships, and others). The population growth has also led to increased numbers of pedestrians on the roads, especially in densely populated metropolitan areas. The dense urban population by and large experience heavy traffic congestion leading to sometimes accidents. The accidents do also occur on highways. The congestion too plays a significant role in reduced vehicle efficiency alongside with fuel consumption of transport infrastructure, air pollution including surge in travel time etc. Management of traffic in earlier times was under control due to considerably less number of vehicles. The Intelligent Transport System (ITS) or connected vehicles technology provides solutions for reducing traffic congestion and a synergy of new information technology for simulation, real- time control, and communications networks. ITS supports safe and efficient transportation of goods and humans using information and communication technologies (ICT).

The Research and Development (R&D) activities relating to core technologies of ITS have started since 1995. Some countries have started deploying ITS for vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N) and vehicle-to-pedestrian (V2P) communications. Fig. 6 below illustrates radiocommunications connectivity for V2X, for which radio spectrum would be needed. At international levels, ITU-R, ISO, and IEEE etc. are conducting studies and developing standards for ITS applications. At Regional levels, organizations namely Asia-Pacific's AWG, ARIB, ETSI are working too in these directions.

4.2 Radio Spectrum Requirements for ITS Applications

This section briefly discusses the radio spectrum requirements for ITS applications. The International Telecommunications Union (ITU) is the international organization, which allocates global radio spectrum for various radio services/applications. International Telecommunication Union (ITU), a specialized agency of the United Nations for all global telecommunication matters, sets out high-level guidance that national bodies adhere to in setting more detailed policy on the management of Radio Frequency Spectrum (RFS). ITU's

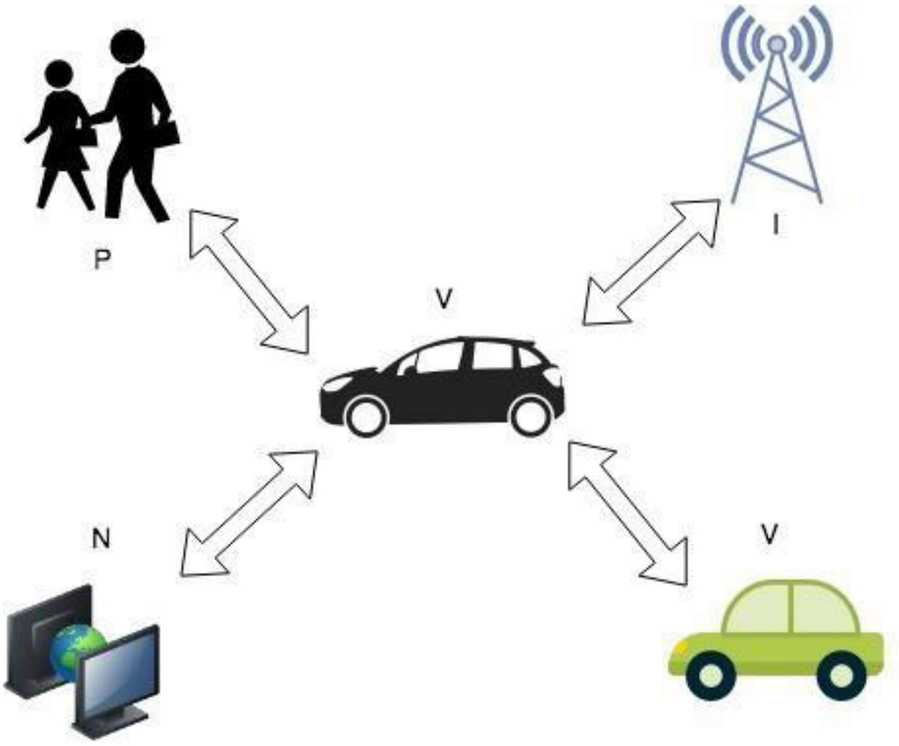


Fig. 6 V2X Communication Modes

Radio Regulations also stipulate how different countries should develop national frequency plans and coordinate with each other particularly in the case of global services, such as satellite etc. The Radiocommunications Sector of ITU (ITU-R) through the World Radio Conferences (WRCs), held typically every 3-4 years, conducts the key parts of radio spectrum management. WRCs are attended by a large number of delegates ranging from spectrum managers, technology developers, academicians and users from all over the world. It may be mentioned that for the sake of better spectrum allocations/management, ITU has divided the world into three Regions, Region 1, 2 and 3 as shown in Fig. 7. Region 1 includes the whole of Europe, Africa, Middle East and north- ern part of Asia, Region 2 covers the Americas, and Region 3, the southern part of Asia, Australia and Oceania.

The Radio Regulations (RR) [17] [18] incorporates the decisions of WRCs, including all Appendices, Resolutions, Recommendations and ITU-R Recommendations incorporated by reference The latest edition of RR is 2016, the majority of the provisions of these Regulations have entered into force from 1 January 2017. Section IV of Article 5 of RR deals with Table of Frequency Allocation (TFA) in frequency range from 8.3 KHz to 275 GHz. TFA elaborates earmarking of different radio services across

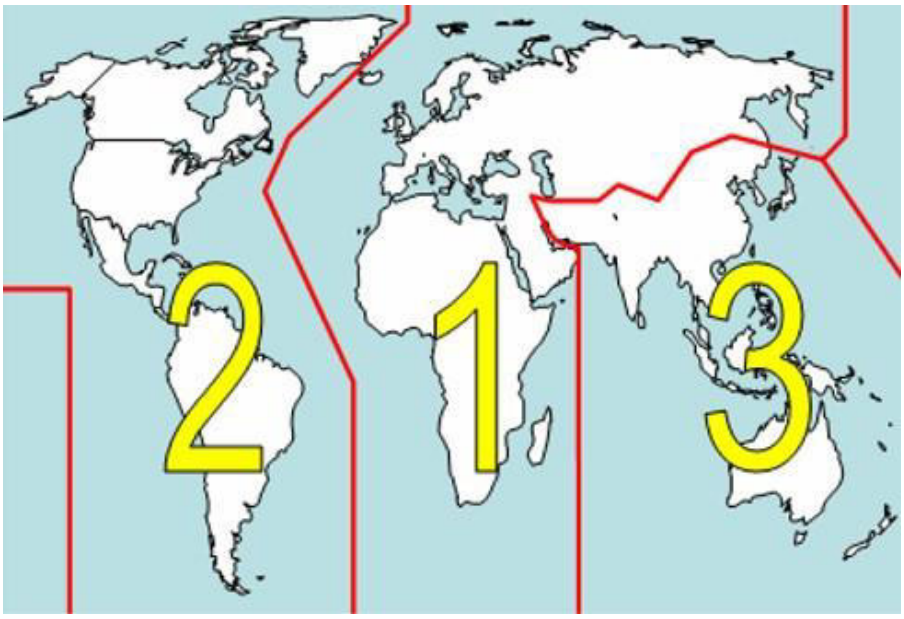


Fig. 7 The Three ITU World Regions.

frequency bands and sub-bands. It may be seen from FAT that in a frequency sub-band, more than one radio service stand earmarked, this situation may vary from Region to Region.

Regarding the need for radio spectrum for ITS [19], some countries are using the frequency band 5855 – 5925MHz. This band stand earmarked for 'mobile' service too. In this band, Fixed Satellite Services (FSS) has primary allocation and systems are globally in use. The sharing studies reveal that there could be harmful interference from FSS earth station to ITS receivers. However, there might be negligible interference from ITS devices to FSS space receivers. Additionally, FSS also has a primary allocation in the band 5850 – 5855MHz. This demonstrates that while ITS applications are planned in an area of operation (AoO), exhaustive sharing studies need to be done for ensuring an interference free environment. This is an example to illustrate the depth of challenges encountered in the radio spectrum management. DSRC operates in the 5.8 GHz band [20]. Asia-Pacific Telecommunications (APT) has also approved this proposal. An active (transceiver) method and a backscatter (transponder) method as DSRC technologies can be exploited for ITS. The bands 5795 – 5805 MHz and 5805 – 5815 MHz are identified for the systems. The reader is referred to several ITU reports that serve as general references for acquiring further knowledge regarding spectrum allocation [21], [22], [23]. Table 1 presents the usages of various frequency bands for ITS applications in various regions/countries. Deployment of radio spectrum of the above ITS radiocommunication can be pictorially be depicted as in Fig. 8.

Table 1 The usage of different frequency bands for ITS applications in various regions/countries

Region 1	
Country or Group	Frequency bands
CEPT	5 855-5 925 MHz
United Arab Emirates (UAE)	5 855-5 925 MHz
Region 2	
Country or Group	Frequency bands
Canada	5 850-5 925 MHz
United States (US)	5 850-5 925 MHz
Region 3	
Country or Group	Frequency bands
Australia	5 855-5 925 MHz
China	5 905-5 925 MHz
Japan	755.5-764.5 MHz 5 770-5 850 MHz
Korea	5 855-5 925 MHz
Singapore	5 855-5 925 MHz
India	5 875-5 925 MHz

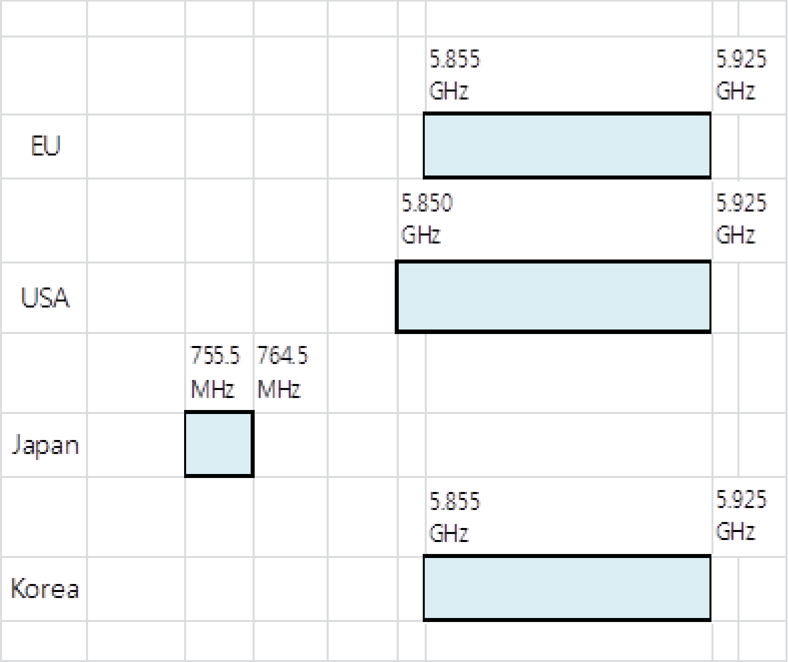


Fig. 8 The usage of different frequency bands for ITS applications in various regions/countries

In accordance with ITU's TFA, the region-wise status of abovementioned frequency bands with regard to 'allocation' for various radio services, is given in Table 2.

Table 2 Allocation of Spectrum for Various Radio Services

Region 1	**Region 2**	**Region 3**
5 725-5 830	**5 725-5 830**	**5 725-5 830**
FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur	RADIOLOCATION Amateur	RADIOLOCATION Amateur
5830-5 850	**5830-5 850**	**5830-5 850**
FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur Amateur-satellite (space-to-Earth)	FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur Amateur-satellite (space-to-Earth)	FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur Amateur-satellite (space-to-Earth)
5 850-5 925 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE	**5 850-5 925** FIXED FIXED-SATELLITE (Earth-to-space) MOBILE Amateur Radiolocation	**5 850-5 925** FIXED FIXED-SATELLITE (Earth-to-space) MOBILE Radiolocation

It may be seen from the above Table 2 that in frequency sub-band more than radio service such as FIXED, FIXED SATELLITE, RADIOLOCATION, Amateur including MOBILE are allocated on primary and co-primary basis. Hence, while making provision for introduction of IT'S under MOBILE service allocations, sharing studies with other radio services would need to be thoroughly carried out.

4.3 Vehicular Collision Avoidance 'Automotive Radar (AR)' Operating at 24.05 to 24.25 GHz, 76-77 GHz and 77-81 GHz

The automotive radar (AR) systems consisting of transmitter and receiver are widely deployed to locate vehicles and pedestrians, in the vicinity of another vehicle. By properly orienting steerable transmitting antenna, the 'objects' with parameters such as distance, speed and direction can be known. AR are broadly categorized into long range (for measuring the distance to and speed of other vehicles), medium range (for detecting objects within a wider field of view) and short range (for sensing in the vicinity of the vehicle required for parking or identifying any obstacle.)

The Federal Communications Commission (FCC) and the Ministry of Internal Affairs and Communications (MIC) in Japan have designated 7 6 -77 GHz band for these purposes. MIC is studying introduction of high resolution radar in 77-81 GHz band. The Russian Federation identified the 77- 81 GHz band for automotive radar. Further, European Conference of Postal & Telecommunications (CEPT) has considered the band 77-81 GHz as the only globally harmonized frequency band for automotive radars. Whereas, the European Commission has decided that for use of automotive radar, harmonization of radio spectrum in the 79 GHz range shall be considered. For the applications of short range radars, ETSI has adopted the harmonized standard in the frequency band 77-81 GHz.

The Frequency band 57.0-66.0 GHz has been proposed for data communications between vehicles and between vehicles and roadside infrastructure.

Table 3 and Table 4 depict region-wise designation/usages of frequency bands in 24 GHz, 57-66 GHz, 76-77 GHz and 77-81 GHz.

Table 3 Region-wise designation/usages of frequency bands in 24 GHz, 57-66 GHz, 76-77 GHz and 77-81 GHz.

Region 1	Region 2	Region 3
24.05 to 24.25 GHz, 76-77 GHz and 77-81 GHz	24.05-24.25 GHz, 22-29 GHz, and 76-77 GHz	24 GHz, 60 GHz, 76 GHz and 79 GHz.

Table 4 Usage status of automotive radars in Asia-Pacific Countries

Country	Frequency band
Australia	22-26.5 GHz, 24.00-24.25 GHz, 76-77 GHz, and 77-81 GHz
China	24.00-24.25 GHz, 24.25-26.65 GHz, 76-77 GHz, and 77-81 GHz
Japan	24.0-24.25 GHz, 24.25-29 GHz, 60-61 GHz, 76-77 GHz, and 77-81 GHz
Republic of Korea	24.25-26.65 GHz, 34.275-34.875 GHz, 76-77 GHz, and 77-81 GHz
Singapore	76-77 GHz, and 77-81 GHz
Thailand	22.00-24.05 GHz, 24.05-24.25 GHz, 24.25-26.65 GHz ,76-77 GHz, and 77-81 GHz
Viet Nam	24.00-24.25 GHz, 76-77 GHz, and 77-81 GHz

4.4 Frequency Usage of Millimeter (mm) Wave Vehicle and Road Radar

In accordance with ITU's TFA, Table 5 depicts the region-wise status of

abovementioned frequency bands with regard to 'allocation' for various radio services.

It may be seen from Table 5 that in the frequency sub-band more radio services such as SATELLITE, RADIOLOCATION, RADIO ASTRONOMY, AMATEUR, AMATEUR-SATELLITE, FIXED, MOBILE, Amateur etc. are allocated on primary and co-primary basis. Hence, while making provision for harmonization of spectrum in the concerned frequency bands for automotive radars, sharing/compatibility studies with other radio services would need to be undertaken for ascertaining interference free operations. It may also be borne in mind that portions of these frequency bands are also earmarked for deployment of International Mobile Telecommunications (IMT).

Table 5 Region-wise status of abovementioned frequency bands with regard to 'allocation' for various radio services

Region 1	Region 2	Region 3
24.05-24.25 RADIOLOCATION Amateur Earth exploration-satellite (active)	**24.05-24.25** RADIOLOCATION Amateur Earth exploration-satellite (active)	**24.05-24.25** RADIOLOCATION Amateur Earth exploration-satellite (active)
57-58.2 EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE MOBILE SPACE RESEARCH (passive)	**57-58.2** EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE MOBILE SPACE RESEARCH (passive)	**57-58.2** EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE 5.556A MOBILE 5.558 SPACE RESEARCH (passive)
58.2-59 EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE SPACE RESEARCH (passive)	**58.2-59** EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE SPACE RESEARCH (passive)	**58.2-59** EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE SPACE RESEARCH (passive)
59-59.3 EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE MOBILE RADIOLOCATION SPACE RESEARCH (passive)	**59-59.3** EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE MOBILE RADIOLOCATION SPACE RESEARCH (passive)	**59-59.3** EARTH EXPLORATION-SATELLITE (passive) FIXED INTER-SATELLITE MOBILE RADIOLOCATION SPACE RESEARCH (passive)
59.3-64 FIXED INTER-SATELLITE MOBILE RADIOLOCATION	**59.3-64** FIXED INTER-SATELLITE MOBILE RADIOLOCATION	**59.3-64** FIXED INTER-SATELLITE MOBILE RADIOLOCATION
64-65 FIXED INTER-SATELLITE MOBILE except aeronautical mobile	**64-65** FIXED INTER-SATELLITE MOBILE except aeronautical mobile	**64-65** FIXED INTER-SATELLITE MOBILE except aeronautical mobile
65-66 EARTH EXPLORATION-SATELLITE FIXED INTER-SATELLITE MOBILE except aeronautical mobile SPACE RESEARCH	**65-66** EARTH EXPLORATION-SATELLITE FIXED INTER-SATELLITE MOBILE except aeronautical mobile SPACE RESEARCH	**65-66** EARTH EXPLORATION-SATELLITE FIXED INTER-SATELLITE MOBILE except aeronautical mobile SPACE RESEARCH
76-77.5 RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)	**76-77.5** RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)	**76-77.5** RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)
77.5-78 AMATEUR AMATEUR-SATELLITE RADIOLOCATION Radio astronomy Space research (space-to-Earth)	**77.5-78** AMATEUR AMATEUR-SATELLITE RADIOLOCATION Radio astronomy Space research (space-to-Earth)	**77.5-78** AMATEUR AMATEUR-SATELLITE RADIOLOCATION Radio astronomy Space research (space-to-Earth)
78-79 RADIOLOCATION Amateur Amateur-satellite Radio astronomy Space research (space-to-Earth)	**78-79** RADIOLOCATION Amateur Amateur-satellite Radio astronomy Space research (space-to-Earth)	**78-79** RADIOLOCATION Amateur Amateur-satellite Radio astronomy Space research (space-to-Earth)
79-81 RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)	**79-81** RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)	**79-81** RADIO ASTRONOMY RADIOLOCATION Amateur Amateur-satellite Space research (space-to-Earth)

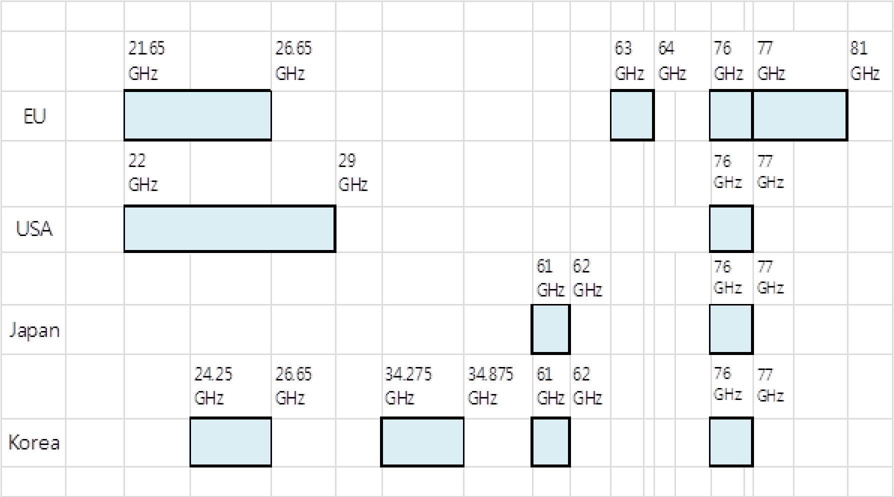


Fig. 9 Frequency Usage of mm Wave Vehicle and Road Radar

5 Security and Privacy in Connected Vehicles

After more than one decade of continuous research, standardization, and trials, Intelligent Transport System is maturing into the application of advanced ICT (including information communication, control, sensing) technologies to road transportation systems, with the objective of enabling information exchange between human, vehicle, and infrastructure, thereby establishing a more efficient, convenient, environmental-friendly, and safer comprehensive transportation system. Various standards have been developed to realize this fascinating technology, ETSI ITS, IEEE 802.11p, Society of Automotive Engineers (SAE) J2945/1, working divergently and yet at the same time converging on to what has become known as V2X communication. It has created an entire eco-system encompasses the connected cars (cars equipped with Wi-Fi, LTE, 3G), roadside infrastructure (intelligent control systems, warning systems, sensors), and communication infrastructure (LTE, satellite, and 5G) so on and so forth uniting the car manufacturers, safety sensor manufactures, regulators, and service providers alike. Essentially, ICT, 5G and ITS join a perfect union providing vehicular communication, autonomous driving, traffic safety, cooperative traffic efficiency as well as taking into consideration for addressing of security and privacy concerns of users using V2X services. As illustrated in Fig. 10, V2X and vehicular communication is not just about vehicle to vehicle any more, it broadly covers all things vehicle, from vehicle to vehicle, vehicle to infrastructure, and vehicle to pedestrian.

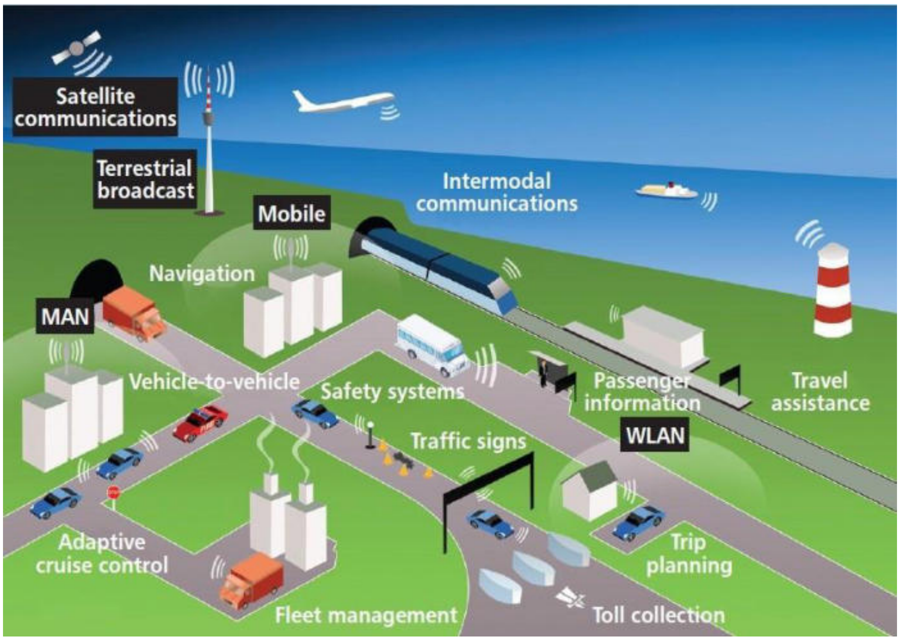


Fig. 10 V2X Communication Use Cases.

5.1 V2X Security Overview - Security of ETSI ITS

Figure 11 illustrates the ETSI ITS security architecture [24] , [25] , [26] , [27] . The security defined in the ETSI ITS (Intelligent Transportation System) standards specifies the main security components, including the security headers, certificate formats and security profiles, protection scheme, and key management details. Because the vehicular communication essentially encompasses of broadcast of messages such as V2V, Cooperative Awareness Messages (CAMs), I2V/V2I, and Decentralized Environmental Notification Messages (DENMs). Security can be viewed as a broadcast protection scheme in the simplest terms. But because of the large number of potential broadcast recipients involved (vehicles and pedestrians), the simple broadcast scheme is not so simple after all. The basic idea behind protection of broadcast messages relies on public key cryptography to provide assurance of both authenticity of the origin and content of the message being sent. The message is first hashed to produce a message hash. The message hash is then encrypted using the sender's private key to form the digital signature of the message. The message along with the digital signature is then sent. Upon receiving the message, the recipients use the public key of the sender to decrypt the digital signature, compute the message hash by hashing the message, if the decrypted signature is the same as the computed message hash, the message is verified as authentic. Using public key cryptography and public key certificates requires additional infrastructure of certificate authority (CA), revocation authority

(RA) and means to management certificates on a large scale. In addition to the authenticity of the message (i.e. integrity), the message can also be protected by a combination of symmetric key algorithm and public key algorithm.

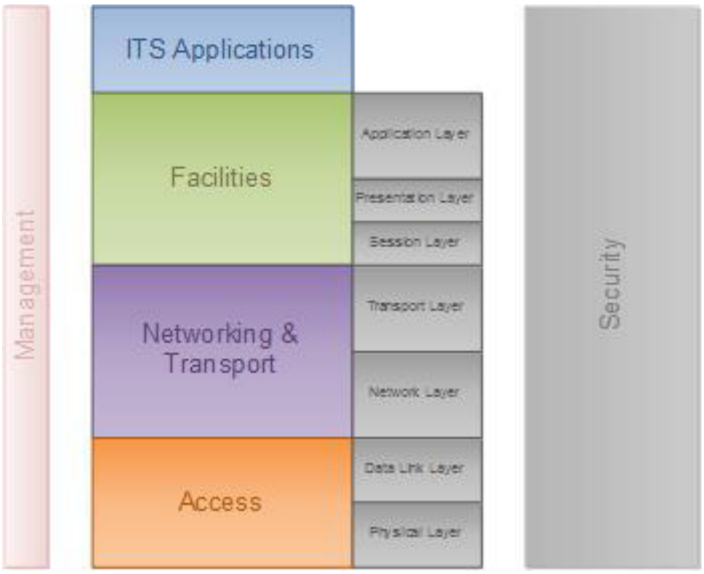


Fig. 11 ETSI ITS Security Architecture

The certificate management issues are complex and require a single global CA or a series of interworking regional CAs in order for the scheme to work because cars are expected to move across regional and possibly national boundaries. Details of these management issues (including certificate provisioning, certificate revocation, certificate update, key management, etc.) are left out for the readers to explore further.

5.2 Security of IEEE DSRC WAVE

Figure 12 illustrates the application level security for the 802.11p system which is based on IEEE 1609.2 DSRC WAVE [28] , with some aspects further defined in SAE J2945/1 [29] . Essentially, it is quite similar to ETSI ITS in that the security is provided to integrity-protect (most of the time) broadcast messages making sure that the messages are signed to ensure that they come from authorized senders and that the messages are unaltered upon receipt by the recipients. IEEE 802.11p also uses the same public key cryptography concept to provide the protections and will have the same issues to deal with, namely the same issues with regard to the management of certificates.

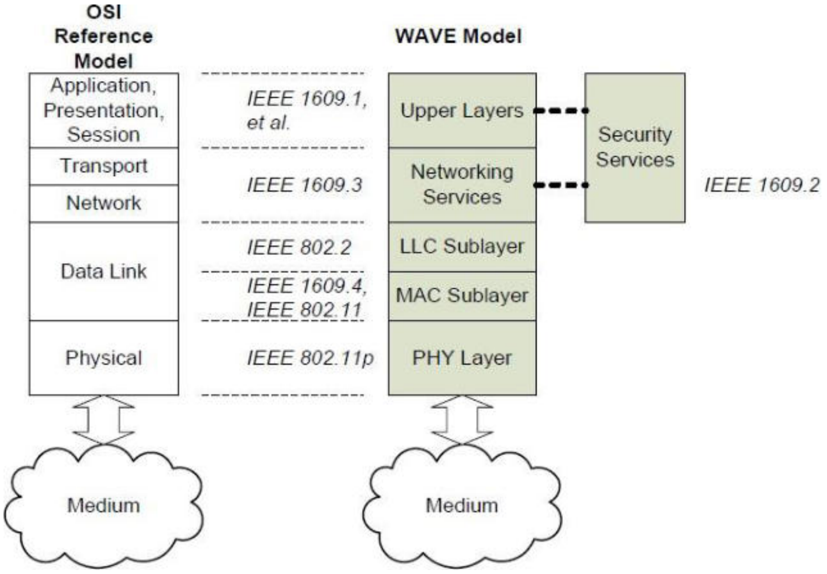


Fig. 12 IEEE 1609.2 Security for V2X Application

5.3 Harmonization of ETSI ITS and DSRC WAVE

As V2X and 5G heat up, the vertical community and Standards Developing Organizations or SDOs (IEEE, ETSI, ISO, SAE, etc.) responsible for the working on the divergent standards have decided to harmonize the two approaches toward a single set of standards, with possible flavor to take into consideration for regional requirements. It turns out that the difference is not that divergent after all. Efforts have been made to considerably to harmonize the various aspects of the standards, including architecture (using the ETSI ITS architecture in Figure 11 as a base), protocol stack, use of media, frequency and channel coordination, congestion control, communication protocol as well as security.

The security before the harmonization is already quite aligned, for example the protection scheme, the use of public key algorithms and symmetric key algorithms of Elliptic Curve and Advanced Encryption Standards (AES) encryption algorithm, security message formats, etc., although the main difference is in where the layers these security services operate cryptographic details, and efficiency optimizations. At a high level, there is very little difference between the two main competing standards in terms of providing security capabilities as a whole with the goal of providing protections to the array of messages that are mostly sent in broadcast mode. In the case of ETSI ITS specifications, the security is applied to the messages at the geo-networking layer, a network layer protocol specifically defined in the ITS framework that provides packet routing in an ad hoc network by making the use of geographical position information available for packet transport, while IEEE DSRC WAVE specification applies security to messages at the application sub layer. Fig. 13 and Fig. 14, respectively, depict the ETSI ITS and IEEEE DSRC security message formats.

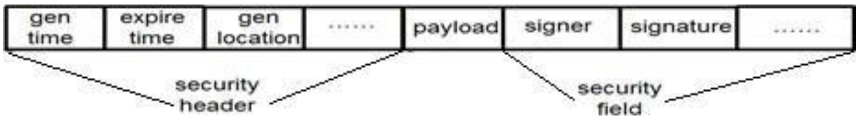


Fig. 13 ETSI ITS Security Message Format

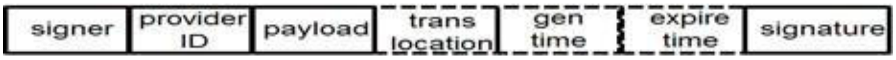


Fig. 14 IEEE DSRC Security Message Format

This make the SDO that specifies 5G standards much easier to have a single standard. To this effect, 3GPP has already finalized the work to be used in LTE, starting with cellular V2X in Release 14.

5.4 3GPP V2X security

Requiring a vast telecommunication network (e.g. LTE, IEEE 802.11-based, satellite communication, mesh networks, etc.) to provide the needed communication among cars, people, sensors, and various infrastructure components, various standards bodies have envisioned V2X as an application layer add-on to support the functions and features that are necessary to provided services for the various use cases that are constantly evolving. The most basic of these uses are providing communication (broadcast messages) of road safety to vehicles, and pedestrians by, for example, sending timely warnings to pending hazards or accidents. Because of the need for an underlying communication, V2X needs a reliable and secure transport mechanism to carry the information between all stakeholders as part of the eco-system of V2X communication. Such a transport network can be easily realized using the LTE networks that is now ubiquitous around the world. Various standards that have been evolving for the past 10 years, starting with the 802.11P standards, WAVE, DSRC, have now just about merged into one standard, giving the vertical industry in the automotive landscape the leverage, unity, and interoperability needed to ensure that the V2X communication a success story in terms of sustainability and commercial viability.

Though V2X communication technology was originally developed as an application layer add-on, the underlying technology that can support the communication requirements is unmistakably wireless such as IEEE 802.11-based

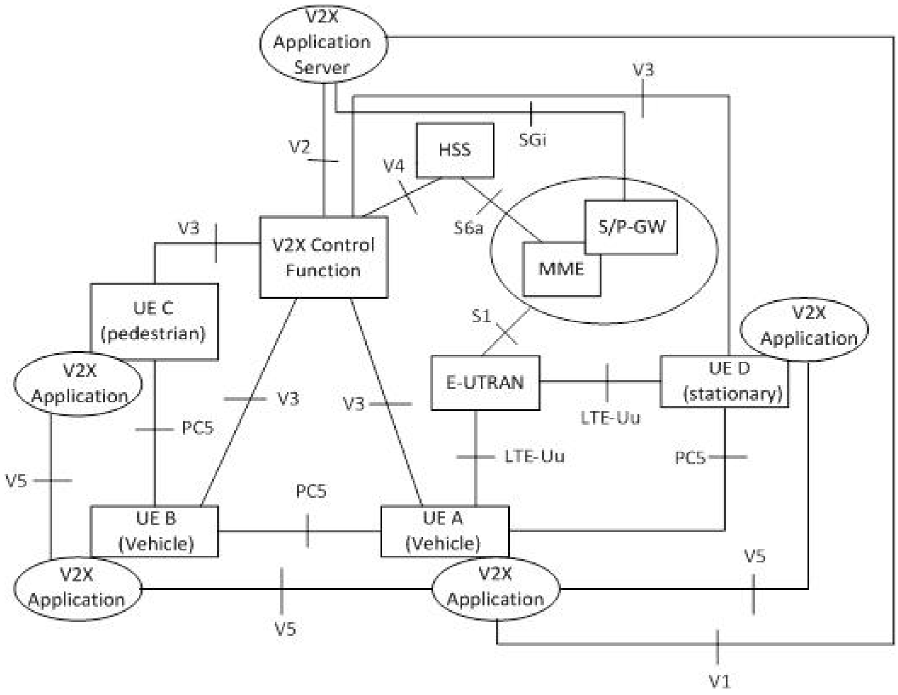


Fig. 15 LTE-based V2X Security Architecture

or LTE and with the advent of 5G, it will not only make the communication more secure, but it will also make it more reliable, fully taking advantagesof the benefit of 5G. The architecture that has been defined in 3GPP is an overlay of the LTE network that can be fully integrated into the existing infrastructure. Security and privacy requires not only security and privacy functions, but also provisioning and management of the user credentials, identities, keys and certificates for those functions.

Figure 15 depicts the LTE-based V2X security architecture [30] where new network elements and interfaces are incorporated or defined into the architecture to support the new V2X services:

V2X Application Server: It is the logical function that is used for network related actions required for V2X services. The V2X application server can be either within the 3GPP operator domain or in the domain of the applications that provide V2X services (e.g. third-party service provider).

V2X Control Function: It is the logical function that is used for network related actions required for V2X, such as the use of 3GPP defined Generic Bootstrapping architecture for protecting the provisioning of UEs (User Equipment, e.g. handset or a terminal) with security and operational parameters either from internal to the LTE network or interfacing between the V2X ap- plication server and the UE, handling of any security related capabilities from the network perspective. This functions draws parallel to the control function that has been defined for proximity services (e.g. ProSe) that provides device to device communication for public safety purposes.

PC5 interface: It is the interface that provides direct communication capabilities between UEs that are capable of receiving and sending V2X communications.

Uu interface: It is the newly defined interface between the UE and the LTE network that is still needed to run LTE-based security such as user authentication even if the UEs rely exclusively on application for V2X security.

Though most of the security privacy features are standardized as defined in 3GPP, it offers added capabilities with additional layer of over-the-air security provided in LTE, which offers secure credential provisioning and management, and inherent physical layer aspect that provides efficient use of resources (e.g. scheduling of transmissions, broadcast nature of over-the-air communication). Consequently, the combination of LTE security and application security in V2X applications and services can provide security unmatched by the security of each layer alone.

5.5 Privacy in V2X

Regulators and operators are so concerned with the privacy of the users (e.g. location privacy, personal data privacy) and concerned with the upcoming more stringent data privacy regulations that they have put in strong requirements to protect the privacy of users of the system. So much so that 3GPP has consolidated the input from the regulators and operators into a very strong privacy requirement, namely that “it shall not be possible for a single entity (including third parties and operators) to be able to track a user over an extended period of time”, for example by looking at the V2X messages or by linking the identity of the user to a temporary identity or a pseudo identity.

Because V2X messages can be either application layer messages or 3GPP-based messages sent on the PC5 interface, let us look at how privacy is addressed on the PC5 interface. The entities that could potentially track a particular UE based on V2X messages transmitted in a region are other V2X UE (e.g. a car or another non-car UE who is V2X-capable) and V2X infrastructure (including road side controllers or operator’s network entities). Since tracking an UE on either the application layer or on the 3GPP layer is typically done by intercept the unencrypted V2X broadcast messages sent by that particular UE, recovering the identities (e.g. UE identity, vehicle identification number, driver/user identity, temporary or permanent 3GPP identities) used in transmitting the V2X message and associating these identity to a single UE. But because many of these identities are changed as per the standards requirement, for example 3GPP V2X security standards specifies that “The UE shall change and randomize the source Layer-2 ID, and the source IP address (in case of IP-based V2X communication) when indicated by the V2X application that the application layer identifier has changed.”, the constantly changing of identities (via directly changing the identities or via use of short term certificates) certificates that the potential attacker recovers would appear to be either random or unrelated UEs and therefore making tracking nearly impossible, even to the determined attacker.

In the case of ETSI ITS or IEEE WAVE/DSRC, the identities are part of the certificate that is used to sign the message are either pseudonymous, the identities are buried in the message payload are temporary, or the message (payload and security headers) simply do not contain any privacy sensitive data. Intercepting these messages would not net the attacker any valuable information that can be used to correlate to a particular user or driver that is tractable.

In either case, the use of these mechanisms to update the identities frequently or use of short term or pseudonymous certificates work well in the characteristics of the V2X operational model as the V2X client (e.g. a vehicle) are almost constantly moving. Regardless of the security mechanisms of these privacy features, privacy of the users can be achieved, even at the phase of upcoming stringent data privacy requirements. However, it is generally always a good practice to make users aware of the privacy implications when they agree to use V2X services, and to seek their consent (e.g. opt-out) so that both operators and users have the common understanding as to what the expectations are.

5.6 V2X: Perfect marriage of telecom and vertical industry

The strong use case for connected cars, driverless cars, vehicular safety, pedestrian safety, efficient transportation, and endless possibility to offer value added services to the users is making V2X services more and more mainstream. By combining application security developed by ETSI ITS, IEEE DSRC/WAVE, and the security developed by 3GPP, V2X is a perfect example of how LTE and 5G is embracing the vertical industry to make a success story, a success story of an eco-system that extends beyond the traditional telecom vendors, operators, and regulators. As 5G is looming, the stakeholders in this eco-system are working more and more closely to expand and perfect the technology, making it as ubiquitous as communication services and accessible to everyone.

References [24] through [30] shed further insights into the aspects of V2X security and privacy.

6 Cyber Security Issues Relevant to Connected Vehicles

Connected cars consist of a vehicle with electronic control units (ECUs) and an in-vehicle network, a portal to provide the vehicle with various services and a communication link to connect the vehicle and portal. [31, 32] As such connected vehicles are pervasive computing environments and as such are potentially vulnerable to attack. Checkoway et al. [33] analyzed the external attack surface of a modern automobile. They discovered that remote exploitation is feasible via a broad range of attack surfaces (including mechanics tools, CD players, Bluetooth, and cellular radio). Moreover, wireless communications channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft.

Vehicles also communicate with each other using among other methods automotive radar which is used for adaptive cruise control, forward collision warning, or blind spot detection [34]. Many vehicles will be connected using DSRC, a wireless communications standard that enables reliable data transmission in active safety applications [35]. Wireless communication used by cars is also increasing. Each technology, however, comes with its own security risks.

6.1 IoV Security and Privacy

A vehicular network consists of a large number of distributed heterogeneous resources and computational functionalities. The distributed and heterogeneous nature of vehicle ad hoc networks (VANETs) makes security a significant technical challenge [36]. Vehicles in VANETs broadcast unencrypted messages that contain a vehicle identifier together with the vehicle's location, speed and di- rection. From this information a driver profile may be developed that may be used for legitimate reasons such as providing emergency services and law enforcement, as well as a range of illegitimate reasons such as surreptitious surveillance by employers, insurance companies or criminals [37].

VANETs have led to an important trend for the automotive industry, namely context awareness. Context awareness implies that a vehicle is aware of its environment (including the activity and location of other vehicles) [38]. In order for such a network to operate, it is necessary for vehicles to exchange information with each other. For the typical driver, understanding how personal data is being used and expecting them to provide meaningful consent on how their personal information is used is becoming increasingly unrealistic.

It should be noted that cars are personal devices that are usually kept for a long time. They are increasingly storing considerable amounts of personal information that can be used alone or with other data in order to reveal the identity of an individual driver. Dotzer warns that "[a] very dangerous and often ignored fact about privacy is that innocent looking data from various sources can be accumulated over long period of time and evaluated automatically" [39]. However, privacy regulation depends crucially on determining whether a company is dealing with identifiable, and therefore personal information, within the meaning of the privacy regulation and whether the information is anonymous and therefore non-personal information that is not caught by legislation. This is the source of considerable uncertainty for parties dealing with vehicle data.

6.2 Trust and Repudiation Management

The fact that vehicles communicate with each other gathering and disseminating the information within a dynamic network necessitates the requirement of trust. Trust plays an important factor in the viability of networked technology. Frenk et al., examine trust in connected vehicles with respect to the acceptability of the decisions automated vehicles make [40]. They tested the system on 57 participants and concluded that systems sharing user goals (i.e. providing description/reason while taking a decision) are more trustworthy to the users. This implies that user acceptability is correlated to the transparency of the actions taken by autonomous vehicles.

Kaur et. al., also identify trust to be a vital barrier in the adoption of smart cars [41]. They tested the adoption of smart vehicles based on the various factors including trust, privacy, and security, and presented that reliability is directly proportional to the trust factor building in connected vehicles.

Since the network in connected vehicles is dynamic where information changes within seconds, the trust may only be valid for a very short period of time. Moreover, the trust in connected vehicles is subjective; what one thinks as safe to be trusted, other might not think the same. Therefore, there is a need of consensus system in making trust decisions such as recommendations and ratings to choose an option with the minimal risk. The basic goal is to build a trusted network where every node could trust on other nodes and this is where repudiation becomes important.

If we could identify the trustworthy nodes with the network, we can establish a trust system with them and knock out the nodes that seem untrustworthy. An effective approach to this problem might be achieved via unique identifiers of vehicles such as electronic license plates and the positive or negative ratings associated with them. We might then rely on the ratings of vehicles to establish the kind of trust in its particular context within the network. This might give rise to cold start problems where there is not enough data to produce a recommendation or give a rating, but could be solved using artificial intelligence techniques or other solutions to cold start problems. However, the security of the identifiers i.e. license plates must be considered to avoid repudiation of recommendations being given by the nodes.

Ltifi et.al., presented “Active Vehicle” which used Petri Nets to enable the vehicles to evaluate the trustworthiness of communication between other vehicles in real time [42]. They particularly focused on the scenario where an accident occurs and a vehicle transmits a warning message to other vehicles. In this case, vehicles would be able to accept the message after performing the evaluation on trustworthiness of the message. The paper suggests a similar concept as platoon, but with a difference that every vehicle enters into a session to create/join a network and broadcast a hello message to all vehicles in the network. At that point, trust level evaluation is performed and connection is established and a message of ‘bye’ is broadcast to other vehicles as soon as the vehicle exits the network. This however, puts high reliability requirements in the network connection.

Kerrache et. al., describe the existing security solutions to be focused on two main categories: trust and cryptography [43]. They presented a survey on existing trust management solutions in connected vehicles and claimed that cryptography solutions might not work in high mobility areas and hence trust management between VANETS is mandatory. They described trust management as an additional security solution which can act successfully when cryptographic solutions do not work. However, such system should be context-aware in order to successfully run.

6.3 Social and Ethical Issues

Intelligent transport systems will enable social interactions among vehicles, among drivers and between infrastructures and drivers/vehicles/pedestrians. The fact that vehicles will increasingly connect with each other and with public networks (e.g. V2V, V2I) make it inevitable that nodes will exchange neighbourhood information on a regular basis. Thus in the context of the social internet of vehicles we will increasingly become concerned with privacy harms among users of the network. It will be necessary to determine in advance the degree of privacy that is appropriate in the circumstances and design the system accordingly. An important task is to devise appropriate privacy preserving protocols, which are typically based on anonymity schemes, relying on temporary pseudonyms. Most of the privacy threat scenarios in relation to VANETs are related to position identifiers.

To guard against unauthorized use of data, the system's security architecture must be very carefully designed, especially if it is deployed between countries. Hubaux et. al. have argued that because of the information it will protect, registration authorities must devise an appropriate Public Key Infrastructure. They write that "this challenge is equivalent to securing credit cards or mobile phones, but it also includes newer, more difficult problems: it must embed security features in stringent real-time protocols such as those used to prevent accidents, secure physical location and distance, and support communication within highly sporadic groups of participants." [38]

7 Emerging Research Relevant to IoV

7.1 Cloud Based Secured VANET with Real-Time Access to IoV Applications

Recent advances in IoT and ITS have paved the way for the onset of intelligent connected vehicles. Aided by the various sensors and Internet of Things mounted on them, the connected vehicles are now capable of gathering enormous amount of data, as much as 1.4 to 19Tbyte/hour [3], from the ad hoc vehicular environment. The data collected can then be processed and useful information extracted using machine learning or other such tools can then be shared with drivers, other connected vehicles in the ad hoc network, and other infrastructure as well as applications so as to engineer an environment for safe driving [44]. With autonomous vehicles, IoV will have the intelligence, and learning capabilities to anticipate the drivers' intentions and, with the help of the information available, can take smart and safe decisions so as to facilitate a safe driving environment. By integrating cloud computing with VANET [45], machine learning applications and other novel multimedia applications and services can be developed that can avail of the computing resources available to them. Autonomous and connected vehicles will then be able to offer to the drivers increased accessibility to multimedia services, novel cloud based applications, and enormous computing power [46]. This document proposes such an architecture for cloud based VANET that enhances resource management.

Many emerging IoV applications, such as real-time video sharing [47], require larger bandwidth, secure storage, complex computation, enhanced resource management, cloud-based dynamic bandwidth sharing [48], and social media sharing [49], [50]. VANET's connected vehicles continuously collect data related to real-time traffic, driver behavior, road condition, and bandwidth utilization [51], and upload the data to the cloud servers for further processing. The machine learning tools executing in the cloud serves may then mine useful information that can help in improving driver and vehicle safety, easing traffic congestion, and enhancing driving comfort. The cloud servers may then transmit the mined information to data centers for further processing and share the information with the connected vehicles of VANET for safe route optimization. Due to the availability of mined information, it is possible to reduce traffic congestion, and, consequently, traveling duration. The process of Big Data mining transforms a VANET into a smart VANET [52], [53].

The vehicle sensors gather information like GPS location, vehicle health conditions, roadside businesses, driver behavior and road conditions and upload to the cloud based so that the information mined from the data can be utilized to optimize the performance of vehicles and improve the safety and comfort of drivers, passengers, and pedestrians [54], [55]. The IoV applications in cloud based VANET will provide virtual connectivity between vehicles and hence among drivers or passengers. They can also share their interests and manage their resources during trips [56], [57]. In cloud based VANET, the autonomous vehicle and non autonomous vehicles can efficiently participate to maintain smooth traffic flow in urban areas and highways. Network operators can manage the bandwidth requirements of the vehicles in an efficient manner as well.

The autonomous vehicle systems are expected to be complex systems that will empower a new generation of reliable applications and services using the cloud based VANET architecture. Cloud based VANET resource management system will rely on a large ecosystem of autonomous vehicles systems where collaboration at large scale will take place. This is only possible due to the distributed, autonomous, intelligent, proactive, fault tolerant, reusable systems, which offer their capabilities and functionalities as services located in the "IoV service cloud".

Ref. [58] discusses integrating cloud computing with vehicular ad hoc network (VANET) so that the vehicles can share network resources and avail of a variety of information collected by them to make useful decisions. The paper proposes an architecture that includes a cloud-based VANET and studies an application management system for this cloud-based Internet of Vehicles (IoV). This architecture facilitates the recognition of available resources in real-time. In addition, it provides cloud-based IoV applications to cloud-based VANET enabled vehicles. The paper proposes a distributed security methodology to facilitate secure communication within the cloud-based vehicular network. The paper also demonstrates the potential of the cloud-based VANET architecture to facilitate real-time access to IoV applications.

Cloud platforms provide essential services and applications to support connected vehicles. Cloud infrastructure consist of distributed computing, storage and networking resources. This infrastructure needs to manage and process at scale enormous amounts of data, for an autonomous car over 2Gbps [59]. [60] has gone one step further in proposing an architecture for Vehicular Cloud Computing, where each vehicle infrastructure is provided as a computing resource.

Ref. [61] analyzes the different formations that can be considered in Vehicular Cloud Computing scenarios. Stationary vehicular cloud formation can be provided through parked vehicles, through shared computing and storage resources. Another scenario consists on the provisioning of vehicular cloud computing through fixed infrastructure, such as RSU. Finally, dynamic formation allows the formation of autonomous vehicular cloud.

In order to describe the benefits of cloud-based IoV, various services and applications are presented. Primary services provide the grounds for allocating cloud-based IoV applications [62]. These services can be classified in well known categories, such as Network as a Service (NaaS) and Storage as a Service (STaaS), or novel services such as the following. Cooperation as a Service (CaaS) focuses on subscribing and announcing important information to the network, with the purpose. Similarly, Information as a Service (INaaS) considers the acquisition of information for safe driving. Entertainment as a Service (ENaaS) focuses on entertainment facilities. Computation as a Service (CompaaS) provides computing resources on stationary vehicles. Finally, Pictures on a Wheel as a Service (PicWaaS) provides distributed shots of a given position in order to help for forensic and insurance claim purposes.

Several applications can beusefully run in a cloud-based platform. These applications include [61]: Traffic Information, Accident Alert, Evacuation, Road Safety and Managing Parking.

7.2 AI/ML-based Spectrum Management for Connected Vehicles

In the era of explosive growth of multimedia applications and services, with the onset of new autonomous vehicles, the future presents an excellent opportunity for telecom, automotive, IoT and OEM industry. This opportunity requires an advanced management of available spectrum and a new mindset amongst wireless service providers that calls for reallocation of available spectrum resources to reposition them in the next-generation of connected vehicles technology market. Establishing communication among autonomous vehicles for long period with very little delay poses a formidable challenge. Ref. [63] proposes a decentralized approach to spectrum management amongst multiple operators. Each operator collects and evaluates data about autonomous vehicle user and manages spectrum allocation independently. So, the 3 objective is to create an algorithm for optimal spectrum utilization and synchronization with other operators. This paper proposes an AI-based, linear programming and game-theoretic approach to cooperation between, and distributed spectrum management by, multiple wireless service providers (WSPs'). This paper also explores the need for such a system that employs a suitable artificial intelligence mechanism that may provide a better solution to the problem of spectrum management. Based on the results obtained from simulations, the paper shows that artificial intelligence mechanisms improve spectral utilization in comparison to the traditional methods for spectrum allocation. The paper claims that the AI mechanism proposed provides the theoretical principles for formalizing the complex interrelations between the wireless service providers and it may lead to the formulation of effective policies for autonomous vehicles.

7.3 Blockchain-Based Security for Connected Vehicles

While connected vehicles technology is experiencing phenomenal growth in the auto industry, it is still studded with many security and privacy vulnerabilities. Today's IoV applications are part of cyber physical communication systems that collect useful information from thousands of smart sensors associated with the connected vehicles. The technology advancement has paved the way for connected vehicles to share significant information among drivers, auto manufacturers, auto insurance companies and operational and maintenance service providers for various applications. The critical issues in engineering the IoV ap- plications are effective to use of the available spectrum and effective allocation of good channels in an opportunistic manner to establish connectivity among vehicles, and the effective utilization of the infrastructure under various traffic conditions. Security and privacy in information sharing are the main concerns in a connected vehicle communication network. Ref. [64] proposes an approach imparting privacy and security using the blockchain technology to facilitate se- cured communication among users in a connected vehicles network. Originally, blockchain technology was developed and employed with the cryptocurrency, Bitcoin, to provide increased trust, reliability, and security among users based on peer-to-peer networks for transaction sharing. In this paper, the authors propose to integrate blockchain technology into ad hoc vehicular networking so that the vehicles can share network resources with increased trust, reliability, and security using distributed access control system and can benefit a wider scope of scalable IoV applications scenarios for decision making. Blockchain technology allows multiple copies of data storage at the distribution cloud. Distributed access control system is significantly more secure than a traditional centralized system. The ad hoc vehicular networking may become one of the most trendy networking concepts in the future that has the potential for the development innovation applications that can benefit the society with secured applications.

7.4 The Role of Artificial Intelligence and Machine Learning in the Evolution of Connected Vehicles

The use of artificial intelligence (AI) and machine learning (ML) is aimed at improving the protection and efficiency of vehicles and drivers of existing transport systems through access to information among connected vehicles. AI plays an important role in autonomous driving through the development of the driving actions of human beings. A few AI techniques are: Swarm Intelligence, Expert Systems, Evolutionary Algorithms, Inference, Fuzzy Logic, and Machine Learning. The paper by Tong, et.al., provides a survey of AI techniques for connected vehicles [65].

7.4.1 Swarm Intelligence

The collective actions of self-organized and decentralized systems can be defined as swarm intelligence. The term Swarm Intelligence (SI) was first introduced in [66] for the cellular robotic systems. A population of vehicles communicating among connected vehicles locally with each other and their environment exhibits swarm intelligence, thus defining a new paradigm of connected vehicles. The vehicles follow straightforward rules without a control system. Swarm intelligence is the basis for the action of ants-colonies, flocks of birds, fish schools, animal herding, intelligence and bacterial development. A group of ants was given two paths (short and long) in an experiment carried out by Deneubourge in 1990, linking their nest to the food site [67]
. From their findings, it was found that, eventually, the ant colonies were most likely to choose the shortest trail collectively [68]. The most commonly known techniques of the application of swarm intelligence are: 1) Particle Swarm Optimization (PSO), 2) Ant Colony Optimization (ACO), and 3) Swarmcasting.

7.4.2 Machine Learning (ML)

Reference [69] provides an ML framework for intelligent vehicular networks. A substantial part of AI is covered by ML. ML techniques can be classified into three categories: unattended learning, supervised learning and strengthened learning. Other ML structures, such as online learning and transfer learning, can be classified along the three basic ML schemes. ML consists essentially of two main phases: training and testing. A model is trained in the training process based on practical data. Based on the learned model, predictions are then made in the testing process. Machine learning methods are divided into three categories i.e., supervised, unsupervised, and reinforcement learning.

In supervised analysis, the Artificial Intelligence (AI) network is used to find a map function to map input data into output by using an input and target value dataset. Supervised learning is further divided into classification and regression. Linear regression, vector support, and random forest constitute some common examples of supervised learning.

There is no guidance available in unsupervised learning, only an unlabeled and unclassified input dataset is given and used to train the AI network in connected vehicles to find hidden patterns, responses, and distributions. Clustering and association are various forms of unattended learning problems. The k-means and self-encoder algorithm are only a few examples.

The Markov Decision Process (MDP) [70] provides the basis for the majority of the Reinforcement Learning (RL) problems. The goal of the MDP is for sequences of decisions (SDPs) to be optimized. For stochastic SDPs, an MDP cannot provide absolute solutions, but it can contribute to providing the best solutions among all possible solutions. A model of MDP is defined by a number of states, a number of acts, a transition model and a recompense function. The current condition, the behavior chosen, and the following outcome depend on reward and change. Based on its multiple experiences with the given context, the RL agent's objective is to maximize its long-term aggregate reward in connected vehicles. The part of the RL algorithm is known as an agent that does interactions and learns. This target was accomplished by an agent by an optimum strategy. A policy is a series of actions for a given set of states and one that maximizes the total long-term reward is an optimal policy. The crucial task for an agent is to take advantage of the actions already identified and, at the same time, to discover new actions that can offer a better incentive for the best actions that are currently taking place. In the RL setup, the balance between discovery and exploitation is a key problem, i.e. a balance between optimizing reward from established movements or looking for new horizons that might even yield a better result. RL algorithms can generally be split into two groups, i.e., model-based and model-free. Model-based RL algorithms use the approximator function and are known to be effective for samples. A significant problem in the RL context, however, is generalization of model-based algorithms for probabilistic and complex models with large dimensions. The value function, policy search, return function, and transition models are different techniques for solving model-based RL problems. The model-free RL algorithms are Monte Carlo (MC) and Temporal Difference (TD). Examples of the TD processes are the Q-Learning and SARSA strategies that stand for State Action Reward State Action. Dynamic programming (DP), developed in the middle of the twentieth century by Richard Bellman, provides an approach to solving optimization problems. DP is a recursive method which, in simpler and smaller problems, sequentially breaks down a complex task. The approach to DP is model-based, requiring complete measurable environmental awareness.

In some RL problems where the environment model is an MDP model, DP is used to find an optimal strategy by using the Monte Carlo (MC) method of value iteration or strategy iteration. The Monte Carlo (MC) method uses randomness for problem solving. Two different MC techniques exist. First-Visit MC is the average of returns during a set of episodes by following the first visits to a state while the Every-Visit MC is the average of returns after all visits to a state during a set of episodes. The key advantages of MC over DP are: i) its applicability for sample models. (ii) ease of efficient and rapid implementability, and (iii) ability to learn optimal solutions through direct interaction.

Q-learning [71] is a TD algorithm of model free, off policy and forward learning for control in connected vehicles. By using off policy, i.e. learning by observation, the Q-learning algorithm learns the optimum policy. The next behavior is chosen in Q-learning for the next state's maximum Q-value, which is a greedy policy, and it does not obey the current policy, i.e. it is off-policy learning. By using eligibility traces, we can also speed up convergence in Q-learning. In the case of discrete acts and a large number of repeated states, the prior protocol efficiency becomes low. Most often, function approximations are required by the Q-learning technique. The technique of actor-critic is based on common RL algorithms. It is a hybrid approach consisting of functions and policies of importance. The critical part of the algorithm estimates the value function, while, in compliance with critical input, the actor updates the regulation.

This type of methodology stands between methods based on policy and methods based on value; i.e., it estimates both the role of policy and value. It refers both to small spaces of state-action and large spaces of action-state. Myopic and Thompson Sampling are a few popular methods used for Bayesian approximations. Thompson sampling can be used for solving the problem of exploration-exploitation. In particular, the Deep Q Network TD algorithm Q-learning is one of the commonly used algorithms in RL, but in broad state space it has a lack of generality problems. In Q-learning, for instance, we store the Q table in a two-dimensional array. Visiting and estimating the value function for all states is difficult for environments with broad state space and much related behavior. It is possible to address the problem of generalization with the implementation of RL based on neural network for function approximation. To estimate the value function in large-state space, the Deep Q-Network (DQN) uses a Neural Network. The training of the network is done by using the Q-learning update rule [65].

Deep Learning (DL) [72] is closely connected to the three ML groups above. Implemented in several layers, it is a deeper neuron network that aims to extract information from the data representations in connected vehicles that can be produced from the three ML categories previously discussed. The network consists of three types of layers: an input layer, several hidden layers, and an output layer. The network's ability to learn improves as the number of hidden layers improves. After a certain stage, however, no improvement in output is provided by any increase in the number of hidden layers. Training a deeper network is also difficult because it requires extensive computing resources and network gradients can burst or disappear. The deployment of these resource hungry deeper networks has raised the importance of edge computing technology. Vehicles on the move can benefit from mobile edge computing servers.

7.4.3 Open Source Tools or Implementing AI-Based Connected Vehicles Applications

There are quite a few open source tools that can be used for AI based connected vehicles applications.

TensorFlow, developed by Google, is one of the most common tools [73]. For a variety of AI duties, it is a software library for data-flow programming. It has been widely used in autonomous vehicular systems for deep learning networks. Tensorflow runs on multiple CPUs and Graphical Processing Units (GPUs), .

Apache Spark is a cluster-computing distributed general purpose system [74]. It offers an interface for whole clusters to be configured. Spark core uses an application programming interface such as Java, Python, Scala, and R to provide distributed task dispatching, scheduling, and simple I/O functionalities. Spark cloud computing is gaining immense use of vehicular edge computing. This is because it is possible to use Spark in conventional data centers and in the cloud.

Scikit-learn is a library for Python based on free ML [75]. It features different algorithms for classification, regression and clustering, making it a great candidate for connected vehicles scenarios for ML applications. Support Vector Machine (SVM), random forest, gradient boosting, k-means, and Density- Based Noise Application Spatial Clustering (DBSCAN) are the algorithms used.

Scikitlearn tools for connected vehicles simulations can be readily imported by a recent Python and NS3 based application known as PySNS3. The Scikit, or SciPy Toolkit, is written in Python with some algorithms written in Cython faster [76].

Another Python open source library used for applications such as natural language processing is PyTorch [77]. It was created primarily by the research group Facebook AI and the software team "Pyros" of Uber. It offers high level features such as Deep Neural Networks (DNN) built on a tape-based autodiff framework, Tensor computation with heavy GPU acceleration. Tensors are multidimensional arrays that can be computed on Nvidia's Compute Unified System Architecture (CUDA) toolkit-supported graphics processing units (GPUs). PyTorch, since it uses a system called automatic differentiation, is a powerful candidate for vehicular cyber social computing. This system tracks what tasks have been done, and then it replays it for gradient computing backwards. In order to save time on an epoch by measuring differentiation of the parameters at the forward pass itself, this technique is also effective when constructing neural networks.

Big traces of vehicular data can also be analyzed effectively using another important method known as H2O [78]. As part of exploring data patterns, it helps users to suit thousands of possible models and can be run using R and Python. It is used to explore and evaluate large databases, such as the Apache Hadoop Distributed File System, maintained in cloud storage systems. Huge datasets of vehicular traffic are too broad to examine using conventional tools such as R. H2O therefore offers data structures and methods that are acceptable for this form of data generated by connected vehicles. H2O comprises statistical algorithms such as clustering K-means, generalized linear models, distributed random forests, machines for gradient boosting, naive Bayes, and PCA, etc. H2O utilizes iterative techniques that use all the data of the vehicular customer to provide quick responses. The computations can be interrupted by a vehicular client running out of time and can use an estimated solution. Other DL frameworks are: Keras, Theano, Torch, Caffee, Deeplearning4j, PaddlePaddle, DataMelt, Dlib, BigDL, Seq2SeqSharp and OpenNN.

In this group, one of the most popular software tools is known as Amazon Web Services (AWS) [79]. It is an Amazon.com affiliate that offers subscription-based on-demand cloud computing platforms for the AI research community. This enables subscribers to have a virtual cluster of computers accessible through the internet all the time. Its own console inputs/outputs are also visualized by each AWS system. It allows AWS subscribers to use any modern browser to connect to its AWS scheme. This platform is suitable for developing ML-based connected vehicles applications.

Google Prediction is a series of application programming interfaces (APIs) that make it possible to connect with and incorporate Google Services into other vehicle services [80]. The embedded Google map on a website and the retrieval of traffic information can be done using the Google Earth API, particularly for connected vehicles applications. The API supports various languages, such as Java, .NET, Objective-C, PHP, and python. Autonomous vehicles benefit from the dynamic loading or auto-loading feature which enhances the performance of applications.

Microsoft Azure is a cloud computing web service for AI [81]. It can be used for connected vehicles AI applications for construction, training, testing, and deployment. The platform offers Software-As-A-Service (SAAS), Platform-AsA-Service (PAAS) and Infrastructure-As-A-Service (IAAS). Multiple programming languages and specialized applications and systems are also supported. This service is a component of the Cortana Intelligence Suite that allows natural communication between humans and machines. Microsoft's connected vehicle platform facilitates cloud processing of connected vehicle data enables the development of innovative applications.

Another possible platform for the connected vehicles paradigm is IBM Data Science eXperience (DSX) [82]. An ML developer may build a project on this platform with a community of collaborators who have access to different models of analytics and different programming languages. In an integrated environment, DSX also cooperates with some open source tools like RStudio, Spark and Python and gives access to datasets that are accessible in the cloud through the Watson Data Platform. It has a broad community developers and embedded tools on the latest innovations from the data science community, such as datasets.

8 Conclusions

This document provides both a tutorial on the state-of-the-art discussion regarding connected vehicles and insights into ongoing research in the field. It is anticipated that LTE C-V2X will drive further the standard 5G C-V2X with improved technology. The 5G NR-based services will facilitate the development of new and innovative services and applications beyond those intended to provide basic safety. Privacy and security assume added importance due to the nature of connected vehicular environment in which there exists a need to share information that are required for legitimate reasons and applications, but which can be exploited for ill-conceived purposes by illegitimate users. There exists an urgent need to impart security to thwart Cyber security threats. AI and ML techniques could be valuable in imparting security along various layers, enabling better communications among vehicles under dynamically changing propagation conditions due to high mobility and traffic, facilitating extraction of meaningful information from big data collected by vehicles, and in spectrum sharing and improving spectrum utilization. Clearly, the standards and research are evolving and accelerating the drive towards autonomous vehicles with the objective to provide totally secure environment and traffic safety and offer new and innovative services and applications beyond those intended to offer basic services, with security and safety.

The contributions brought forth by the authors to this WWRF Outlook are summarized below. It provides

- a pedagogical exposition of the field of connected vehicles with a discussion of the standardization activities that have taken place in standards organization such as IEEE, 3GPP, ETSI, ITU-T, and ITU-R. This will benefit practicing engineers as well as students and researchers interested acquiring knowledge in this rapidly growing field;
- an overview of 3GPP's C-V2X standard, specifically as formulated in Releases 14, 15, and 16. The releases are about both LTE-based C-V2X (Rel. 14 and 15) and 5G C-V2X (Rel.16). It also provides information concerning the stake holders of the technology, the timeline of C-V2X and 5G C-V2X, and discusses both time critical and advanced use cases;
- a discussion of the need to provide V2X connectivity with a range of heterogeneous radio access technologies such as DSRC, LPWAN, multi-hop D2D, cognitive radio, unmanned aerial vehicles (UAVs) communication and Wi-Fi networks;
- an introduction to spectrum allocation for various ITS applications, including applications for connected vehicles. Specifically, the section discusses

ITU-Radio communications concerning the allocation and management of frequency spectrum to the three regions of the world;
- a discussion of security and privacy issues and protocols as laid out in ETSI ITS, IEEE DSRC WAVE, 3GPP C-V2X;
- a discussion of ongoing research and approaches to offering security, privacy, and trust using technologies such as cloud, blockchain, and AI/machine learning techniques;
- a classification and taxonomy of AI and machine learning techniques and a discussion of the use of Markov Decision Processes, Q-Learning and Deep Learning; and
- a handle on the open source tools available for the practicing engineers, developers of applications for connected vehicles, and the research community.

References

1. Statista, "Internet of Things - active connections worldwide 2015-2025 Published by H. Tankovska, Sep 1, 2020. [Online]. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#:~:text=Internet%20of%20Things%20%2D%20active%20connections%20worldwide%202015%2D2025&text=The%20total%20installed%20base%20of,billion%20units%20worldwide%20by%202025.
2. IDC, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219
3. Tuxera, "Autonomous and ADAS test cars produce over 11 TB of data per day," October 2018. [Online]. Available: https://www.tuxera.com/blog/autonomous-and-adas-test-cars-produce-over-11-tb-of-data-per-day/

4. 3GPP SA Wg1, “Study on LTE support for Vehicle-to-Everything (V2X) services,” Specification #22.855, 2015.
5. 3GPP SA Wg2, “Study on architecture enhancements for LTE support of V2X services,” Specification #: 23.785, 2016.
6. 3GPP SA Wg1, “Service requirements for enhanced V2X scenarios,” Specification#: 22.186, 2018. 7. S. Wg2, 2018.
7. 3GPP SA WG2, “Architecture enhancements for V2X services,” Specification#: 23.285, 2016.
8. 3GPP RAN Wg1, “TS 38.211, NR; Physical channels and modulation,” 2018.
9. 3GPP RAN Wg1, “Study on evaluation methodology of new Vehicle-to-Everything V2X use cases for LTE and NR,” Specification 37.855, 2018.
10. EU Website, 2016. [Online]. Available: http://ec.europa.eu/transport/themes/its/c-its_en.htm
11. ERTRAC WG, Automated driving roadmap, PC Draft, ERTRAC Working Group “Connectivity and Automated Driving,” 2017.
12. QUALCOMM “Accelerating C-V2X Commercialization,” https://www.qualcomm.com/media/documents/files/accelerating- c-v2x-commercialization.pdf, 2017.
13. 5G Americas, “5G Americas White Paper: Cellular V2X Communications Towards 5G,” 2018. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/07/2018_5G_Americas_White_Paper_Cellular_V2X_Communications_Towards_5G___Final_for_Distribution.pdf
14. Contreras-Castillo *et al.*, “Internet of Vehicles: Architecture, Protocols, and Security,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018. [Online]. Available: https://dx.doi.org/10.1109/jiot.2017.2690902
15. Hu *et al.*, “Vehicular multi-access edge computing with licensed sub-6 GHz, IEEE 802.11p and mmWave,” *IEEE Access*, vol. 6, 1995.
16. Guan *et al.*, “5-GHz Obstructed Vehicle-to-Vehicle Channel Characterization for Internet of Intelligent Vehicles,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 100–110, 2019. [Online]. Available: https://dx.doi.org/10.1109/jiot.2018.2872437
17. ITU-RR, “Radio Regulations Articles, Edition 2016,” 2016.
18. ITU-RR1, “Radio Regulations Resolutions and Recommendations, Edition 2016.” 2016.
19. ITU-R M.1890, “Recommendation ITU-R M.1890, Intelligent Transport Systems – Guidelines and Objectives”, 2011,” 2011.
20. ITU-R M.1453-2, “Recommendation ITU-R M.1453-2, “Intelligent Transport Systems – Dedicated Short Range Communications at 5.8 GHz”, 2005.” 2005.
21. ITU-R M.2228-1, “Report ITU-R M.2228-1, "Advanced intelligent transport system radiocommunications”,” 2015.
22. ITU-R M.2084-0, “Recommendation ITU-R M.2084-0, Radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure communications for Intelligent Transport System applications,” 2015.
23. ITU-R. M.1452-2, “Recommendation ITU-R M.1452-2, Millimeter wave radiocommnication systems for ITS applications,” 2012.

24. ETSI TS 102 731, “Intelligent Transport Systems (ITS); Security; Security Services and Architecture,” 2010.
25. ETSI TS 102 940, “Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management" (V1.2.1; 2016- 11),” 2016.
26. ETSI TS 102 941, “Intelligent Transport Systems (ITS); Security; Trust and Privacy Management" (V1.1.1; 2012-06),” 2012.
27. ETSI TS 103 097, “Intelligent Transport Systems (ITS); Security; Security header and certificate formats, (V1.1.1; 2013-04).” 2013.
28. IEEE 1609.2, “IEEE Std 1609.2-2016, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages,” 2016.
29. SAE J2945/1_2016-03, “On-Board System Requirements for V2V Safety Communications,” 2016. [Online]. Available: http://standards.sae.org/j2945/1_201603
30. 3GPP-TS-33.185, “Security aspect for LTE support of V2X services,” 2017.
31. P. Kleberger *et al.*, “Security aspects of the in-vehicle network in the connected car,” *Intelligent Vehicles Symposium (IV)*, pp. 528–533, 2011.
32. D. Nilsson, “Creating a secure infrastructure for wireless diagnostics and software updates in vehicles,” *International Conference on Computer Safety, Reliability, and Security*, pp. 207–220, 2008.
33. S. Checkoway, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *USENIX Security Symposium*, 2011.
34. Hasch *et al.*, “Millimeter-Wave Technology for Automotive Radar Sensors in the 77 GHz Frequency Band,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 3, pp. 845–860, 2012. [Online]. Available: https://dx.doi.org/10.1109/tmtt.2011.2178427
35. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States,” *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011. [Online]. Available: https://dx.doi.org/10.1109/jproc.2011.2132790
36. A. K. Panghal, “Vehicular Ad-hoc Network (VANET)-Privacy and Security,” *International Journal of Advanced Research in Computer Science*, vol. 6, 2015.
37. Maglaras *et al.*, “Social Internet of Vehicles for Smart Cities,” *Journal of Sensor and Actuator Networks*, vol. 5, no. 1, pp. 3–3, 2016. [Online]. Available: https://dx.doi.org/10.3390/jsan5010003
38. Hubaux *et al.*, “The security and privacy of smart vehicles,” *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49–55, 2004. [Online]. Available: https://dx.doi.org/10.1109/msp.2004.26
39. Dötzer, “Privacy issues in vehicular ad hoc networks,” *Privacy enhancing technologies*, pp. 197–209, 2005.
40. Verberne *et al.*, “Trust in smart systems: Sharing driving goals and giving information to increase trustworthiness and acceptability of smart systems in cars,” *Human factors*, vol. 54, pp. 799–810, 2012.
41. Kaur *et al.*, “Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars,” *Journal of Engineering and*

Technology Management, vol. 48, pp. 87–96, 2018. [Online]. Available: https://dx.doi.org/10.1016/j.jengtecman.2018.04.006

42. Ltifi *et al.*, “Smart Trust Management for Vehicular Networks,” *Computer, Energetic, Electronic and Communication Engineering*, vol. 10, pp. 1128–1135, 2016.
43. Kerrache *et al.*, “Trust Management for Vehicular Networks: An Adversary-Oriented Overview,” *IEEE Access*, vol. 4, pp. 9293–9307, 2016. [Online]. Available: https://dx.doi.org/10.1109/access.2016.2645452
44. Gerla *et al.*, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” *Proc. IEEE World Forum Internet Things (WF-IoT)*, pp. 241–246, 2014.
45. Sharma *et al.*, “Cognitive Radio Adhoc Vehicular Network (VANET): Architecture, Applications, Security Requirements and Challenges,” *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, 2016.
46. Yang *et al.*, “An overview of Internet of Vehicles,” *China Communications*, vol. 11, no. 10, pp. 1–15, 2014. [Online]. Available: https://dx.doi.org/10.1109/cc.2014.6969789
47. Xiang *et al.*, “Multi-hop transmission and retransmission measurement of real-time video streaming over DSRC devices,” *Proc. IEEE 15th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, pp. 1–9, 2014.
48. Sharma *et al.*, pp. 43–46, 2016.
49. Ma, “Social network and tag sources based augmenting collaborative recommender system,” *IEICE Trans. Inf. Syst*, no. 4, pp. 902–910, 2015.
50. Fu *et al.*, “Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing,” *IEICE Trans. Commun*, vol. 98, no. 1, pp. 190–200, 2015.
51. Chen, “Measuring the Performance of Movement Assisted Certificate Revocation List Distribution in VANET,” *Wireless Commun. And Mobile Computing*, vol. 11, no. 7, pp. 888–898, 2011.
52. Su *et al.*, “Smart city and the applications,” in *Proc. IEEE Int. Conf. Electron*, 2011, pp. 1028–1031.
53. Campolo *et al.*, “SMARTCAR: An integrated smartphone-based platform to support traffic management applications,” in *Proc. IEEE Int. Workshop Veh. Traffic Manage. Smart Cities (VTM)*, 2012, pp. 16–16.
54. Amadeo *et al.*, “Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs,” *Ad Hoc Networks*, vol. 10, no. 2, pp. 253–269, 2012. [Online]. Available: https://dx.doi.org/10.1016/j.adhoc.2010.09.013
55. Guerrero-Ibez *et al.*, *Vehicular ad-hoc networks (VANETs): Architecture, protocols and applications, in Next-Generation Wireless Technologies*. London, U.K.: Springer, 2013.
56. Aslam *et al.*, “Extension of internet access to VANET via satellite receive-only terminals,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 14, no. 3, pp. 172–172, 2013. [Online]. Available: https://dx.doi.org/10.1504/ijahuc.2013.058235

57. Toor *et al.*, “Vehicle Ad Hoc networks: applications and related technical issues,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74–88, 2008. [Online]. Available: https://dx.doi.org/10.1109/comst.2008.4625806
58. Sharma, “Cloud Based Secured VANET with Advanced Resource Management and IoV Applications,” *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*, 2019.
59. Liu *et al.*, “Creating Autonomous Vehicle Systems,” *Synthesis Lectures on Computer Science*, vol. 6, no. 1, pp. i–186, 2017. [Online]. Available: https://dx.doi.org/10.2200/s00787ed1v01y201707csl009
60. Sookhak *et al.*, “Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing,” *IEEE Vehicular Technology Magazine*, vol. 12, no. 3, pp. 55–64, 2017. [Online]. Available: https://dx.doi.org/10.1109/mvt.2017.2667499
61. Whaiduzzaman *et al.*, “A survey on vehicular cloud computing,” *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014. [Online]. Available: https://dx.doi.org/10.1016/j.jnca.2013.08.004
62. Aloqaily *et al.*, “Vehicular clouds: State of the art, challenges and future directions,” *Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on*, pp. 1–6, 2015.
63. Sharma *et al.*, *Advanced Spectrum Management For Next-Generation Vehicular Communication: An AI Approach*, U British Columbia, Vancouver, Canada, 2019.
64. Sharma, *et al.*, “Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture,” in *IEEE 5G World Forum*, and others, Ed., 2019.
65. Tong *et al.*, “Artificial intelligence for vehicle-to-everything: A survey,” *IEEE Access* , vol. 7, pp. 10 823–10 843, 2019.
66. G. Beni *et al.*, “Swarm Intelligence in Cellular Robotic Systems,” in *Proceedings NATO Advanced Workshop on Robots and Biological Systems*, 1989.
67. J. Deneubourg, “The Dynamics of Collective Sorting Robot-Like Ants and Ant-Link Robots,” *From Animal to Animats I*, pp. 356–363, 1990.
68. I. Kassabalidis *et al.*, “Swarm Intelligence for routing in communication networks,” in *IEEE Global telecommunications Conference (GLOBECOM).* IEEE Press, 2001.
69. L. Liang *et al.*, “Towards Intelligent Vehicular Networks: A Machine Learning Framework,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 124–135, 2019.
70. A. Ruan *et al.*, “A Reinforcement Learning Based Markov-Decision Process (MDP) Implementation for SRAM FPGAs.” *IEEE Transactions on Circuits and Systems II: Express Briefs* , vol. 67, no. 10, 2019.
71. J. Fan *et al.*, “A theoretical analysis of deep Q-learning,” *Learning for Dynamics and Control*, 2020.
72. J. Chen *et al.*, “Deep learning with edge computing: A review,” *Proceedings of the IEEE*, no. 8, 2019.

73. B. Ramsundar *et al.*, *Tensorflow for Deep Learning: From Linear Regression to Reinforcement Learning*. O'Reilly Media, 2018.
74. Z. Matei *et al.*, *Spark: The Definitive Guide*. O'Reilly Media, 2018.
75. F. Pedregosa *et al.*, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2015.
76. T. Wang *et al.*, "PySNS3: A Real-Time Communication Interface and Protocol for Vehicular Ad-Hoc Networks," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine*, 2017.
77. B. Lorica *et al.*, "Why AI and machine learning researchers are beginning to embrace PyTorch," 08 2017.
78. D. Gage, 6 2015.
79. L. Tung, "Amazon gets startup-friendly with AWS Loft space in London," 1 2017.
80. G. APIs, "Google APIs Client Libraries," 2020. [Online]. Available: https://developers.google.com/discovery/libraries,2020.
81. M. Azure, "Microsoft Azure," 2020. [Online]. Available: azure.microsoft.com
82. K. Noyes, "IBM targets data scientists with a new developmentplatform based on Apache Spark," 11 2011.

Imprint

Wireless World Research Forum
c/o Format A AG
Wiesenstraße 9
CH-8034 Zürich

Secretariat:
Vinod Kumar
e-Mail: vinod.kumar@wwrf.ch
Phone and Fax : +33611181622

The WWRF is a non-profit organisation registered in Switzerland.

Chairman of the Forum:
Dr. Nigel Jefferies

Editor-in-Chief: Dr. Nigel Jefferies

The WWRF Outlook Visions and research directions for the Wireless World
ISSN 1662-615X is published non-periodically by the Wireless World Research Forum
http://www.wwrf.ch

Responsibility for the contents rests with the Steering Board of the Forum.