Sustainable Adoption of Connected Vehicles in the Brazilian Landscape: Policies, Technical Specifications and Challenges

Douglas Aguiar do Nascimento, Yuzo Iano, Hermes José Loschi, Navid Razmjooy, Robert Sroufe, Vlademir de Jesus Silva Oliveira, Diego Arturo Pajuelo Castro, Matheus Montagner

Abstract—This paper addresses the intervehicular communication in Connected Vehicles (CV) by emphasizing V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communications in terms of evolution, current standards, state-of-the-art studies, embedded devices, simulation, trends, challenges, and relevant legislation. To accomplish the objective this review is based on studies conducted from 2003 to 2019, government reports about the sustainable deployment of these technologies and their adoption in the Brazilian automotive market according to experts. Moreover, WAVE (Wireless Access in Vehicular Environment) and DSRC (Dedicated Short-range Communication) standards, the performance analysis of communication parameters and intervehicular available at the market are also described. The current status of ITS (Intelligent Transportation System) development in Brazil is reviewed, as well as the research institutes and governmental actions focused on introducing the concept of connected vehicles into the society. The Brazilian outlook for technological adoption concerning CVs was also discussed. Besides those, challenges related to technical aspects, safety and environmental issues, and the standardization for vehicle communication are also described. Finally, this review highlights the challenges and proposals from available technologies devoted to the roads and vehicular infrastructure communication, their evolution and upcoming trends.

Index Terms—Connected Vehicles, Intelligent Transportation System, Vehicular Communication, Policies, Specification, Sustainability.

I. INTRODUCTION

The number of deaths from traffic accidents has reached about 1.25 million per year around the world, representing the first fatality cause across people aged 15-29 years old [1]. Despite Brazil's legislation on the best traffic practices (prohibiting drunk driving and the awareness of using the helmet, seat belt, and child restraint), the total number of fatalities recorded in 2016 was about 34,850 [2]. It is estimated

D. A. Nascimento, Y. Iano, H. J. Loschi and D. A. P. Castro were with the Department of Communications, School of Electrical and Computer Engineering, University of Campinas, Campinas, SP, 13083-852 BR, e-mail: eng.douglas.a@ieee.org.

N. Razmjooy is with Tafresh University, Department of Electrical and Control Engineering, Tafresh 39518 79611, Iran.

R. Sroufe is with John F. Donahue School of Business, Duquesne University, Rockwell Hall 820, 600 Forbes Avenue, Pittsburgh, PA 15282, USA.

V. J. S. Oliveira is School of Exact and Technological Sciences, Mato Grosso State University, Av. dos Ingas, 3001, Jardim Imperial, Sinop, MT, 78555-000.

M. Montagner is with Santa Catarina State University, Paulo Malschitzki St., 200, Bairro: Zona Industrial Norte, Joinville, SC, CEP: 89219-710.

Manuscript received on February 10, 2019 and revised on March 17, 2019.
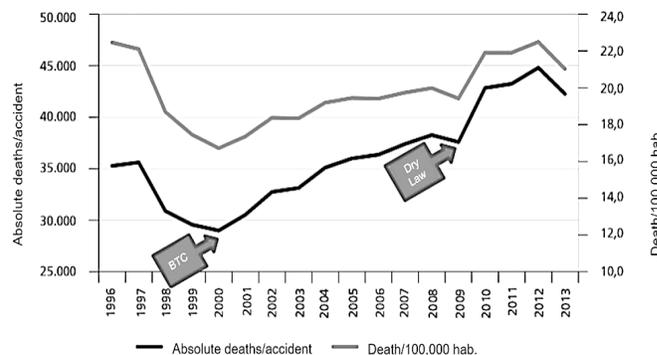
Fig. 1. Evolution of mortality from terrestrial transport [4].

that Brazil spends US$ 12.3 billion [1] annualy on economic production losses since the victims are absent from work and hospital expenses from traffic accidents on Federal and State highways, municipal and urban agglomerate streets [3]. In 2014, for example, the cost to society was US$ 3.16 billion, due to the 167,247 traffic accidents only on Federal roads, as shown in Table 1. The cost of each accident is the sum of the cost components associated with the control variables of the additive model - costs associated with people, vehicles and other costs.

As shown in Figure 1, the economic production losses arising from labor capacity is the most expensive to society due to accidents involving workers.

According to Figure 1, there were some sudden death drops from terrestrial accidents (i.e., 1997-2000 and also 2008-2010), which were caused by the adotion of a more rigid legislation according to the new Brazilian Traffic Code (BTC) and the enforcement of the DWI (Driving While Intoxicated) Law, respectively. The long-term trend is the increase in the number of fatalities. The adoption of public policies introduced by the US Department of Transportation was effective in reducing fatalities and injuries [5]. The adoption of V2V technologies could also help avoid 439,000-615,000 crashes, which represents 13-18% of crashes involving light vechicles, reducing up to 418,000 MAIS (Maximum Abbreviated Injury Scale) within a scale of 1-5 injuries and avoid 746,00 damages

[1] 1 USD: BRL 4.05 (Sept. 22nd, 2018).

Cost	Description	Value ($)	%
People	Hospital expenses; attendance; treatment of injuries; removal of victims; and economic production losses	1,963,186,281.98	62.01
Vehicle	Removal of vehicles; damage to vehicles; and loss of production capacity over its lifetime	1,185,294,508.64	37.44
Institutions and property damage	Attendance; prosecution and damage to public and private properties	17,282,788.40	0.55
Total		3,165,763,579.02	100.00

to PDOVs (Property-damage-only vehicles) [6]. Technologies based on partial automation levels (e.g. ESP - Electronic Stability Control) are responsible for reducing the number of accidents. It is estimated that reducing damages or avoiding crashes in 18% of the total accidents and 34% of those resulting in fatalities is feasible [7]. Regarding secutiry applications, such as CICAS (Cooperative Intersection Collision Avoidance Systems), 80% of crashes could be avoided if 50% of the crossings were equipped with RSU devices (Road-side Unit) from V2I (Vehicle-to-infrastructure). Moreover, 50% of crashes could be avoided if 20% of the crossings were equipped with RSU V2I [5], [8]. Therefore, stakeholders from many countries believe that the systems of connected vehicles (CV – Connected Vehicle), also known as Cooperative Intelligent Transportation System (C-ITS), have the ability to enhance traffic in terms of transport security and efficiency [9]. This scenario of connected cars would be associated to Smart Cities, where several devices are connected in the cloud (data storage network infrastructure) and able to communicate to each other in order to exchange information and data storage. This data, after it was processed and analyzed, would still be useful in providing services and further processing needs. Hence, the term "connected car industry" has been widely used and the revenue forecast for the sales of connected cars is shown in Figure 2 [10].
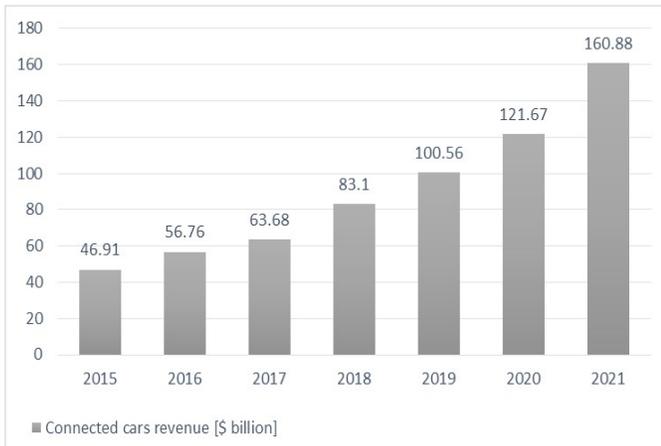

Fig. 2. Global market for connected cars.

Many market surveys provide a number of 380 million connected vehicles [11]–[14]. The development of connected vehicles is taking place in conjuction with underlying technologies devoted to network and communication infrastructure capable of meeting the bandwidth demand required by connected vehicles, such as the 5G mobile communication and WAVE (Wireless

Access in Vehicular Environment) [15]–[18]. Therefore, this work proposes an overview on different types of communication methods for Connected Vehicles and the analysis of prospects and trends for the Brazilian scenario. It is out of the scope of this work covering intelligent cooperative transport systems (CITS) or intervehicular communication for platooning (convoy), since this approach should describe the routing of VANET networks, cognitive applications and case studies in VANET. Readers interested in those technological aspects are encouraged to search elsewhere [19]–[23]. Connected vehicles belong to a new model known as Intelligent Transportation System (ITS), which is focused on improving traffic safety and efficiency by means of wireless electronic communication. Connected vehicles rely on GPS (Global Positioning System) data, connectivity (wireless communication), and data processing to enable vehicles, smart road infrastructure and mobile phones to exchange information for providing warning and security messages to road users [8]. Therefore, this work was structured as follows: Section 2 introduces IoV (Internet of Vehicles) and associated definitions. Section 3 addresses vehicular communication in terms of infrastructure and data exchange, protocols and technologies to connect vehicles. Section 4 describes the Brazilian adoption of vehicular technologies. Section 5 deals with the challenges from technical aspects (e.g., which frequency range to use and allocation issues), safety, and public acceptance within the Brazilian scenario. Section 6 describes the legislation, public policies and legal perspective. Section 7 provides conclusions based on the idea of vehicle communication.

II. INTERNET OF VEHICLES

The Internet of Things (IoT) [25] is a paradigm that establishes a world of embedded physical objects, based on sensors and actuators, connected to wireless networks. They can communicate through the Internet, which gives rise to a network of intelligent objects able to do various types of data processing, get environmental variables, and react to external event. These objects are connected to each other and to other resources (physical or virtual). They can be controlled through the Internet, which allows a plethora of applications that will be able to use new types of data, services and operations available. IoT is an example of an emerging technology that contributes to the achievement of
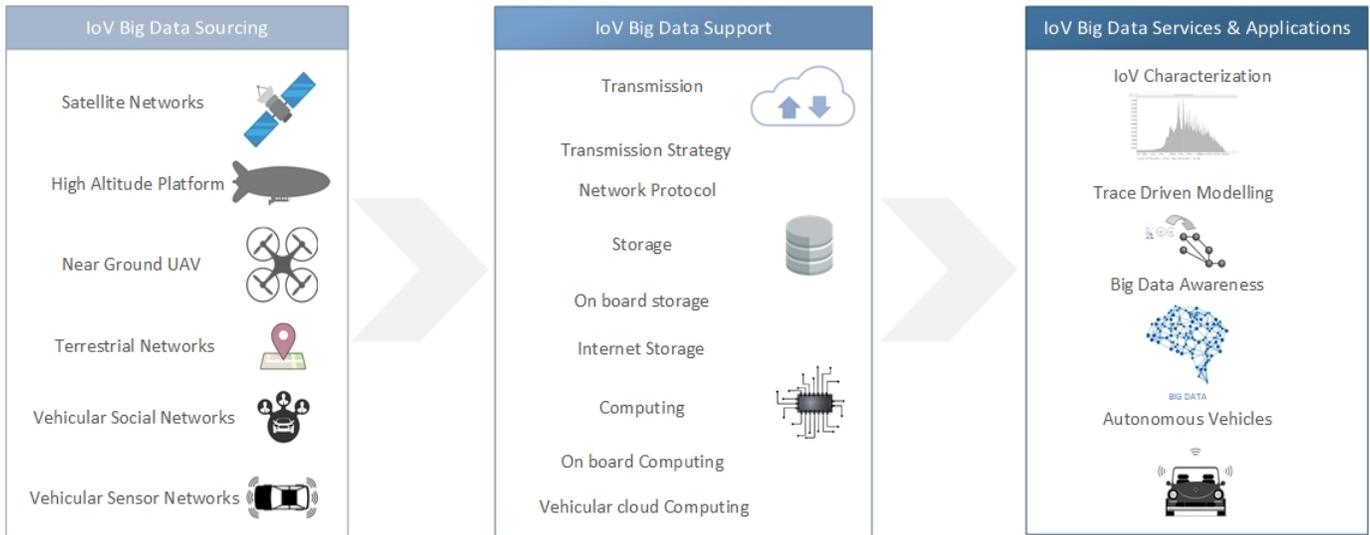
Fig. 3. IoV big data architecture, based on [24].

new fields of application for information and communication technologies (ICTs). One of these domains can be understood as that from smart cities, wherein the use of communication and sensing technologies provides value-added services to the administrative bodies of such cities and their citizens [26], [27]. One of the applications regarding the ICT domain is the intelligent mobility. As described elsewhere [28], mobility is part of the daily life of the modern society, since it requires transportation systems based on different types of vehicles and communication infrastructure. With the recent advances in information and communication technologies, mobility has an important role in providing a better quality of life. The Internet of Things integrates intelligence into existing research and development areas, such as smart-health, smart-home, smart-energy, smart industry and smart transport - or smart mobility as described in [29] (see Figure 3).

The Internet of Vehicles (IoV) is one of the revolutions mobilized by IoT, which involves the concept of VANET - Vehicular Ad hoc Networks, to convey the vision of the smartphone to the smart car [30], [31]. VANET is aimed at improving traffic efficiency and safety by means of real-time communication between advanced wireless access technologies, enabling vehicles with or without RSU (Road Side Unit) [31]. VANETs are a special class of Mobile Ad hoc Networks (MANET) in which the vehicles work as people. These networks are characterized by the high speed of vehicles, low intercontact times among hosts, intermittent connection and real-time data exchange requirements [32]. Moreover, these networks rely on a minimum or temporary infrastructure and are characterized by high mobility, fixed road networks, traffic patterns and predictable speed under traffic congestion conditions, low power requirements, and storage limitations. Even though other communication systems rely on high message throughput, VANETs primarily focus on reliable communication and fast dissemination of safety mes-

sages [33]. This way CVs may communicate with each other or with the traffic infrastructure (RSU) by using consolidated Technologies, which are divided as [32]: 1. Vehicle-to-vehicle (V2V) communication; 2. Vehicle-to-infrastructure (V2I) communication; 3. Hybrid communication composed of V2V and V2I, and 4. Vehicle-to-everything (V2X) communication. V2V communication is also known as C2C (Car-to-car), or inter-vehicle communication (IVC). The term "Connected Vehicles" refers to the applications, services, and technologies for connecting vehicles. By adopting a similar definition as New Cars Auto Connected, a connected vehicle is basically formed by the presence of devices that connect this vehicle to other services, devices, networks, applications and services outside the vehicle. Applications include traffic efficiency and safety, infotainment, parking assistance, roadside assistance, remote diagnostics and telematics for self-driving vehicles, and Global Positioning System (GPS). Vehicles with advanced interactive driver-assistance systems (ADAS) and Cooperative Intelligent Transport Systems (C-ITS) can be considered the typical connected vehicles. Safety applications for connected vehicles are designed to increase the awareness and reduce traffic accidents through vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [34], [35]. An increasing number of factories are equiping their vehicles with on-board computers, sensors, and navigating systems able to create mass scale vehicle networks [36]–[38]. By using a myriad of sensors, cameras, computers, and communication services, vehicles are able to harvest, process, analyze, and send information to help drivers [38]. Traffic Information Systems (TISs) allow a better use of road networks by providing real-time traffic conditions and by guiding drivers to make better routing decisions [39], [40]. Vehicle network applications may be classified as [38]: 1. Safety; 2. Entertainment, and 3. Driving assistance. Safety includes applications intended to provide information to the driver about dangerous road conditions,

such as the weather, traffic jams, accidents, etc, with the dissemination of emergency information. The entertainment applications provide the support for Internet access, advertising, content sharing, chats and related services. The driver assistance applications will provide the exchange of information for helping drivers to find gas or power stations, restaurants, and toll roads. Moreover, the systems of CVs also allow: reduction of greenhouse gas emission and fuel consumption, enhanced safety and protection, higher efficiency, mobility and accessibility, besides the adoption of economical opportunities for advancing investments and research on clean technologies [41].

III. VEHICULAR COMMUNICATION

It is a global network of WAT (Wireless Access Technology), which includes vehicles, the Internet and other heterogeneous networks, such as the Internet of Vehicles (IoV). The heterogeneous network architecture of IoT includes five types of vehicular communication (Figure 4): V2V (Vehicle-to-Vehicle), by using WAVE (Wireless Acess in Vehicular Environment) through the 802.11p protocol; V2R (Vehicle-to-Roadside unit) with WAVE and 802.11p protocol; V2I (Vehicle-to-Infrastructure) available through Wi-Fi (Wireless Fidellity) 802.11b, Wi-Fi 802.11g and also mobile networks such as 4G, LTE (Long-Term Evolution) and 5G [16], [42], [43]; V2P (Vehicle-to-Personal devices) through technologies such as CarPlay, OAA and NCF, for example; V2S (Vehicle-to-Sensors), in which the ECU (Electronic Control Unit) from vehicles is able to communicate with sensors installed in the vehicle by using protocols such as Ethernet, WiFi and MOST (Media Oriented Systems Transport). Therefore, each vehicle communication from IoV is enabled by using a different WAT, which includes, IEEE WAVE for V2V and V2R, WiFi and 4G/LTE for V2I, CarPlay/NFC for V2P and MOST/WiFi for V2S. The inclusion of a plethora of devices makes the architecture more complex, even though more market oriented, such as VANETs. The structure of a heterogeneous vehicle network of IoV has a significant power for guiding and monitoring vehicles [31], [44], [45].

Even though the vehicle communication technology is mainly used for traffic safety, connected vehicles are also able to support technologies other than safety, such as telematics and traffic management, which includes the control over road congestion, smart tolling and optimization of routes and directions [8]. A suitable description for better understanding this is proposed elsewhere [46], according to the zones of interest, which may be: personal (communication based on PAN), information exchange among vehicles and personal devices; local network (LAN), communication among vehicles and vehicle to vehicle and local infrastructure; and regional (by using mobile networks), applications based on broadcasting, in which the traffic center or manager sends information to vehicles in the region.
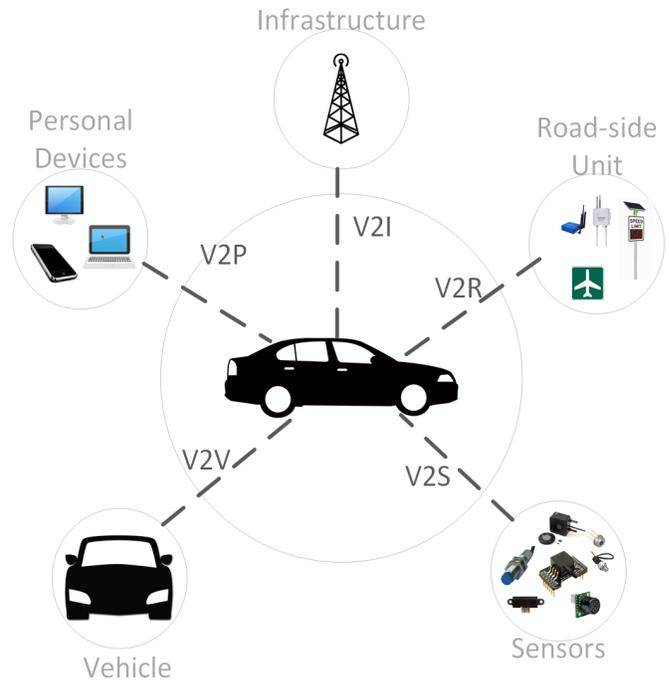

Fig. 4. Types of IoV communication, based on [31].

A. Technologies and Protocols for Vehicular Communication

Within the vehicular communication, each device in the network (vehicle or infrastructure device) is considered a node. The communication among nodes from vehicular networks may be done in three different ways: vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and hybrid (V2X) [47], [48]. The Intervehicular Communication (IVC), which is part of the ITS (Intelligent Transportation System) and its real applications in mobile ad hoc networks, has been researched at the academia and also at industries, most notably in the US, Europe and Japan. The most important achievement from IVC is its ability to expand the horizon of drivers and on-board devices (radar or sensors, for example), besides improving traffic safety and efficiency on the roads [49]. ITS enhances not only transport safety and mobility but also the American economic productivity by integrating advanced communication technologies into transport infrastructure and vehicles. ITS encompasses a myriad of information and electronic technologies based on wired and wireless communication [50]. Table 2 shows an overview from the main countries developing research and the implementing ITS.

There are three different categories for automobile applications based on communication [9], [52]: 1. Safety-driven: examples include the alert for a parked or slow vehicle and electronic emergency brake lights, V2V warning of an accident, an alert for road resources and cooperative collision warning. 2. Comfort-driven: alerts for congested roads, traffic probes, and warning of parking availability, parking lot finder, are some examples. 3. Commercial-driven: such as remote

	Japan	USA	Europe
Standard / Committee	ITS-Forum	IEEE802.11p/1609.x	CEN/ETSI EN302 663
Frequency Range	755 – 765 MHz	5850 – 5925 MHz	5855– 5925 MHz
Number of Channels	One 10 MHz channel	Seven 10 MHz channels (Two 20 MHz channels formed by combining 10 MHz channels)	Seven 10 MHz channels
Modulation		OFDM	
Data rate per Channel	3 -18Mbit/s	3 -27Mbit/s	3 - 27Mbit/s
Output power	20 dBm (Antenna input)	23 - 33 dBm (EIRP)	23-33 dBm (EIRP)
Communication	One direction multicasting service (broadcast without ACK)	One direction multicasting service, One to Multi communication, Simplex communication (broadcast without ACK, multicast, unicast with ACK)	
Upper protocol	ARIB STD-T109	WAVE (IEEE 1609) / TCP/IP	ETSI EN 302 665 (incl. e.g.GeoNetworking) TCP/UDP/IP

customization or diagnostics of a vehicle, advertising services, download of contents and real-time video broadcasting.

1) Inter-vehicular Commmunication: WAVE (Wireless Acess in Vehicular Environment) is a wireless technology primarily developed for harsh environments, wherein it enables the fast communication among vehicles with the advantages of high mobility, threshold delays for security messages with severe QoS, optimal energy consumption and respect for privacy and anonymity from roaming users, besides other environmental challenges [53]. According to [47], IEEE has started the standadization of vehicular communcation networks within the IEEE 802.11 working group. This standard has been under development since 2004 and is called IEEE 802.11p – Wireless Acess in Vehicular Environment (WAVE). It is governed by the IEEE 1609 [54] and IEEE 802.11p [55] standards, which establish vehicular communications. A scheme to show the integration among WAVE components is shown in Figure 5.
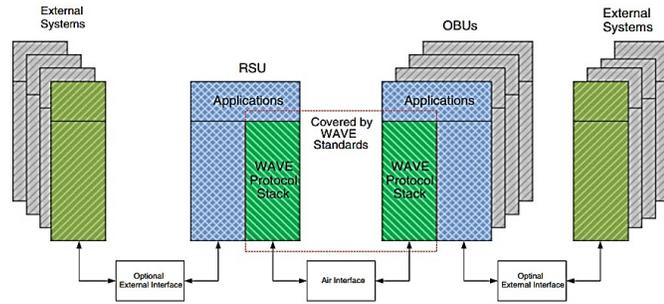

Fig. 5. Example of a WAVE system component, based on [53], [54].

As a global term, WAVE is nowadays employed to define all wireless vehicular communications. It became arbitrarily used as a general term, such as DSRC. Regarding the standardization, WAVE is used for projecting a set of IEEE1609.x standards over the 802.11p standard [53]. Therefore, a DSRC/WAVE offers [8], [54], [56], [57]: 1. Low latency - 802.11p standard states essencial events (functions and services) for data exchange without establishing a Basic Service Set (BSS); 2. Data rate – 802.11 defines a 10 MHz-bandwidth channel and eight data rates' types, i.e. 3, 4, 5, 6, 9, 12, 18, 24, 27 MHz; 3. High reliability – in order to comply within harsh envinronments (sandstorm, rain, etc) IEEE 802.11p stablishes

a 10 MHz-bandwidth channel rather 20 MHz; 4. Security and privaty – DSRC protocol provides securing management and messages of application to overcome attacks from malicious and and untrusted events and softwares such as DoD (Denial of Service), eavesdropping and spoofing. The DSRC (Dedicated Short-Range Communication) wireless technology devoted to vehicular communication was designed for ITS applications within vehicular environments. Its primary aim is to offer support to safety applications and the communication among vehicles (V2V), and from vehicle to infrastructure (V2I), this way decreasing the number of accidents. Moreover, DSRC also supports ITS applications, such as managing traffic conditions, information and entertainment (infotainment) [8], [56], [57]. Figure 6 shows the DSRC protocol stack.

The comercial success of the WiFi technology and IEEE 802.11 standards led to the development of a new standard, known as IEEE 802.11p WAVE. IEEE 802.11p is based on the IEEE 802.11a standard, but with improvements on its physical (PHY) and medium access control (MAC), which are aimed at reaching low latency and high communication reliability in short-range radio connections [8], [54], [56]. The IEEE 802.11p standard defines the WAVE physical layers (PHY) and MAC, which are extensions to IEEE 802.11 standard, in order to communicate outside the BSS context. It has also standardized other specifications, such as 5.9 GHz OFDM PHY (within 5,850 – 5,925 GHz in the U.S. and 5,855 – 5,925 GHz in Europe), channel bandwidth, operating
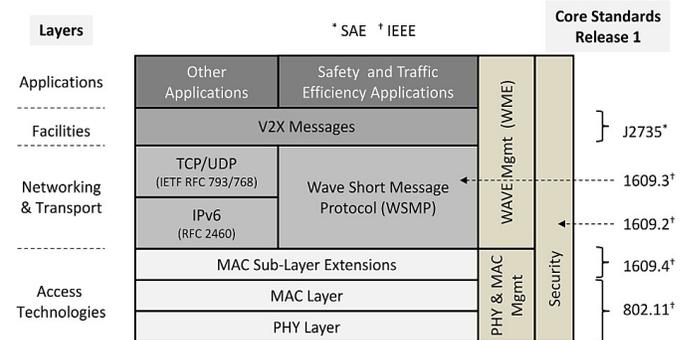

Fig. 6. DSRC protocol stack [58].

ranges, transmission power requirements, transmission masks and alternate channel, and alternate adjacent channel rejection requirements [8]. The IEEE 1609 family of standards defines the architecture and a set of standardized protocols which provide the foundation for a wide range of DSRC/WAVE applications. The most important IEEE 1609.x protocols are [8], [57]: IEEE 1609.3 – defines the using of IPv6 (Internet Protocol version 6) and employs the Wave Short Message Protocol (WSMP) to prevent overhead through the Wave Short Messages (WSM) and the WAVE Service Advertisement (WSA), also setting management functions; IEEE 1609.2 – defines services related to applications and messages of management for authentication using optimal encryption of DSRC messages based upon signals and digital certificates; IEEE 1609.4 – stablishes the multichannel operations by MAC extension and address the channel timing and switching considering IEEE 802.11 standard. Also, it defines the control channel (CCH), created to send messages of advertisement and information through service channels (SCH); SAE j2735 – SAE (Society of Automotive Engineers) standard upper layer containing 15 message, frames and data elements types, and the message specifications; SAE j2945.1 – also defines an upper layer which stablishes the minimum requirements for communication performance. According to [58] the SAE J2735 standard stablishes syntax and semantics of V2X messages and BSM (Basic Safety Message) is the most relevant amongst all other message formats available due BSM address core state information about the broadcasting vehicle and other important informations e.g. location, size, etc. Even though BSM is designed to be compact and efficient, additional frame and data elements may extend it, and add-ons may optionally be added within a subset of messages, such as in every second message. All these DSRC/WAVE functionalities are provided by the communication interface and network technologies as described in the next section.

2) Intra-vehicular Commmunication: Intra vehicular communication allows modules, sensors, and actuators to communicate with each other. It provides the operation for only one vehicle and operates under OBD (On-board diagnostics) services. Local networks also support aftermarket telematic devices, which can access data through OBD's standardized interface. Nowadays, Original Equipment Manufacturers (OEMs) implement sensors and networks shared over the OBD hardware by following OEM standards that carry relevant information for vehicle optimization and support applications concerning future communication. In terms of non-OBD intravehicle communication, communication systems related to drive-by-wire systems are especially built for robustness and security of critical data, whereas other systems host peripheral data, provide fault tolerance, determinism and flexibility, and support network technologies such as CAN, LIN, MOST and FlexRay [59]–[63]. The main traditional intra-vehicular communication networks are [64]:

- LIN (Local Interconnect Network): it is a low-cost and low speed (20 kbps) serial intra-vehicular communication network. LIN is widely used for distributed body control

electronic systems in vehicles since it is a user-friendly and a low-cost technology. It is also applied to some comfort functions;

- CAN (Controller Area Network): it is a serial databus communication protocol developed by Robert Bosch GmbH. Nowadays, CAN has become a standard for transmitting data over intra-vehicular networks with a data rate reaching from 125 kbps up to 1 Mbps. It is widely used for automotive communication due to its flexibility and robust nature, which also includes its limited delay, simplicity and low cost;

- Byteflight: it was developed by BMW and supports a data rate of up to 10 Mbps. This network requires broadband services and has been applied to vehicular networks with high level safety requirements (e.g. passive safety);

- TTP/C (Time-Triggered Protocol): it offers a data rate of up to 25 Mbps and is based on TDMA. Despite its complex project, it provides low cost applications. A TTP frame may contain 240 bytes of data and 4 bytes of overhead. The ability to schedule the communication makes the TTP/C protocol less flexible, but its time-triggered communication allows it to be predictable;

- TTCAN (Time-Triggered Controller Area Network): it was also developed by Robert Bosch GmbH and is based on the TDMA mechanism. TTCAN relies on the same standard and message formats from CAN (supports a data rate from 125 kbps up to 1Mbps), but in contrast to CAN, it has a master node responsible for time synchronization among nodes;

- FlexRay: it is used for high speed and flexible intra-vehicular communication and offers a data rate of up to 10 Mbps. It seems to be the best choice for safety and high speed automotive applications. FlexRay is based on TDMA and FTDMA mechanism. It offers star and multiple star topologies. This network exchanges messages with 254 bytes of data and 5 bytes for the header;

- MOST (Media-Oriented Systems Transport): it was developed to make information and entertainment (infotainment) and multimidia systems easier to handle, with a data rate up to 24.8 Mbps for streaming audio, video, data and control information. This allows such a cost-effective technology to offer an efficient data communication infrastructure;

Figure 7 shows the main systems and communication protocols that make up the vehicle, in which the Ethernet protocol was proposed for transmitting and receiving data from the vehicle. The CAN protocol is applied to comfort electronics and powertrain systems. The USB protocol is used for information and entertainment systems, whereas FlexRay is applied to safety systems and chassis control. Considering the main wireless technologies devoted to vehicular communication, it is relevant to mention the review on intra-vehicular communication technologies summarized in Table 3.

According to the work from [68], wireless technologies are preferable over Zigbee and Bluetooth when taking into account
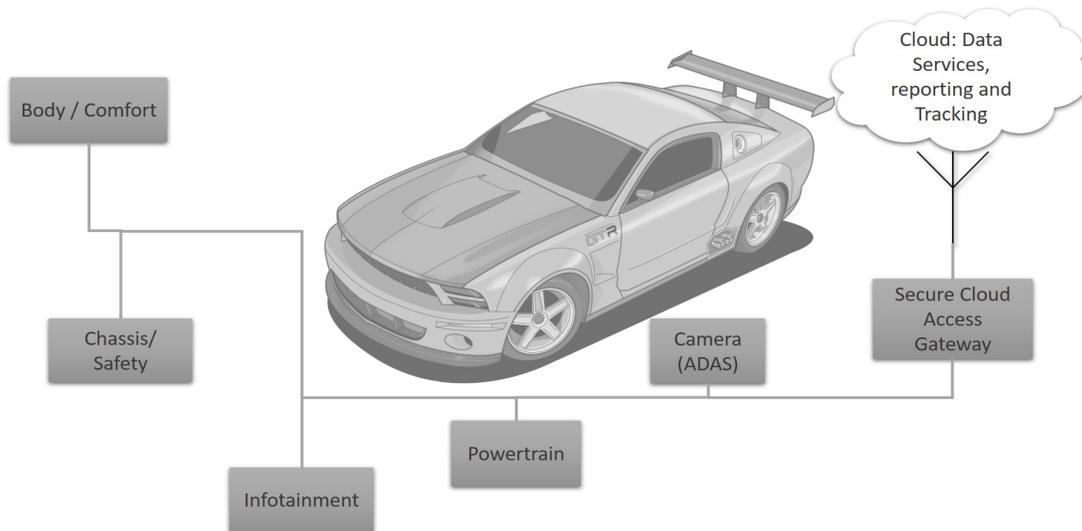
Fig. 7. Example for the application of an in-vehicle communication, based on [65].

TABLE III
THE MOST COMMONLY USED TECHNOLOGIES FOR IN-VEHICLE NEWTWORKS. ADAPTED FROM [66], [67].

Standard	Bluetooth	UWB	ZigBee	Wi-Fi
IEEE specification	802.15.1	802.15.3	802.15.4	802.11a/b/g
In-vehicle applications	In-vehicle communication and device connectivity	High speed intra-vehicular communication environments	In-vehicle communication	In-vehicle communication
Domain	Telematics and body	Telematics and Powertrain	Body	Telematics
Data rate	1 Mbps	100 Mbps	250 Kbps	54 Mbps
Range	10 m	10 m	10-100 m	100 m
Power consumption	Low	Ultra-low	Very low	High
Mode (spreading)	FHSS	DS-UWB	DSSS	DSSS, CCK, OFDM
Modulation type	GFSK	BPSK, QPSK	BPSK, O, QPSK	BPSK, QPSK
Frequency	2.4 GHz	3.1-10.6 GHz	868 MHz, 915 MHz, 2.4 GHz	2.4 GHz, 5 GHz
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit
Topology	Star	Peer-to-peer	Star/Mesh	Star
Maximum number of cell nodes	8	8	> 6500	Unlimited 2007 (infra-structured)

in-vehicle applications relying on a low bitrate and limited power source, as well as its low power consumption that could provide a longer lifetime. On the other hand, high speed data in-vehicle applications could benefit from the use of UWB and WiFi due to their low normalized energy consumption.

3) Underlying Technologies: The need for inter vehicle communication has grown out of some safety issues, such as maintaining or improving road safety for drivers with the ever increasing traffic density. The initial communication was mainly based on the broadcasting type from one central station spreading traffic information. The need for a feed-back channel beween vehicles was noticed a long time ago and, consequently, the need for inter-vehicle communication regarding safety applications, such as the stopping distance, for example. The main limitations of a vehicular network are the requirements for developing a system with the restrictions of a real-time system, while keeping network latency to safe reaction time limits [69].

The vehicles are connected through multiple radio access technologies, such as DSRC, IEEE 802.11 (Wi-Fi), cellular technologies like LTE and improvements arising from the fifth generation (5G) networks. Although 3rd Generation Partnership Program (3GPP) supports telematics and infotainment services for connected cars, cellular networks have received considerable attention for a broader scope with V2X (3GPP release 14) [15] and with 5G providing ultra-high reliability and ultra-low latency demands of tomorrow V2X applications [70].

Inter-vehicle communication may be carried out by means of existing standards, such as cellular networks (3G, 4G) or satellite communications [69]. LTE is the fourth generation of cellular radio network as defined by 3GPP. Even though LTE has a centralized architecture (similar to earlier generations of cellular radio network systems and lacking a native ad hoc mode), it may be useful as a potential access technology for cellular radio networls due to serveral reasons: high data rates (¿100 Mb/s), which is suitable for information and entertainment services, besides the ability to tolerate high mobility with a low transmission latency. These advantages are relevant for road safety applications. Moreover, LTE can cover

a wider area with a higher penetration rate than 802.11p. Major telecommunication companies have been heavily investing in LTE infrastructure, which has already been deployed in some markets around the world. LTE is a promising technology with the ability to fill in major gaps from IEEE 802.11p, such as intermittent coverage and lower penetration rate. Major stakeholders have been testing the LTE technology for specific road safety applications and traffic efficiency messaging, such as nearby road hazards and traffic alerts over large coverage areas [33].

IV. Adoption of ITS Technologies in Brazil

In Brazil, the implemented ITS covers the dimensions of operation and road services [71]: the traveler; in-transit vehile; support systems; coordination and management systems. The Brazilian ITS communication infrastructure is shown in Figure 8.

Information about general traffic conditions is available to users by means of variable message signs and data centers (Wifi services, web portals and mobile applications). The system can also identify travelers through license plate recognition, transponders (RFID tags), MAC address from mobile devices and from shared tracking data between private and public organizations in association with road management companies. The vehicular control system can identify and monitor vechicles based on their goals (emergency, commercial use, personal use or road operation management vehicles). Besides, the system enables in-vehicle communication through open access networks among vehicles endowed with collision warning systems, which can inform (without human interference) accidents to operational control centers and roadside assistance or emergency vehicles. The structure system to support road operation is composed of field equipments devoted to communication and monitoring, e.g., sensors for counting vehicles, surveillance cameras, general telemetry (such as a weather station), tolls and elements for vehicle classification [71]. Brazil has only one OCC (Operations Control Center) for managing road operations, emergencies and maintenance. Public transport, tolls and commercial fleet management are not under the responsibility of OCC, which requires the implementation of communication subsystems through traffic data telematic infrastructure for communication, monitoring and managing protocols to help decision making [71]. Cameras, speed controllers, and traffic count are currently widely explored on Brazilian highways [72]. The electronic identification of cargo vehicles is under way and the enrolment of drivers is mandatory. Drivers must show the National Register of Road Freight Carriers (RNTR) and in the near future, by means of installed RFID (Radio-Frequency Identification) tags into those vehicles, it will be possible to identify them in order to control overload and minimize cargo theft. The remote operation will be carried out right after the identification and within the OCC of each of the road concession companies wherein Integrated Automation Systems (IAS) will be employed, such as video surveillance, cameras for the automatic recognition and identification of license plates, identification tag readers, roadside variable message signs to display the mandatory entrance to the weigh station and electronic display panels inside the patio from the surveillance checkpoints. Those displays will guide and inform drivers about the overweight and the means to solve the issue [72]. The "SEMPARAR" (Non-Stop) system allows the automatic identification of vehicles, Multi-lane Free Flow, Optical Character Recognition and Mobile resources. It works at the frequency range of 915 Mhz and 5.8Ghz [73].

A standard for communication between field and centralized equipments on Brazilian highways has been defined by the National Agency of Land Transportation (ANTT) through the resolutions 3,323/09, 3,323/09-a and 3,576/10. NTCIP (National Transportation Communications for Intelligent Transportation System Protocol) is a protocol designed from technical standards published by the American Association of State Highway and Transportation Officials (AASHTO). This protocol allows the "center do field" (C2F) or center to center (C2C) communication, which allows the exchange of information between equipments and control centers or among control centers, integrating different agencies. Despite being similar to the IP protocol, the NTCIP provides a dictionary of specific functional data to be used in smart transport systems, simplifying data communication between devices, as well as the installation and configuration of equipments, which allows these systems to be highly interoperable and scalable [71]. Deployment of VANETs in the Brazilian context can follow different directions. This will depend on the public policy that the government will adopt regarding this technology. Possibilities could range from private and public partnerships, which could allow the financial solution for development costs based on strategies to guarantee road safety; or place the radio electromagnetic spectrum for vehicle-to-vehicle communication purposes in a public tender offer. This paper aims at opening academic discussions about these different approaches and bringing to this context current local experiences and success stories from external realities. For example, Michigan University has been studying the transition to a new world of connected and automated vehicles and their work goes beyond technology [74]. Hence, the concept of VANETs is not restricted to the type of medium access technology or routing protocol that may be explored, but the impact that it is going to have on each element of the society. In the Brazilian context, there is a Traffic Engineering Company, Companhia de Engenharia de Tráfego (CET) [75], which is owned by the São Paulo City Hall. It monitors all the intersections with high vehicular load and, this way, can contribute with vehicular data to the civil society for road safety issues, traffic management, etc. Nevertheless, this data does not provide vehicular information to drivers in real time. In other words, it is demonstrated that developing cutting-edge technologies with no interaction with other agents involved in a vehicular environment does not solve the real problem, i.e., preventing accidents. On the other hand, the emergence of applications of GeoReferencing [76], in which drivers interact with each other, by notifying the community that there is an ongoing
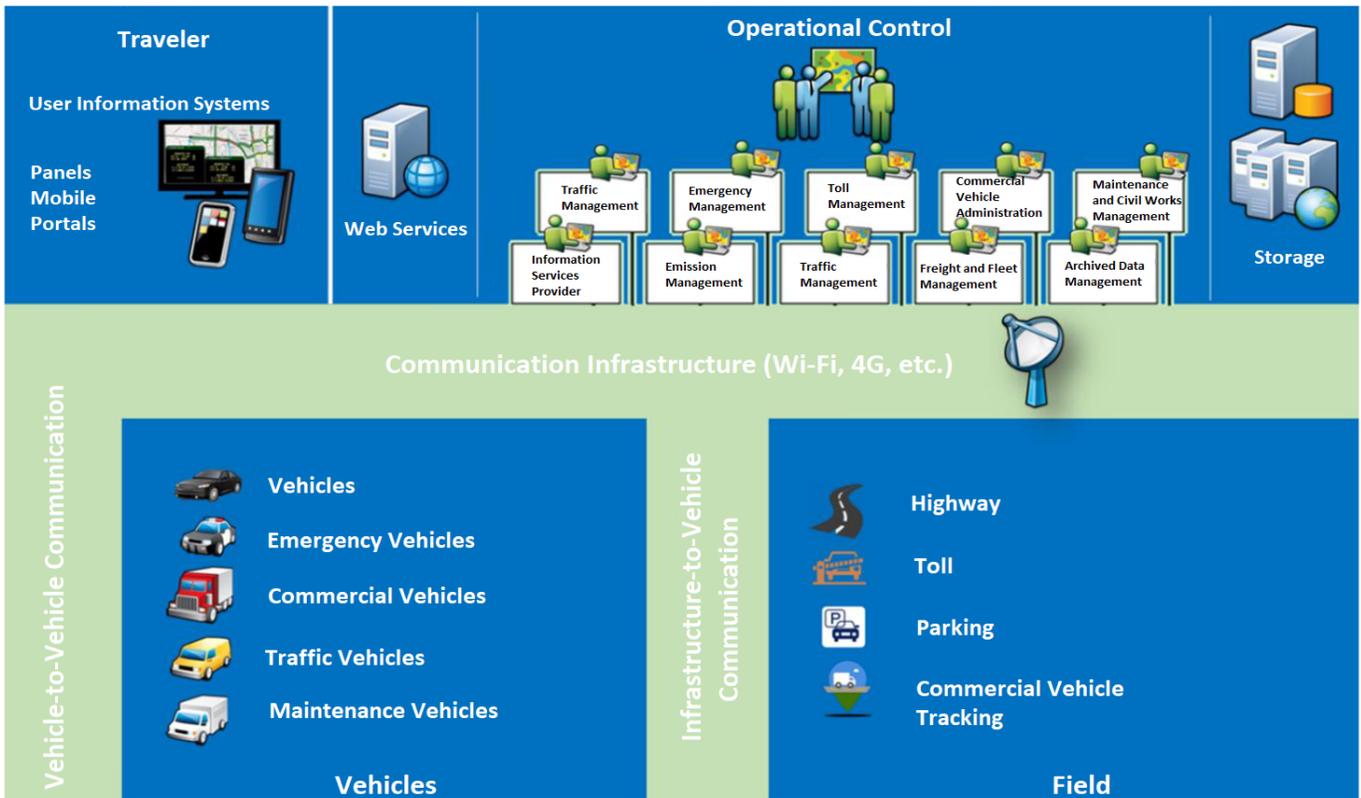
Fig. 8. Brazilian ITS communication infrastructure. Adapted from [71].

operation on a street, the existence of radars or even that an accident happened nearby. Information generated by this type of technology can be fake or cheat because there is no authority who verifies the veracity of posts from users. Again, the lack of communication among users and government agencies is not profitable for the society.

V. TECHNICAL ASPECTS AND CHALLENGES OF VEHICULAR COMMUNICATION

A. Technical Aspects of Vehicular Communication

Smart mobility has a massive interaction with technological advances in the future-driven fields of robotics, artificial intelligence, manufacturing (Industry 4.0), sustainability and global connectivity (Internet of Things) and future vehicles will act autonomously and interact permanently. These systems should undergo a profound change from static and monolithic designs towards much more dynamic and compositional concepts with security, safety, real-time, and maintainability in mind, in order to be prepared for use cases with strict demands on dependability. The concepts must support advanced multi-core and application-specific processor architectures, protection against environmental perturbation and attacks, dynamic update mechanisms, and simplified software portability for long-term operation [29]. The adoption of vehicular communication environments will include big data, security, privacy, reliability, mobility, and standards. These issues should be addressed to make IoV highly reliable and widely adopted.

A major challenge is the processing and storage of big data created in IoV due to the large number of connected vehicles. For example, driverless cars are expected to process 1 GB of data per second. Mobile cloud computing and big data analytics will play important role in handling big data. Since IoV involves integrating many different technologies, services and standards, there is the need for data security. As an open, public network, IoV is a target for intrusions and cyber-attacks that may lead to physical damage and privacy leakages. Cars, sensors, and network hardware can malfunction. The system must deal with incorrect data, as well as faulty communications, such as denial of service attacks. As a rule, the safety of the vehicle is more important than entertainment. In a situation where vehicles are moving fast and network topology keeps changing continuously, it is a challenge to keep the nodes connected and provide them with resources to transmit and receive in real time. To accelerate adoption, standardization and interoperability are vital. The lack of standards makes an effective V2V communication more difficult. Adopting open standards will enable smooth sharing of information. Governments should participate and encourage industries to collaborate on the development of technological best practices and open international standards [77]. As discussed elsewhere [33], those authors describe communication and reliability among the technological challenges regarding vehicle communication: 1. Communication: a fully operating vehicular network will require unicast and multicast/broadcast delivery

capabilities for V2P, V2V, V2I and applications. However, this will require communication systems able to support both short-range and long-range communications. In this respect, the speed of vehicle trajectories, network density, changes in network topologies, and constrained bandwidth in vehicular networks are some of the challenges not found in smartphone internet applications. Open problems have not been fully addressed yet by the technology community, such as ensuring communication systems will not interfere with transmission schemes and how to provide low latency and high data rate for vehicular applications; 2. Reliability: it is critical that vehicular communication networks have robust and fault-tolerant softwares able to recover from connection downtime and system errors. Unlike other electronic devices that are prone to frequent hardware turnover, such as in smartphones, the computing hardware for vehicular networks (onboard units, vehicle sensors, etc) must have much longer usage once the lifespan of a vehicle is relatively high (they can last for more than a decade), whereas repair and maintenance may or may not occur according to manufacturers' guidelines. The reliability of both computing software and hardware components remains major technical hurdles which need to be solved so that car manufacturers could adopt and deploy them in large scale. It is possible to assign technological challenges to two communication environments: in-vehicle and inter-vehicle. In vehicle connectivity faces the following drawbacks [68]: harsh environment due to severe scattering in a very limited space and often none-line-of-sight. This is the major reason for extensive effort to characterize the intra-vehicle wireless channels [78]; data transmissions require low latency and high reliability to satisfy the stringent requirement of real-time intra-vehicle control system; Interference from neighboring vehicles in a highly densed urban scenario may not be negligible; security is critical to protect the in-vehicle network and control system from malicious attacks [79]. Moreover, a couple of wireless technologies have been studied to find the most convenient technique for connected vehicles. Inter-vehicle networks include DSRC, WAVE, 4G, LTE, etc, technologies which may allow the V2V, V2I, and V2R communication, regardless of being broadcast or unicast packets. The most cumbersome challenge is to combat the harsh communication environment [68] and the challenges are mainly related to ways for protocol access due to error estimates and high intensity of nodes and the underlying Physics behind vehicle mobility, power consumption, broadcasting support and self-interference, as shown in Table 4.

In urban scenarios, the line-of-sight (LOS) path of V2V communication is often blocked by buildings at intersections. On the other hand, on a highway, the trucks on a communication path may introduce significant signal attenuation and packet loss [81]. Field tests in [82] demonstrated that multipath fading, shadowing, and Doppler effects due to high vehicle mobility and the complex urban environment will lead to severe wireless loss, and with a large scale of vehicles transmitting simultaneously, the mutual interference plays an important role as well. Reference [83] presents an overview of the state-of-the-art vehicular channel measurements. It is noteworthy that there is a lack of unified channel model that can be applied for all scenarios (e.g., urban, rural, and highway), and the existing channel models, only for a specific scenario, have their own merits and deficiencies. The authors also provide suggestions for V2V communication systems based on the channel characterization. The adoption of multiple antennas, for example, would enhance the communication reliability [68]. From a network perspective it is possible to point out the following challenges [68]: 1) The network topology changes frequently and very fast due to high vehicle mobility and different movement trajectory of each vehicle. 2) Due to the high dynamics of network topology and limited range of V2V communication, frequent network partitioning can occur, resulting in data flow disconnections. 3) Surrounding obstacles (e.g., buildings and trucks) can lead to an intermittent link to a mobile vehicle. In addition to the technical challenges, in the [68]: 1) To enable various wireless connectivity, multiple radio interfaces have to be implemented, such as DSRC/WAVE, WiFi, and 3G/4G-LTE interfaces, which may incur a high cost and thereby hinder the development of connected vehicles. A unified solution to provide V2X connectivity with low cost might be required. 2) In-vehicle systems have stringent requirements on latency and reliability for control/monitoring purposes. The full adoption of V2S connectivity may not be feasible in the near future unless V2S connectivity can provide the same performance and reliability as the wired communication [84]. 3) Connected vehicle offers drivers a variety of information. However, research from [85], [86] suggests an up limit on information provided to the driver. Excessive information increases the driver's workload and hence has a negative impact on safety. Therefore, the vehicle information system has to be appropriately designed for offering information to drivers. The Brazilian infrastructure for ITS is still in its infancy and it is not yet integrated to vehicles and RSU. Nonetheless, the ITS communication from center to center through NTCIP C2C is already working [87]. Thus, there are many challenges to adapt Wi-Fi technologies to support the unique requirements of vehicular communications, such as achieving high and reliable performance in highly mobile, often densely populated, and frequently none-line-of-sight environments. The automotive and the communication industries, academia, and governments around the world have been devoting tremendous efforts to address these challenges and significant achievements have been made. Over the last decade, there have been vigorous joint efforts from the industry, academia and government to validate the DSRC technology and also to identify and address key technical and business challenges. In [10] the author provides the lattice AI which gives a solution on how to enable the sync between multiple companies, which provide connected car solutions so that they can connect with each other on a unanimous network running on machine learning and swarm algorithm, and how to share resources. This remark is in good agreement to what happened in Brazil when telecommunication companies deployed cell phone technologies into the national market by the gradual

Medium	Challenge	Proposed solution
PHY Layer	Channel Estimation in Vehicular Environments	a) Turbo receiver: Using tools from modern coding theory to deal with channel estimation errors: e.g. introduce a Turbo receiver [83]; b) Decision feedback receiver: for the case as already-decoded bits as pilots for the remaining packets to improve channel estimation by tracking the channel variations significantly better than standard non-iterative schemes.
	Time selective fading without time interleaving	It can be solved using a better coding scheme (e.g. Turbo or LDPC code). However, this indeed requests a standard change and is better to be addressed in future versions of DSRC
MAC Layer	CSMA behavior at high node density pottentialy resulting in congestion control	A natural approach to reduce congestion is to reduce the number of transmitters within the carrier sense range of each device [59], [84]–[87]. A typical scheme to balance collisions and channel utilization is to use a distributed congestion control mechanism as described in [59], [87]; Another promising method is to use a time-slotted synchronous system with a fixed set of broadcast resources. One can employ a simple MAC protocol, [88], [89] to manage which transmitters should use which resources (e.g., time slots); Slotted TDM systems are typically well suited for periodic transmissions of roughly equal size packets for prolonged durations so the addition of such "hooks" into the DSRC can be beneficial (not specified).
Multi-channel Operations	Single Radio Devices (reduced capacity to support the broadcasting of safety messages)	Many simulation studies have shown that to support vehicle safety broadcasts in typical vehicle densities, most or all of the sync interval would be required; Some studies [80], [81] indicate that even with a fully dedicated 10 MHz channel for safety and control, the channel congestion issues still remain.
	Multiple Radio Devices (The spillage of power into adjacent bands when transmitting and self- interference cancellation)	Certain techniques, which are well studied in the full duplex context, including analog cancelation and digital cancelation can be applied here.

and successful adoption in many cities. This has been shown for the implementation of cellular network technologies such as 2G, 3G, and 4G which reached, respectively, a coverage area of 100% of Brazilian cities (5570 municipalities), 96.46% (5,373 municipalities) and 74.60% (coverage reaches 4,155 municipalities) [88] through investments from companies such as Algar, Claro, Nextel Oi, Sercomtel, Tim and Vivo. They were regulated accordingly by ANATEL (National Telecommunications Agency) based on constitutional principles of economic activity, according to Art. 126 from the General Telecommunications Law, through Personal Mobile Service – SMP [89]. Therefore, it was noticed that the Government has to offer tax breaks for private companies so that they can succeed into the automotive market with less restrictions, but without any reduction in the quality and security of services provided. One of the biggest challenges for ITS is the search for a cooperative and safe environment (C-ITS), which could share data among all the applications developed by the diverse independent players [90]. The success of ITS depends on a significant number of players, such as public administration, transport authorities and companies of various segments such as vehicle manufacturers and OEM (Original Equipment Manufacturer), telecommunication companies, service providers, etc. Within the industrial and technological perspectives, ITS is considered one of the biggest challenges of the TIC community. Therefore, the presence of world standards is a key requirement for exploring its entire potential. Since 1990 standardization efforts have been evolving from various organizations such as IEEE (Institute of Electrical

and Electronics Engineers), ISO (International Organization for Standardization), CEN (European Committee for Standardization), ETSI (European Telecommunications Standards Institute), among others [72].

B. Frequency Spectrum Allocation

Even though a global harmonization of DSRC standards and its spectral allocation are not available yet, IEEE committee for standardization (Institute of Electrical and Electronics Engineers) and ETSI (European Telecommunications Standards Institute) have been working on the harmonization of standards for the North American and European regions. There is a second band for DSRC applications (915 MHz for the USA and 700 MHz for Japan), which has been mainly explored for ETC and commercial applications [8]. A complete survey on the history and description of all countries and the allocation spectrum for DSRC is out of the scope of the present study, which is focused on describing only the most important ones. A brief historical study on ITS communication in Japan and in Europe was described herein in Section 2.1. Further information on the architecture and ITS communication concepts in Japan and Europe is available elsewhere [33], [91]. Differently from wireless networks based on frequency ranges from restricted radiation equipments (ISM – Industrial, Scientific and Medical applications), the communication range employed in vehicular networks is exclusive for the DSRC protocol [47]. However, regulations for adotpting dedicated frequency ranges for DSRC in Brazil have not been established yet. Figure 9 depicts the frequency ranges for vehicular communication explored in the main ITS development communities: ITU-R,

Europe, and the United States. It may be noticed that the ITS frequencies chosen in Europe and the United States range from 5.8 and 5.9 GHz.
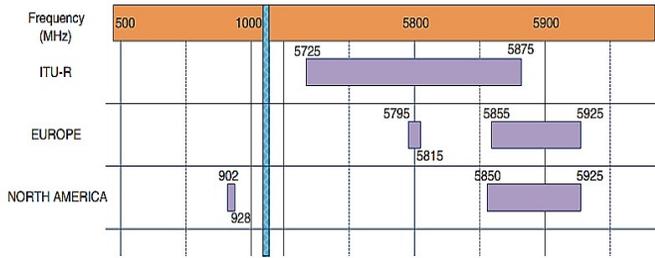

Fig. 9. Spectral range for ITS applications [55].

Regarding spectrum allocation, while FCC (United States Federal Communication Commission) and the Canadian industry allocated a radio band of 75 MHz from 5,850 to 5,925 GHz, in Europe ECC (European Electronic Communications Commitee) assigned 70 MHz from 5,855 to 5,925 GHz, whereas in Japan the allocation was 80 MHz for a band of 5.8 GHz. Nevertheless, in Japan DSRC is not compatible with the American and European standards due to the Japanese development of ETC (Electronic Toll Collection). The frequency range of 75 MHz was allocated by the FCC for vehicular communication in the frequency spectrum of de 5.9 GHz – from 5,850 GHz to 5,925 GHz, which is restricted and licensed to vehicular communications, even though it is free of charge and can be used for free as well. According to the European Telecommunications Standards Institute [92], the following frequency ranges have been reserved for vehicular communications: 5,855 GHz to 5,875 GHz (general applications); 5,875 GHz to 5,905 GHz (emergency applications and traffic security); 5,905 GHz to 5,925 GHz (reserved for future needs) [8], [56]. The standard supports four modulation techniques (BPSK, QPSK, 16-QAM, and 64-QAM). Since a transfer rate of 6 Mbps (QPSK) seems to provide a suitable balance between channel load and noise-to-signal ratio, many tests involving IEEE 802.11p in the United States rely on 6Mbps. In order to reach a higher performance in terms of DSRC communication, the system may adapt its data rate according to the distance between the vehicle and RSU. If a vehicle is away from the RSU (more than 150 km away), for example, it is preferred to send data by using a low data rate. In case the vehicle is rather close to the RSU (less than 150 m), commuting is advisable for reaching higher data rates. The SAE J2945.1 standard defines the requirements for transmitting data, transmit power control and adaptive message rate control [8] in order to allow minimum performance. In Brazil, the organization liable for regulating the automotive sector is ABNT (Brazilian Association of Technical Standards) by means of the Brazilian Automotive Committee ABNT/CB-005 [93], which works on the standardization of different automotive areas (cars, trucks, tractors, buses, mopeds, bicycles, motorcycles, autoparts and components), as well as in vehicle repairs and emissions. Nevertheless, reports or descriptions of connected vehicles or their regulation and legislation have not been found yet on the ABNT database. In terms of the legislation governing telecommunications, ANATEL (Brazilian Telecommunications Agency) is responsible for, among other duties, managing and supervising the use of the frequency spectrum. When searching its database, regulations for the use of the frequency spectrum according to WAVE/DSRC (from 5,850 to 5,925 GHz) standards were not found. By analyzing the Frequency Ranges Assignment, Destination and Distribution Plan in Brazil [94], it was noticed that the frequency ranges for Region 2 (according to ITU – International Telecommunication Union), the geographical location which includes Brazil, have similarities to those currently adopted in Brazil, as shown in Table 5. In Table 5 the labels are space-to-ground (*), ground-to-space(**) and international notes (***).

TABLE V
ASSIGNED SERVICES ACCORDING TO FREQUENCY RANGES [94]

Ranges (MHz)	Region 2 (ITU)	Brazil
5725-5830	Amateur radio	ANATEL Res. N452/2006 (D.O.U., Official Gov. publication on 12/20/2006)
	Restricted radiation	ANATEL Res. N506/2008 (D.O.U., Official Gov. publication on 07/07/2008)
5830-5850	Radiolocation Amateur radio Amateur radio over Satellite* 5.150, 5.453, 5.455***	Radiolocation Amateur radio Amateur radio over Satellite* 5.150***
5850-5925	Fixed Fixed-Satellite** Mobile Amateur radio Radiolocation 5.150***	Fixed-Satellite** Amateur radio 5.150***

The services described for assignment and destination of radiofrequency ranges (see Figure 9) are arranged in two columns: primary service (fixed, limited, etc), were written in upper case letters and secondary service (mobile, plain old telephone service – POTS, etc) were written in lowercase letters. Therefore, it is noticed that the last range (5,650 to 5,925 GHz), which should be assigned to V2X communication, is explored in Brazil for primary services (fixed-satellite) and secondary amateur services, whereas the assignment from ITU is for primary service "Mobile" (cell phones). Such terms (Fixed, Fixed-Satellite, Radiolocation and Mobile) are related to radiocommunication services defined by ITU, under its Radio regulations (RR), which can be reached at: http://www.itu.int/pub/R-REG-RR-2016. Nonetheless, the ANATEL plan contains an international footnote 5,150, which describes the frequency range of 5725-5875 MHz as also devoted to industrial, scientific and medical (ISM) applications. Radiocommunication services operating within this range should accept harmful interference arising from the use of this range for any application. Therefore, the use of frequency ranges destined by the DSRC protocol may be adopted within the national territory for vehicular applications, as well as VANET. Modeling VANET communication net-

works should consider which infrastructure would be mounted. Re-using existing infrastructure or planning new networks are viable possibilities. LTE infrastructure is well deployed in Brazil and worldwide. VANETs can rely on this network to carry information, despite sharing the same spectrum with other services, such as data, voice or video, which will be a drawback, besides high latency and less reliability [95]. New advances on LTE will allow operators to configure a Broadcast Service, LTE broadcasting or eMBMS (evolved Multimedia Broadcast Multicast Service) [96]; the operators should give up a portion of the spectrum that will be allocated for VANETs communications. The design of how much bandwidth would be allocated for VANETs is a challenge for future networks and additional tests focused on delay measurements in this technology are desirable.

C. Security Aspects in Vehicular Communication

Vehicular applications from IoT have data exchanges involving security and privacy issues [11]. Otherwise, attackers could send corrupt or subverted information aiming at wrong warnings for drivers or even wrong automatic reactions from cars in case of autonomous driving, which could give rise to accidents, injuries or fatalities. An example would be the message of electronic emergency brake light that was fabricated or replayed, which would make the receiving vehicle to immediately brake without any obstable ahead. Thus, safety mechanisms for intelligent transport systems (ITS) are crucial for supporting safety applications based on V2X communication [97]. Many applications for vehicular networks are directly related to reliable information, non-disclosure of sensitive information and the protection between the receptor and the emitter. Many attacks can be done to any kind of electrical vehicle communication, such as those summurized in Table 6.

TABLE VI
VULNERABILITIES RELATED TO CONNECTED VEHICLES [98].

Category	Vulnerability		
V2S	DoS, Jamming, False data injection, GPS deception		
V2V	DoS, Selfish attack, Modification, Sybil attack, False data injection, Eavesdropping, Black Hole, Gray Hole and Wormhole attack.		
V2I	Replay, Router Advertisement Forgey, Privacy, RSU Spoofing, DoS of the DAD		
V2N	Mobile Femtocell	MOBIKE	DoS, MiTM, Spoofing
		Femtocell	Physical Attacks, Configuration Attacks, MiTM, DoS, privacy, among others
	5G		Mmwave and D2D: Eavesdropping, privacy; jamming attack

According to [98], the communication attacks can be classified according to the communication category, as: Vehicle to Sensor (V2S) attacks – attacks that affects the sensitive data between sensor and vehicle and directly impacts on Urban Platform for Connected Electric Vehicles due to wired communications which are vulnerable to malware, enabling third part to control the communication interface, e.g. CAN bus. It can result in essential services damaged and system failture, i.e. Denial-of-Service attack (DoS) [99]. For Wireless Sensor Network (WSN) attacks, a malicious node can seriously cause malfunctioning of the vehicle operation by executing attacks on the vehicle sensor network such as jamming attack (malicious nodes block legitimate communication by causing intentional interference in networks [100], false data injection attack (sending false data from sensors to ECU), Global Positioning System (GPS) deception (fase information about vehicle location or GPS around) and DoS (uninterrupted message bombarding to ECU); Vehicle-to-Vehicle (V2V) attacks: attacks on communication between two or more vehicles and can be classified as selfish attack (refusing to send or receive message with vehicles or server or message not reaching all vehicles if selfish nodes increase), modification attack (modify or alter content of message sent to server), sybil attack (multiple identities and from different positions to inject false information in the network), false data injection attack (a node sending information to vehicles around to affect the prediction in the server), eavesdropping (detect sensitive information by an unauthorized node about a vehicle and leading to privacy attacks), Black Hole attack (putting a sender node into erroneous condition of shortest path [101], [102]), gray hole attack (extension of black hole attack but dropping messages in a selective way), wormhole attack (by revoking legitimate links between vehicles and hence any data transmitted between legitimate vehicles will pass through the attacker [103]), denial-of-service (when attacker try to cause failure to the system's operation); Vehicle to Infrastructure (V2I) attacks: replay attack (through replaying old messages to neighbors resulting in causing connection failure), router advertisement forgery (forging a router advertisement- RA message with an invalid next hop), privacy attack (assuming that the prefix sent by the RSU in the RA message remains unchanged and prefix is associated to a geographic area, a malicious node on the Internet can create a map based on this association), RSU spoofing (spoof the IP address of the RSU and send an invalid prefix), Duplicate Address Detection (this mechanism is vulnerable to a denial of service attack). The attacker responds to all address duplication detection messages that it has already taken the requested IPv6 address [104]). Vehicle to Network (V2N) attacks: DoS on the roadside WiFi Access Point (WiFi AP), MOBIKE vulnerability - many attacks can be performed on MOBIKE such as Denial of Service (DoS), Man-in-the-Middle (MiTM) and spoofing attacks [105]. Besides that, mobile Femtocell is based on femtocell (Home eNodeB (HeNB) [106]) and it can be subject to several types of attacks as Physical Attacks (the hacker can modify or replace HeNB components), Configuration Attacks (misconfiguration of the Access Control List – ACL - of the targeted HeNB), Protocol Attacks (e.g. man-in-the-middle attacks on HeNB), DoS on Mobile Operator's Core Network, User Data and Identity Privacy Attacks, Radio resource management tampering [107]; 5G technology can be perceived as a revolution for Vehicle to Network communications, even considering vehicles are able to connect to the 5G cellular

network through direct links with the mmWave small cells or by via other devices using D2D communication. The mmWave and the D2D can be subject to the eavesdropping attack [108]. The authors in [109] classify next-generation networks (e.g. 5G) as vulnerable to the jamming attack since they are based on the densification (ultra-dense networks - UDNs). Spoofing attacks have been reported [110], as well as PII (Personally Identifiable Information) and SPI (Serial Peripheral Interface) leaks were some of the threat types for IoT (Internet of Things) in-car WiFi smart appliances. Such attacks could turn cars into mobile hotspots, connecting passenger devices to the Internet and grabbing sensitive information. Some studies have shown some security requirements should be found in vehicular communication environments. These requirements are [97]: 1. confidentiality: overall, V2X communication tries to improve the awarness of car's surroundings, such as the existence of other cars or hazards, for example. Therefore, vehicular communications are typically open, since confidentiality represents a minor requirement. Only some specific issues such as transactional applications (e-tolling, pay-per-view, for example) will require confidentiality. 2. integrity: V2X messages are the basis for decision making, such as in warning drivers or trigerring an automatic response from the vehicle. The latter requires messages in their integrity. Assuring messages were not manipulated may be carried out by using integrity mechanisms, such as digital signature, for example, which has been explored in current Telecommunications Standards [92]; 3. authentication: each message sent over a vehicular network may be authenticated to prevent malicious attackers from inserting messages. The authentication is usually provided by digital signatures and public key infrastructures; 4. Availability: V2X communication must be available for real-time safety applications. Nonetheless, this is a hard task considering that jamming is likely to happen in wireless communication [111]; 5. Protection of privacy: even though there are some requirements for authentication, as described before, vehicles and drivers should not be identifiable, otherwise the location profiling of drivers could be exposed; 6. liability or non-repudiation: this feature requires that any receiving entity could prove to third parties the message was sent by a unique sender. This is somewhat challenging when confronted with privacy protection and the fact that authorized entities, such as those responsible for law enforcement, should identify vehicles or not, is currently under scrutiny. The unique characteristics of moving vehicles have been underlined and some improvement suggestions from literature have been presented elsewhere (improving transport protocols, enhancing MAC protocols for mobility related devices etc.) [68]. As described by [112] main constraints under which VANET must operate, as well as the security requirements: authentication, availability, non-repudiation, privacy, real-time guarantees etc. A novel privacy-preserving randomized authentication protocol is proposed by [113]. The principle of homomorphic encryption is used to allow each individual vehicle to generate its own identities. Therefore, the public acceptance and the addoption of cooperative V2V

safety applications will depend on suitable levels of security as an integral part of the system. Differently from other safety technologies, V2V safety applications are cooperative, since both vehicles must send, receive, and analyze data in real time. This cooperative data exchange about potential threats and hazards is crucial for alerting and warning drivers on their decisions and actions towards avoiding imminent accidents. This is a new paradigm which is at odds with stand-alone vehicle systems based on sensors. Nevertheless, a cooperative system can only work when participants in that system trust the alerts and warnings broadcasted by other V2V devices relying on messages from other V2V devices [5]. As described in [114], the already existing and/or proposed mitigation strategies depend on the attack type. But despite this still open emerging security problems such as the trustworthiness evaluation of nodes in VANET, data context trust and verification and so on. The DSRC, for example, received more security and privacy improvements than traditional WiFi and the connected vehicle environment is guarded by physical controls (physical protection around equipment such as tamper-proof casings), technical controls (technologies designed to protect data, such as firewalls, access management, and encryption) and administrative controls (Laws and regulations regarding unauthorized collection, storage, and disclosure of data and fair information practice principles) [5]. Moreover, the polytics for data access and its availabitlity in Brazil provides the confidence to consumers about IoT resources. This may be observed from the Laws: 1. The Brazilian Civil Rights Framework for the Internet (Law 12,965/2014) regulates the use of the internet in terms of principles, warranties, rights, duties and Government actions in order to ensure the organization and order about the Internet; 2. Brazilian General Data Protection Law (Law 13,709/2018) – this law provides on gathering, processing, protecting, and using data by a natural person or legal entity governed by public or private law, in electronic or physical support the processing of personal data. It is expected to go into effect in February 2020. These laws impose criminal and administrative penalties when the norms are violated. However, despite the existence of laws and safety protocols to be followed by information-sharing communication entities, consumers should rely on best practices regarding information security, such as those described elsehwhere [115], as well as general recommendations on information secutiry, e.g.: ensuring all security and operation systems, and technological devices are up-to-date or automatically updated when their hardware or operating system provider issues new fixes; preventig the execution of malicious code on macros (e.g. by disabling automatic runs), analyzing and improving the configuration setup (firewall, sharing, privilege levels and access permission) and generating strong-type passwords and properly store sensitive information.

D. Social Challenges

The organizations liable for managing, regulating, and supervising the National Traffic System in Brazil are public institutions composed by the entities: National Traffic Council

(CONTRAM), National Authority for Terrestrial Transport (ANTT), National transport infrastructure department (DNIT), State Traffic Department (DENATRAM), Federal Highway Police (PRF), State Traffic Council (CETRAN), Department of Roads (DER), Municipal Traffic Department, and Municipal Highway entities [116]. Therefore, the adoption of new technologies on municipal roads or Federal/State highways must undergo the scrutiny of the public jurisdiction before its implementation. This allows for a higher control over traffic infrastructure (e.g. legislation, signaling, road maintenance, and construction of new roads), monitoring traffic conditions, counting vehicles, weighing and tolling. Public institutions must be properly aligned with technological innovations for integrating the Smart Transport System. This way they would enact laws on the adoption of new technologies and vehicle services, such as the frequency spectrum, homologation of electronic equipments (electronic circuits from control circuit, processing, communication and power boards), besides motivating the integration among many technological assets (e.g. vehicles, RSU, infrastructure and personal devices). Therefore, the adoption of a vehicular communication technology will depend on the population, wherein most contributors come from, who should notice the importance of implementing the ITS traffic infrastructure, the gradual incorporation of vehicular technology and the use of information arising from data processing for social welfare, i.e., the best transport option to choose from (subway, bus or private car), traffic and weather conditions, jamming and route optimization (algorithm for predicting arrival times in mobility applications [117], [118]), so that users could reduce their travel time from origin to destination. An example is given by the progressive use of urban mobility services such as 99 (available in 1705 cities) [119], Uber (100 cities) [120] and Cabify (8 cities) [121], thanks to the alliance and mobilization of private companies and the population against polytics favoring taxi services aimed at keeping high transport costs and the restriction of using mobility applications [122]. This was possible because the population noticed the benefits from sustainable mobility arising from mobility applications (affordable prices when compared to conventional transport modes for short distances due to their low operating costs, flexibility in terms of service availability and practicality in terms of service use) and kept aligned to the interests of the companies. This achievement may be understood through methodologies and implemented actions by means of laws or resolutions devoted to make people aware of and show the feasibility of using and adopting new technologies, besides successful case studies such as that from Mcity Driverless Shuttle, developed by the University of Michigan [74] and the awareness of how sustainable urban mobility is in the city of Curitiba [123]. The compelling motivation comes from: 1. Gradual investment in preventing accidents by the use of ITS technologies in order to save 3.1 billion US dollars spent on accidents, as shown in Table 1; 2. Brazil renewed its commitment towards the United Nations, during the Decade of Action for Road Safety 2011/2020, which means reducing by half the number of traffic deaths and injuries through the National Plan for the Reduction of Deaths and Injuries in Road Accidents (Pnatrans), Law 13,614/18, according to [124].

VI. LEGISLATION, PUBLIC POLICIES AND LEGAL ASPECTS

The adoption of connected vehicles and ITS Technologies in conjuction with the increasing level of vehicular automation has economical, legal, criminal, and administrative consequences. According to [7], the economical consequences impact the allocation of vehicles, the supply chain from automakers, passenger transportation services and the income of those working as drivers, such as taxi services and mobility applications, due to the gradual replacement of the driver; on-demand use of vehicles, instead of a daily rent; and redesign of automakers to adapt themselves to the new consumption requirements without the need of a car per family member. It expected that the productivity of workers increases, once the time for daily trips from home to work and vice-versa (which means 64 minutes on average in Sao Paulo) will be reverted to production capacity by using technological resources (tablets, laptops, etc). Expected legal consequences are the implementation of the social function of property in light of car sharing, which will require usage fees, renting a vehicle and higher traffic efficiency. Finally, there is the civil responsibility and the convenience of compulsory insurance: on the basis of Negligent Entrustment, the Brazilian Superior Court of Justice (STJ) understood that the losses caused to third parties are the responsibility of the owner of the vehicle, even if it is proven that he/she has not driven it, since the owner has the intellectual command and will be responsible for damages caused to third parties independently of being considered guilty. However, in case the damage was caused by a manufacturing defect, it is legal that the owner asks the manufacturer or the company responsible for the maintenance the reimbursement of the amount of money awarded in compensation, on the basis of prohibiting unjust enrichment, according to Article 934 from the Brazilian Civil Code and on the analogical application of Article 13, sole paragraph, from the Brazilian Consumer Defense Code; the same situation happens when a consumer suffers damages arising from an accident. In such a case the legislation must be adapted for enforcing a mandatory insurance from vehicle owners. Therefore, it is noticed that the specific legislation in Brazil for the use of ITS technologies is outdated, even though it was implemented since 2009, it is still restricted to the adoption and implementation of norms, protocols, specifications and prices for highway communication infrastructure, such as ANTT n. 3,323-A on 11/18/2009 [125]. This regulation provides for the adoption of Data Communication Protocols and libraries of data standards from NTCIP (National Transportation Communications) for ITS protocols developed by the National Electronics Manufacturers Association (NEMA), in conjunction with the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE) and ANTT n. 3,576 on 09/02/2010 [87]. This resolution

provides for the specifications and prices for ITS systems (Intelligent Transportation Systems) based on Vehicular Traffic Sensing; Variable Message Signs - fixed; of Variable Message Signs - Mobile; Weather sensors; surveillance cameras (CFTV) and height detection to be adopted on Federal concession highways, regulated by ANTT [125]. However, a transport partnership between Brazil and the United States is under way, whose primary aim is to allow a technical exchange in order to boost ITS and reinforce the implementation of National Transportation Communications for Intelligent Transportation System Protocols (NTCIP), besides fostering the discussion on the evolution of the architecture and support for integrating connected vehicles [126].

VII. Conclusion and Prospects

The vehicle communication technology, mainly driven by the development of V2V, V2I, and the IoV concept, is already a reality in the aftermarket and it is possible to acquire equipments to connect vehicles and traffic infrastructure. The connectivity solutions already available in the automotive industry are restricted to V2D communication, via Bluetooth and USB connection applications. Regarding traffic infrastructure solutions, other resources were found, such as e-toll payment and the opening of gates by using RFID. Many researches and practical tests have been carried out since the late 1980s, and today the advance of scientific research is well ahead of the solutions found in the market (such as the use of 5G for V2I communication). In addition, although the current development phase of connected vehicles is not sophisticated, it allows vehicles to communicate with each other and with the traffic infrastructure. It has been found that many countries (from the European Union, the United States, Japan, and China) have their own vehicle communication standards and are implementing tests in real-life traffic situations for later standardization and description of relevant legislation for connected vehicles. This demonstrates the need for harmonization of international standards and further research on standards, vehicle experiments, development and adoption of connected vehicles more efficient and easier. During the research it was noticed that the automobile market is very restrictive in terms of adoptiing new technologies due to the costs of manufacturing and assembly, both to the automakers and to the customers and to the time required for certification and homologation of new equipments. The solution would be the use of technological resources in the aftermarket, where the user could choose the type of equipment to be used and install it in the vehicle, to make it connected. The present work aimed at the research and discussion of main studies in connected vehicles, emphasizing the state-of-the-art V2V and V2I communications. In this case, the goal for state-of-the-art technologies was reached, since many studies were searched over the main databases from the academic environment and reports from entities related to ITS. For this purpose, the article objective was accomplished, pointing out the simulation resources, devices used for vehicular connectivity and practical tests developed for communication evaluation. Research case studies were presented for academic and governmental entities and it was possible to observe a comprehensive, diversified state of the art in the field with well-defined technical specifications through the standards and norms of major regulatory institutions such as ISO, IEEE, ETSI, USDOT, and EC. However, no simulation studies were described, nor was it possible to conduct a case study to obtain all the communication requirements necessary to implement a stand-alone vehicle and to correlate the data achieved with the academic or governmental database. There is still a lot of research and development to be carried out, since the implementation of connected vehicles in real ITS environments is in the initial phase and there is a shortage of transit infrastructure and telecommunications able to support all the applications. As research and future studies, it is proposed searching for each communication requirement to keep the vehicles connected, perform simulation for operation analysis and practical tests involving vehicular applications and traffic infrastructure. Other studies can be developed based on the use of 4G and 5G technologies for broadcasting between the traffic center and the vehicles versus the use of devices connected to the Internet through IoT.

References

[1] WHO, "Global Status Safety on Road - Report 2015," World Health Organization, Tech. Rep., 2015. [Online]. Available: http://www.who.int/

[2] V. Maciel, "Óbitos por acidentes de trânsito caem pelo segundo ano consecutivo," 2017.

[3] Institute for Applied Economic Research (Ipea), "Estimativa dos Custos dos Acidentes de Trânsito no Brasil com Base na Atualização Simplificada das Pesquisas Anteriores do Ipea," *Relatório de Pesquisa do Instituto de Pesquisa Econômica Aplicada*, p. 20, 2015. [Online]. Available: http://www.en.ipea.gov.br/

[4] C. H. R. de Carvalho, "Mortes Por Acidentes De Transporte Terrestre No Brasil: Análise Dos Sistemas De Informação Do Ministério Da Saúde," *Instituto de Pesquisa Econômica Aplicada*, p. 50, 2016. [Online]. Available: http://www.ipea.gov.br

[5] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, "Vehicle-to-Vehicle Communications : Readiness of V2V Technology for Application," National Highway Traffic Safety Administration, Washington, DC, Tech. Rep. August, 2014.

[6] NHTSA, "Preliminary Regulatory Impact Analysis FMVSS No. 150 Vehicle-to-Vehicle Communication Technology for Light Vehicles," National Highway Traffic Safety Administration, Tech. Rep., 2016.

[7] C. E. E. de Oliveira and T. A. C. B. Leal, "Considerations on the Autonomous Vehicles - possible economic, urban and legal impacts," Senado Federal, Tech. Rep., 2016. [Online]. Available: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td214/view

[8] A. Chekkouri, A. Ezzouhairi, and S. Pierre, "Connected vehicles in an intelligent transport system," in *Vehicular Communications and Networks: Architectures, Protocols, Operation and Deployment*, W. Chen, Ed. Elsevier, 2015, vol. 1, ch. 10, pp. 193–.

[9] Q. Hong, E. P. Dennis, R. Wallace, and J. Cregger, "Global harmonization of connected vehicle communication standards," Michigan Department of Transportation and the Center for Automotive Research, Tech. Rep., 2016.

[10] K. Ranjan, "The Lattice: An intelligent grid for connected car Industry," in *2017 IEEE Transportation Electrification Conference (ITEC-India)*, IEEE, Ed., 2017, pp. 1–5.

[11] R. A. Badea and L. Stanciu, "A Survey and Research Model for Vehicular Communication and Security Challenges," *2018 International Conference on Communications (COMM)*, pp. 291–296, 2018.

[12] J. Greenough, "THE CONNECTED CAR REPORT : Forecasts , competing technologies , and leading manufacturers," 2016. [Online]. Available: https://www.businessinsider.com.au/connected-car-forecasts-top-manufacturers-leading-car-makers-2016-4

[13] Statista, "Projected size of the global connected car market in 2016 and 2021, by segment (in billion euros)," 2016. [Online]. Available: https://www.statista.com/statistics/297816/connected-car-market-size-by-segment/

[14] G. V. Research, "Connected Car Market Size To Reach $180.30 Billion By 2022," 2016. [Online]. Available: https://www.grandviewresearch.com/press-release/global-connected-car-market

[15] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Enabling Mobile And Wireless Technologies For Smart Cities: Vehicular Social Networks: Enabling Smart Mobility," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 49–55, 2017.

[16] R. Molina-Masegosa and J. Gozalvez, "LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications," *IEEE vehicular technology magazine*, no. December, 2017.

[17] K. A. Rahman and K. E. Tepe, "Towards a cross-layer based MAC for smooth V2V and V2I communications for safety applications in DSRC/WAVE based systems," *2014 IEEE Intelligent Vehicles Symposium (IV)*, pp. 969–973, 2014.

[18] R. F. Atallah, M. J. Khabbaz, and C. M. Assi, "Vehicular networking: A survey on spectrum access technologies and persisting challenges," *Vehicular Communications*, vol. 2, no. 3, pp. 125–149, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2015.03.005

[19] H. Chenguang, Z. Kaiyu, and W. Shouming, "Analysis of the channel capacity with shadowing fading in VANET," *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 577–581, 2018.

[20] P. Salvo, F. Cuomo, A. Baiocchi, and I. Rubin, "Investigating VANET dissemination protocols performance under high throughput conditions," *Vehicular Communications*, vol. 2, no. 4, pp. 185–194, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2015.07.003

[21] D. Das and R. Misra, "Efficient vehicle to vehicle communication protocol for VANETs," *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, pp. 1–6, 2014.

[22] M. Amoozadeh, H. Deng, C. N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Vehicular Communications*, vol. 2, no. 2, pp. 110–123, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2015.03.004

[23] C. Campolo, A. Molinaro, A. O. Berthet, and A. Vinel, "Full-Duplex Radios for Vehicular Communications," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 182–189, 2017.

[24] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2018.

[25] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things : A Survey The Internet of Things : A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[26] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6740844

[27] P. F. Pires, F. C. Delicato, T. Batista, and T. Barros, "Capítulo 3 - Plataformas para a Internet das Coisas," in *XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Universidade Federal do Espírito Santo, 2015.

[28] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. F. Mini, and A. A. F. Loureiro, "Data Communication in VANETs: Survey, Applications and Challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2016.02.017

[29] M. Baunach, R. M. Gomes, M. Malenko, F. Mauroner, L. B. Ribeiro, and T. Scheipel, "Smart mobility of the future – a challenge for embedded automotive systems," *Elektrotechnik & Informationstechnik (2018)*, pp. 304–308, 2018. [Online]. Available: http://dx.doi.org/10.1007/s00502-018-0623-6

[30] S. Q. YANG Fangchun, WANG Shangguang, LI Jinglin, LIU Zhihan, "An Overview of Internet of Vehicles," *China Communications*, no. October, pp. 1–15, 2014.

[31] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges and Future Aspects," *IEEE Access*, vol. PP, no. 99, 2016.

[32] K. Ullah, "On the use of opportunistic vehicular communication for roadside services advertisement and discovery," Ph.D. dissertation, University of São Paulo, 2016.

[33] A. C. Regan and R. Chen, "Chapter 2: Vehicular ad hoc networks," in *Vehicular Communications and Networks: Architectures, Protocols, Operation and Deployment*, W. Chen, Ed. Elsevier, 2015, vol. 1, pp. 29–35.

[34] E. Uhlemann, "Introducing connected vehicles [Connected vehicles]," *IEEE Vehicular Technology Magazine*, vol. 10, no. 1, pp. 23–28, 2015.

[35] IEEE Vehicular Technology Society (VTS), "IEEE Connected Vehicles Initiative," p. 2018, 2018. [Online]. Available: http://sites.ieee.org/connected-vehicles/ieee-connected-vechicles/connected-vehicles/

[36] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular Ad Hoc Networks : A New Challenge for Localization-Based Systems q," *Computer Communications*, vol. 31, pp. 2838–2849, 2008.

[37] U. Lee and M. G. Bell, "A survey of urban vehicular sensing platforms," *Computer Networks*, vol. 54, no. 4, pp. 527–544, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2009.07.011

[38] R. I. Meneguette, G. P. Filho, D. L. Guidoni, G. Pessin, L. A. Villas, and J. Ueyama, "Increasing intelligence in inter-vehicle communications to reduce traffic congestions: Experiments in Urban and highway environments," *PLoS ONE*, vol. 11, no. 8, pp. 1–25, 2016.

[39] D. Levinson, "The value of advanced traveler information systems for route choice," *Transportation Research Part C*, vol. 11, no. 1, pp. 75–87, 2003.

[40] A. Grzybek, G. Danoy, P. Bouvry, and M. Seredynski, "Mitigating flash crowd effect using connected vehicle technology," *Vehicular Communications*, vol. 2, no. 4, pp. 238–250, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2015.10.002

[41] F. R. Yu, "Transportation Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. May, pp. 3843–3844, 2016.

[42] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "IMMINENT COMMUNICATION TECHNOLOGIES FOR SMART COMMUNITIES: 5G for Vehicular Communications," *IEEE Communications Magazine*, no. January, pp. 111–117, 2018.

[43] A. Mastrosimone and D. Panno, "Moving network based on mmWave technology: a promising solution for 5G vehicular users," *Wireless Networks*, vol. 24, no. 7, pp. 1–18, 2017.

[44] J. Contreras-Castillo, S. Zeadally, and J. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet of Things Journal*, vol. 4662, no. c, pp. 1–1, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7892008/

[45] Z. Fantian, L. Chunxiao, Z. Anran, and H. Xuelong, "Review of the key technologies and applications in internet of vehicle," in *2017 IEEE 13th International Conference on Electronic Measurement & Instruments*, 2017, pp. 228–232.

[46] S. Andrews, "Section 9: Vehicular Communications Systems," in *Handbook of Intelligent Vehicles*, A. Eskandarian, Ed. Springer-Verlag London Ltd, 2013, vol. 53, no. 9, pp. 1093–1120.

[47] V. P. Barcelos, "Análise e Experimentaçãoo do Padrão IEEE 802.11P em Redes Veiculares Híbridas," Ph.D. dissertation, Universidade Federal de Lavras, 2014.

[48] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88 – 105, 2008.

[49] J. Luo and J.-P. Hubaux, "Nicht zu warm und nicht zu kalt," in *Embedded Security in Cars*. Springer Berlin Heidelberg, 2006, vol. 155, no. 29.

[50] USDOT, "Connected Vehicles: CV Pilot Deployment Program," 2018. [Online]. Available: https://www.its.dot.gov/pilots/cv{_}pilot{_}apps.htm

[51] L. Ward and M. Simon, "Intelligent Transportation Systems Using IEEE 802 . 11p Application Note," Rohde & Schwarz, Tech. Rep., 2015.

[52] F. Bai, H. Krishnan, and V. Sadekar, "Towards Characterizing and Classifying Communication-based Automotive Applications from a Wireless Networking Perspective," *Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, pp. 1–25, 2006.

[53] J. M. León-coca, D. G. Reina, S. L. Toral, F. Barrero, and N. Bessis, "Intelligent Transportation Systems and Wireless Access in Vehicular Environment Technology for Developing Smart Cities and Wireless Access in Vehicular Smart Cities," in *Big Data and Internet of Things: A Roadmap for Smart Environments*, N. Bessis and C. Dobre, Eds. Springer, 2014, pp. 285–313.

[54] IEEE, "P1609.0/D13, Oct 2018 - IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," IEEE, Tech. Rep., 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8509668

[55] C. S. IEEE, "Specific requirements Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5 : Television White Spaces (TVWS) Operation IEEE Computer Society," IEEE Computer Society, Tech. Rep., 2016.

[56] ITERIS, "Dedicated Short Range Communication at 5 . 9 GHz Standards Group," p. 5590, 2016. [Online]. Available: https://local.iteris.com/spc/html/std/stgrdsrc{_}5ghz.htm

[57] J. B. Kenney, G. Bansal, and C. E. Rohrs, "LIMERIC : A Linear Message Rate Control Algorithm for Vehicular DSRC Systems," in *VANET '11 Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*, no. June, 2011.

[58] A. Festag, "Standards for vehicular communication—from IEEE 802.11p to 5G," *Elektrotechnik & Informationstechnik*, vol. 132, no. 7, pp. 409–416, 2015. [Online]. Available: http://dx.doi.org/10.1007/s00502-015-0343-0

[59] T. Noltet, H. Hanssont, and L. L. Bellot, "Automotive Communications - Past, Current and Future," in *2005 IEEE Conference on Emerging Technologies and Factory Automation*, vol. 1. IEEE, 2005, pp. 985–992.

[60] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and Challenges in Intelligent Vehicle Area Networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, 2012.

[61] D. Paret, *Multiplexed Networks for Embedded Systems: CAN, LIN, FlexRay, Safe-by-Wire...* Wiley, 2007.

[62] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-Vehicle Networks : A Review," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, vol. 16, no. 2, pp. 534 – 545, 2014.

[63] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle Landscape - Architectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2018.

[64] Y. Huo, W. Tu, Z. Sheng, and V. C. Leung, "A Survey of In-vehicle Communications : Requirements , Solutions and Opportunities in IoT," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015.

[65] J. Swanson and M. Serughetti, "Using Ethernet in automotive networks," pp. 1–3, 2014. [Online]. Available: http://www.techdesignforums.com/practice/technique/using-ethernet-automotive-networks/

[66] A. Azman, S. Yogarayan, S. Leong, W. Jian, S. Fatimah, A. Razak, K. J. Raman, M. Fikri, A. Abdullah, S. Z. Ibrahim, A. Hudaya, M. Amin, and K. S. Muthu, "Comprehensive Study of Wireless Communication Technologies for Vehicular Communication," *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, pp. 314–317, 2018.

[67] M. A. Haque and M. D. Hossain, "Technology survey of wireless communication for in-vehicle applications," *SKIMA 2014 - 8th Interna-*

tional Conference on Software, Knowledge, Information Management and Applications, 2014.

[68] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected Vehicles : Solutions and Challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014.

[69] M. Ali, "Chapter 8: standards of communications in the intelligent transport systems (ITS)," in *Autonomous Vehicles*, N. Bizon, L. Dascalescu, and N. Tabatabaei, Eds. Nova Science Publishers, 2014, vol. 3, no. 1, pp. 235–246.

[70] RAMON DOS REIS FONTES, CLAUDIA CAMPOLO, CHRISTIAN ESTEVE ROTHENBERG and A. MOLINARO, "From Theory to Experimental Evaluation : Resource Management in Software-Defined Vehicular Networks," *IEEE Access*, vol. 5, 2017.

[71] ENGIMIND, "Relatório final: desenvolvimento de um manual de referência para concepção, dimensionamento e implementação de praças de pedágio em concessões rodoviárias," National Land Transportation Agency (ANTT), Tech. Rep., 2018. [Online]. Available: antt.gov.br/backend/galeria/arquivos/2018/10/16/Relatorio{_}Final.pdf

[72] L. R. Bencke, A. Luiz, F. Perez, and O. Costa, "Smart Roads: an overview of the technologies in Brazil and in the world," *iSys - Revista Brasileira de Sistemas de Informação*, vol. 10, no. 10, pp. 80–102, 2017.

[73] SemParar, "Como funciona," 2018. [Online]. Available: https://www.semparar.com.br/como-funciona

[74] D. ZHAO and H. PENG, "From the Lab to the Street: Solving the Challenge of Accelerating Automated Vehicle Testing," University of Michigan, Tech. Rep. May, 2017.

[75] CET, "Companhia de Engenharia de Trafego," 2019. [Online]. Available: http://www.cetsp.com.br

[76] Waze, "Waze," p. 2019, 2016. [Online]. Available: http://waze.com

[77] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Internet of Vehicles: An Introduction," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 1, p. 11, 2018. [Online]. Available: http://ijarcsse.com/index.php/ijarcsse/article/view/512

[78] Z. Wang and M. Hassan, "How Much of DSRC is Available for Non-Safety Use ?" in *VANET '08 Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, 2008, pp. 23–29.

[79] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC Multi-Channel Operations and Its Implications on Vehicle Safety Communications," in *2009 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2009, pp. 1–8.

[80] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, T. Zhang, and A. Bucceri, "Vehicular Communications Using DSRC : Challenges , Enhancements , and Evolution," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS/SUPPLEMENT*, vol. 31, no. 9, pp. 399–408, 2013.

[81] M. Boban, T. T. V. Vinhoza, M. Ferreira, J. Barros, and O. K. Tonguz, "Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, no. June 2014, 2011.

[82] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5 . 9 GHz Frequency Band," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 25, no. 8, pp. 1501–1516, 2007.

[83] C. F. Mecklenbrauker, J. Karedal, A. Paier, T. Zemen, and N. Czink, "Characterization and Its Implications for Wireless System Design and Performance," in *Proceedings of the IEEE*, vol. 99, no. 7. IEEE, 2011.

[84] C. U. Bas and S. C. Ergen, "Ultra-wideband Channel Model for Intra-vehicular Wireless Sensor Networks Beneath the Chassis : From Statistical Model to Simulations," *14 IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, vol. 62, no. 1, pp. 14–25, 2013.

[85] J.-M. Girard, N. Tricot, K. Younsi, and J.-C. Popieul, "When does the driver workload reaches its limits?" in *Proceedings of the 2006 IEEE Intelligent Transportation Systems Conference*. Toronto: IEEE, 2006, pp. 578–583.

[86] C. Wu and Y. Liu, "Queuing Network Modeling of Driver Workload and Performance," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, vol. 8, no. 3, pp. 528–537, 2007.

[87] N. L. T. A. (ANTT), "Resolução 3576 Resolução nº 3576 , de 02 de setembro de 2010," 2010. [Online]. Available: http://portal.antt.gov.br/

[88] IBGE (Brazilian Institute of Geography and Statistics), "Brazil - Panorama," Brasilia, p. 1, 2018. [Online]. Available: https://cidades.ibge.gov.br/brasil/panorama

[89] N. T. A. (ANATEL), "Mobile Telephony - Municipalities served," 2018. [Online]. Available: http://www.anatel.gov.br/setorregulado/telefonia-movel/115-universalizacao-e-ampliacao-do-acesso/telefonia-movel/423-telefonia-movel-municipios-atendidos

[90] M. Picone, S. Busanelli, M. Amoretti, F. Zanichelli, and G. Ferrari, *Advanced Technologies for Intelligent Transportation Systems*. Springer, 2015.

[91] S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey," *IET Networks*, vol. 3, no. 3, pp. 204–217, 2014. [Online]. Available: http://digital-library.theiet.org/content/journals/10.1049/iet-net.2013.0065

[92] E. T. S. I. (ETSI), "Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part," European Telecommunications Standards Institute, Tech. Rep., 2011.

[93] Brazilian Association of Technical Standards (ABNT), "ABNT / CB-005 - Brazilian Automotive Committee," 2018. [Online]. Available: http://www.abnt.org.br/cb-05

[94] National Telecommunications Agency (ANATEL), "Plan of attribution, destination and distribution of frequency bands in Brazil," Tech. Rep., 2017. [Online]. Available: http://www.anatel.gov.br

[95] L. Zhang, Y. Wu, G. K. Walker, W. Li, K. Salehian, and A. Florea, "Improving LTE eMBMS with extended OFDM parameters and layered-division-multiplexing," *IEEE Transactions on Broadcasting*, vol. 63, no. 1, pp. 32–47, 2017.

[96] D. Lecompte and F. Gabin, "Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: Overview and Rel-11 enhancements," *IEEE Communications Magazine*, vol. 50, no. 11, pp. 68–74, 2012.

[97] F. Kargl and J. Petit, "Chapter 9: Security and privacy in vehicular networks," in *Vehicular Communications and Networks Architectures, Protocols, Operation and Deployment*, W. Chen, Ed. Elsevier, 2015, vol. 1.

[98] Y. Fraiji, L. Ben Azzouz, W. Trojet, and L. Saidane, "Cyber security issues of Internet of electric vehicles," *IEEE Wireless Communications and Networking Conference, WCNC*, vol. 2018-April, pp. 1–6, 2018.

[99] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networksPractical examples and selected short-term countermeasures," *Reliability Engineering and System Safety*, vol. 96, no. 1, pp. 11–25, 2011.

[100] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, vol. 17, no. 4, 2014.

[101] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annales des Telecommunications/Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[102] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, and Y. Xiong, "Security and Privacy in the Internet of Vehicles," *Proceedings - 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things, IIKI 2015*, pp. 116–121, 2016.

[103] B. Lipiński, W. Mazurczyk, K. Szczypiorski, and P. Śmietanka, "Towards Effective Security Framework for Vehicular Ad-Hoc Networks," *Journal of Advances in Computer Networks*, vol. 3, no. 2, 2015.

[104] N. A. Sahloul, L. Benazzouz, and I. Aouini, "Towards an IPsec security GeoNet Architecture," in *Network of the Future NoF'12*, 2012.

[105] S. Namal, M. Liyanage, and A. Gurtov, "Realization of Mobile Femtocells : Operational and Protocol Requirements," *Wireless Personal Communications*, pp. 339–364, 2013.

[106] C.-K. Han, H.-K. Choi, and I.-H. Kim, "Building Femtocell More Secure with Improved Proxy Signature," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, 2009.

[107] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Chapter 9 Security for 5G Communications," in *Fundamentals of 5G Mobile Networks*, 2015. [Online]. Available: http://openaccess.city.ac.uk/13047/Link

[108] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, vol. 65, no. 10, pp. 7868–7881, 2016.

[109] P. Gandotra and R. Kumar, "A survey on device-to-device (D2D) communication : Architecture and security issues," *Journal of Network and Computer Applications*, vol. 78, no. October 2016, pp. 9–29, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2016.11.002

[110] A. Tarabasz, "The Internet of Things – Digital Revolution in Offline Market. Opportunity or Threat?" *HANDEL WEWNĘTRZNY 2016*, vol. 4, no. 363, pp. 325–337, 2016.

[111] O. Puñal, A. Aguiar, and J. Gross, "In VANETs We Trust ? Characterizing RF Jamming in Vehicular Networks," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications,VANET'12*, 2012, pp. 83–92.

[112] N. K. Chaubey, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study," in *International Journal of Security and Its Applications*, vol. 10, no. 5, 2016.

[113] W. Jiang, F. Li, D. Lin, and Elisa Bertino, "No One Can Track You : Randomized Authentication in Vehicular Ad-hoc Networks," *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom) No*, 2017.

[114] H. Hasrouny, A. Ellatif, C. Bassil, and A. Laouiti, "VANet security challenges and solutions : A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2017.01.002

[115] CERN, "CERN Articles on Computer Security," 2018. [Online]. Available: https://security.web.cern.ch/security/training/en/CERNArticlesOnComputerSecurity(2018).pdf

[116] L. E. d. S. Cardoso, "Sistema Nacional de Trânsito," 2015. [Online]. Available: http://www.conteudojuridico.com.br/?artigos{&}ver=2.52617{&}seo=1{%}3E

[117] Y. Jia, W. Xu, and X. Liu, "An Optimization Framework For Online Ride-sharing Markets."

[118] S. Banerjee, D. Freund, and T. Lykouris, "Pricing and Optimization in Shared Vehicle Systems : An Approximation Framework," in *EC '17 Proceedings of the 2017 ACM Conference on Economics and Computation*, 2017.

[119] 99app, "Cidades: Veja as categorias da 99 em sua cidade," 2018. [Online]. Available: https://99app.com/sobre-a-99/cidades/

[120] Uber, "Descubra quais cidades do Brasil têm Uber," 2018. [Online]. Available: https://www.uber.com/pt-BR/blog/em-quais-cidades-a-uber-esta-no-brasil/

[121] Cabify, "Cidades Cabify. Conheça todas as cidades onde operamos." 2018. [Online]. Available: https://cabify.com/pt-BR

[122] A. Boadle, "Uber, rival apps join forces in Brazil to stem tide of regulation," 2017. [Online]. Available: https://www.reuters.com/article/us-uber-brazil/uber-rival-apps-join-forces-in-brazil-to-stem-tide-of-regulation-idUSKBN1D71KE

[123] H. d. F. Miranda and A. N. R. da Silva, "Benchmarking sustainable urban mobility : The case of Curitiba , Brazil," *Transport Policy*, vol. 21, pp. 141–151, 2012.

[124] J. M. de Araujo, "Plano nacional de redução de mortes e lesões no trânsito," 2018. [Online]. Available: http://www.ctbdigital.com.br/artigo/plano-nacional-de-reducao-de-mortes-e-lesoes-no-transito-por-julyver-modesto-de-a

[125] N. L. T. A. (ANTT), "Resolução ANTT nº 3.323-A de 18/11/2009," Agência Nacional de Transporte Terrestre (ANTT), Tech. Rep., 2009. [Online]. Available: http://www.normasbrasil.com.br/norma/resolucao-3323-2009{_}109723.html

[126] U. D. o. T. (USDOT), "The U . S . Brazil Multimodal Intelligent Transportation Systems (ITS) Workshop," p. 8339, 2017. [Online]. Available: transportation.gov/office-policy/international-policy-and-trade/us-brazil-multimodal-intelligent-transportation-systems