V2X Access Technologies: Regulation, Research, and Remaining Challenges

Zachary MacHardy, Ashiq Khan, Kazuaki Obana, *Member, IEEE*, and Shigeru Iwashina

***Abstract*—As we edge closer to the broad implementation of intelligent transportation systems, the need to extend the perceptual bounds of sensor-equipped vehicles beyond the individual vehicle is more pressing than ever. Research and standardization efforts toward vehicle to everything (V2X), technology is intended to enable the communication of individual vehicles with both one another and supporting road infrastructure. The topic has drawn interest from a large number of stakeholders, from governmental authorities to automotive manufacturers and mobile network operators. With interest sourced from many disparate parties and a wealth of research on a large number of topics, trying to grasp the bigger picture of V2X development can be a daunting task. In this tutorial survey, to the best of our knowledge, we collate research across a number of topics in V2X, from historical developments to standardization activities and a high-level view of research in a number of important fields. In so doing, we hope to provide a useful reference for the state of V2X research and development for newcomers and veterans alike.**

***Index Terms*—Intelligent transportation systems, intelligent vehicles, ad-hoc networks, heterogeneous networks, network security.**

I. Introduction

TODAY we stand closer than ever to ubiquitous vehicle-to-everything communication. Projected benefits, like a drastic decrease in traffic-related fatalities, reduced logistical costs for operating vehicular fleets, and the introduction of a variety of new business models, have attracted attention from a number of different perspectives (see [1]–[5]). From national governments and large industry players to consumer-level demand, interest in cooperative intelligent transportation systems (C-ITS) has emerged from a number of different stakeholders.

The first generations of sensor-assisted vehicles are already taking to the streets and being iterated upon. Though these vehicles can handle an increasing number of road scenarios, the need to extend perceptual bounds beyond the scope of the individual vehicle has become increasingly apparent. Research regarding C-ITS communications has been under way for some time, aimed at supporting applications ranging from fully autonomous vehicle operation and essential road-safety support to traffic flow optimization and in-car delivery of infotainment services. In order to realize these goals, the coordination of a number of different entities and support for a number of modes of communication is necessary. Figure 1 illustrates some commonly identified forms of ITS communication, including vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and vehicle to network (V2N) communications, collectively referred to as vehicle to everything (V2X).

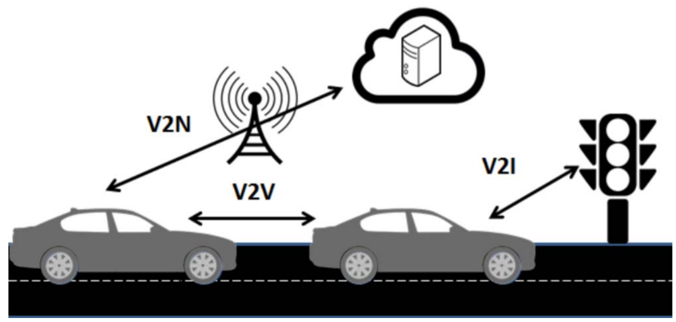

Fig. 1. A simple illustration of V2X communications.

Drawing upon research in the field of mobile ad-hoc networks (MANETs), vehicular ad-hoc networks, or VANETs, have been the focus of much of the research into supporting V2X communications. Most discussions of VANET communications envision the use of dedicated short-range communications (DSRC), supported by the IEEE 802.11p standard [6]. This standard for wireless communication is supplemented by the IEEE 1609 family of standards [7], including definitions of the architecture, management structure, security, and physical access for wireless vehicular networks, referred to collectively as WAVE (Wireless Access in Vehicular Environments). Comprising communication between on-vehicle wireless transmitters referred to as on-board units (OBUs) and infrastructural road-side units (RSUs), DSRC-based communication provides a number of benefits for V2X applications, including low end-to-end latency, flexible organization due to a lack of centralized control, and relatively low cost [8]. But it is also beset by a number of issues, including service degradation in congested scenarios [9], security problems [10], [11], and difficulty coping with compromised line of sight [12]. Though some of these concerns may be alleviated by a robust infrastructure of RSUs, it is as of yet unclear who will be responsible for the costs associated with their construction and maintenance [13], and by when and to what extent such infrastructure will be deployed. Nonetheless, DSRC is the longest considered candidate for V2X, and has been

Manuscript received March 29, 2017; revised September 15, 2017 and December 28, 2017; accepted February 1, 2018. Date of publication February 21, 2018; date of current version August 21, 2018. *(Corresponding author: Ashiq Khan.)*

The authors are with Smart ICT Platform Research Group, Research Laboratories, NTT DOCOMO, Inc., Yokosuka 239-8536, Japan (e-mail: khan@nttdocomo.com).

Digital Object Identifier 10.1109/COMST.2018.2808444

proposed as a mandated standard by the U.S. Department of Transportation (USDOT) [8], as well as the subject of intensive standardization effort by the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN) [14], and the Association of Radio Industries and Businesses (ARIB) [15], among others.

Another candidate access technology for V2X is the mobile cellular network, a proposition often referred to as Cellular V2X (C-V2X). The 'mobile cellular network' here can be taken as referring to both current LTE technology (encompassing both LTE and LTE-Advanced [16]) and potential future 5G developments, as well as older standards. Compared to DSRC, these technologies offer a number of advantages, including a much larger coverage area, pre-existing infrastructure, deterministic security and QoS guarantees, as well more robust scalability. But such advantages, many a result of a centralized architecture, come at the cost of end-to-end latency, dependence on connectivity with infrastructure, and a higher price for network usage. Particularly for V2X applications as time-sensitive as pre-crash sensing or cooperative platooning, latency-inducing overhead poses a major obstacle to the consideration of C-V2X as a viable alternative to DSRC. However, research and development efforts toward increasing the capabilities of the continue, and development of commercial technology like side-link device-to-device (D2D) communications and service-specific network slicing are well under way. Though the commercial mobile network does not yet support the peer-to-peer communications which have been the basis of V2X standardization, standardization of the technology is mature, and implementation in the near term is feasible.

Beyond these two most major candidates for V2X communications, several other technologies, including Bluetooth, satellite radio, and visible light communications have been considered for use for V2X applications. While each of these technologies has features which make it potentially promising, each also has some unavoidable limitations, as covered in Section III-D, below. An additional option is a heterogeneous network solution, combining the features of DSRC and LTE/5G in such a way as to draw upon their respective benefits while ameliorating their drawbacks. Simulation studies have shown significant performance increases across a number of network performance indicators when using heterogeneous solutions [17]–[20], but obstacles to standardization and cost considerations may limit their development and implementation [21]. It does not seem likely, as of this writing, that either the exclusive use of a cellular network or a heterogeneous solution will be the initial solution deployed for V2X communications, but be adopted gradually as V2X and cellular technology continues to advance.

A number of surveys have been written on the topic of C-ITS and VANETs, from both a general perspective and those more specifically focused on particular parts of the vehicular network. Following are a number of surveys that have been particularly valuable in grasping the past and present state of V2X research. References [22]–[24] provide general overviews of C-ITS, including contemporary information about the history, protocols involved with, applications of, and challenges to V2X based on DSRC. The surveys in [25] and [26] provide a robust overview of the breadth of wireless access technologies which could potentially be used to enable VANET communication. The survey in [21] examines the applicability of the LTE network to the C-ITS use case, with particular attention to the delivery of different message types and floating car data, as well as analyzing several preliminary studies on the topic. Alsabaan *et al.* [27] consider the potential of green VANETs, collating information on environmentally relevant topics like potential fuel savings from cooperation both with other vehicles and with infrastructural nodes. In [28], research on the application of clustering (the aggregation of nearby vehicles into distinct clusters, wherein one vehicle manages communication with other clusters, and communications are otherwise kept between only other in-cluster vehicles) to improving VANET performance is examined, accompanied by a thorough accounting of a large number of potential solutions. Whaiduzzaman *et al.* [29] consider preliminary research toward the implementation of vehicular cloud computing, a potentially rewarding field of research involving the use of the large amount of idle computational and storage resources which may be available by a C-ITS system. Recognizing the relative strengths and weaknesses of both IEEE 802.11p and LTE, [30] provides an excellent overview of the advantages of and research efforts toward the implementation of vehicular networks making use of multiple radio technologies. References [31]–[33] tackle issues of security and privacy, ranging from the potential identification and tracking of particular vehicles to the fabrication and jamming of actual message traffic, as well as the potential threat of vehicular malware and vehicular botnets. DSRC-related MAC protocols are covered in great detail in [34] and [35], covering both weaknesses of current standards and potential alternative schemes. Attalah *et al.* [36] review issues in the physical and MAC layers of VANET communication, as well as research into the applications of technology like cognitive radio for coordinating the use of unlicensed spectrum. Vahdat-Nejad *et al.* [37] present a comprehensive taxonomy of current and past C-ITS projects, the information they each consider, and a general overview of the components involved in each implementation. Though millimeter-wave (mmWave) based communications (wireless communications employing frequencies between 30 and 300 GHz) are still very much in the research and development phase, [38] gives a very detailed reckoning of the potential applicability, and related challenges of, servicing V2X communications via mmWave-based technology. Finally, [39] provides an exhaustive meta-survey of VANET surveys circa 2015, as well as a detailed general overview of C-ITS systems.

This survey distinguishes itself from those above in two key ways. First, we set out to review the applicability for V2X communications of not just IEEE 802.11p and LTE, which have been compared frequently (see [9], [40]), but also more recent advances in the mobile network including LTE-A and potential 5G access technologies. Further, rather than being a deep-dive into any one particular research topic, it is written to help give those new to the topic a general overview current research challenges across a number of potential C-ITS access technologies.

To that end, this article is intended to accomplish three main goals. The first is to impart upon the reader a general understanding of C-ITS, its history, and the goals which it is intended to accomplish. A table of the abbreviations used in this paper, which can be somewhat overwhelming for those new to the topic, can be found in Table I. The second is, to the best of the authors knowledge, survey the current state of research into V2X communication, with an eye towards the relative benefits and drawbacks of DSRC-based and mobile cellular network-based technologies. The third is to identify and collate a number of active research challenges, as well as candidate research directions. Through so doing, we hope to bring together research in a number of disparate but closely related fields, in order to contribute to a better overall understanding of where V2X research now stands and where it may yet go.

II. V2X: An Overview

V2X, short for Vehicle to Everything communication, is a specific case of ITS, dealing with wireless communication and coordination between vehicles and their environment. At the most fundamental level, ITS comprise networked systems intended to provide human consumers with safer and more efficient transportation-related services. Though sometimes used interchangeably with connected cars or V2X, ITS does not consist solely of overland road vehicles, also encompassing a number of other vehicular systems from aviation to rail networks and maritime transportation. The applications which fall under the umbrella of ITS are similarly varied, including wireless communication between vehicles, infrastructure-based coordination, on-board operational assistance and simple warning notification systems.

V2X can be taken in this paper to refer specifically to communication between overland road vehicles and other concerned entities, be they pedestrians, infrastructure, or other vehicles. As typically envisioned, this communication occurs in the context of a dynamically changing VANET, forming connections with new nodes as they come within communication range, and severing connections with old nodes as they leave it. This ad-hoc network is supported by stationary infrastructural nodes, which serve functions like collating and distributing data, helping orchestrate traffic across a large area, and providing other services which are not feasible to provide through transient V2V connections. Participants in a VANET communicate by way of a wireless transmitter carried on-board, referred to as an OBU, sending messages to and receiving them from other OBU-equipped entities and special stationary RSUs. By leveraging low-latency communications and information sharing, V2X technologies aim to help drivers of today and the autonomous systems of tomorrow coordinate more economically, efficiently, and safely.

TABLE I
A List of Abbreviations Used in This Paper

3GPP	3rd Generation Partnership Project
ARIB	Association of Radio Industries and Businesses
BSM	Basic Safety Message
BSS	Basic Service Set
CALM	Communications Access for Land Mobiles
CAM	Cooperative Awareness Message
CBR	Channel Busy Rate
CCH	Control Channel
CEN	European Committee for Standardization
C-ITS	Cooperative Intelligent Transportation Systems
CRL	Certificate Revocation List
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
C-V2X	Cellular Vehicle to Everything Communications
D2D	Device to Device Communication
DAV	Detect and Vacate (for inter-operation of Wi-Fi and DSRC)
DCC	Decentralized Congestion Control
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communication
eMBMS	evolved Multimedia Broadcast Multicast Service
EPC	Evolved Packet Core
ETC	Electronic Toll Collection
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
ITS-AID	ITS Application Identifier
ITS-S	Intelligent Transportation Systems
KPI	Key Performance Indicator
LIMERIC	Linear Message Rate Integrated Control
LOS	Line of sight
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MA	Misbehavior Authority
MAC	Media Access Control
MANET	Mobile Ad-Hoc Network
MEC	Mobile Edge Computing
METIS	Mobile and Wireless Communications Enablers for Twenty-Twenty Information Society
MIMO	Multiple Input, Multiple Output
mmWave	Millimeter Wave communications
NFV	Network Functions Virtualization
NGMN	Next Generation Mobile Networks
OBU	On Board Unit
PER	Packet Error Rate
PKI	Public Key Infrastructure
ProSe	Proximity Services
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
RACS	Road/Automobile Communication System
RSU	Road-Side Unit
SAE	Society of Automotive Engineers
SCH	Service Channel
SCMS	Security Credential Management System
SDN	Software Defined Networking
SSP	Service Specific Permissions
TCMA	Tiered Contention Multiple Access
UE	User Equipment
U-NII	Unlicensed National Information Infrastructure
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time
V2I	Vehicle to Infrastructure Communication
V2N	Vehicle to Network Communication
V2V	Vehicle to Vehicle Communication
V2X	Vehicle to Everything Communication
VANET	Vehicular Ad-Hoc Network
VM	Virtual Machine
VPKI	Vehicular Private Key Infrastructure
WAVE	Wireless Access in Vehicular Environments

A. A Brief History of Connected Cars

Though work towards semi-autonomous modern V2X applications has been confined mostly to the last two decades, the idea of wirelessly connected vehicles has been around for much longer (see Table II) [46]. Indeed, as early as the 1926, Harry Flurscheim filed a United States patent claim for a Radio Warning Systems for Use on Vehicles, heralding an interest in cooperative communication between cars via radio [42]. Though at the time radios required a higher voltage than was feasible to provide in contemporary vehicles, general purpose car-fitted radios were available as early as 1933, and had become a standard feature by the early 1940s.

While developments toward bi-directional vehicular communication were largely yet to come, unidirectional radio broadcast became ubiquitous over the following decades. The first standardized communication protocol for conveying digital information to vehicles via radio broadcast arose in 1984, called the Radio Data System [43], but vehicles still remained passive receivers of information broadcast from a centralized source. Among the variety of services offered via radio, including the radio dramas, music, and talk shows we today might classify as infotainment, traffic advisories and other radio-broadcast warnings sourced from public infrastructure also sought to provide some of the same safety-related benefits we continue to pursue today.

FM- and AM-based radio broadcast technologies left vehicles in the role of the receiver, passively listening for information from infrastructural sources. But serious efforts toward rudimentary bi-directional communication were already under way. RFID, a technology whose roots can be traced back to the identification of friendly fighter-planes in the second World War [44], was first used in tolling systems in the 1980s, allowing vehicles passing by stationary beacons to communicate their identity to infrastructural nodes [41], facilitating payment processing and automatic access control. In 1989, scientists in Japan proposed what they referred to as the Road/Automobile Communication Systems (RACS) [45]. Despite being limited to communication between vehicles and stationary road-side transmitters and relatively short-range, similarities between RACS and DSRC are notable, intended as it was to offer navigation assistance, information-distribution services and as two-way communication services [46].

A number of early efforts toward inter-vehicle communication were made in the following years. In 1991 and 1992 respectively, CEN and the International Standards Organization (ISO) set up technical committees concerned specifically with ITS, defining an architecture and infrastructure for general ITS communications systems [47]. The first major steps toward the implementation of VANETs were taken as several standardization bodies, including SAE in the U.S., CEN and ETSI in Europe, ARIB in Japan, and ISO pursued standardization of what they called dedicated short-range communications. Some details of the standards vary, particularly the channelization of the various spectrum allocations, but, in general, DSRC is intended to provide line-of sight or near line-of-sight communications between vehicular peers as well as nearby infrastructural nodes. This simplified peer-to-peer view of vehicular networking was revolutionary, as was the separation of application and network concerns, allowing for a more straightforward standardization of ITS communications systems. Many standards organizations have also pursued a broader standardization of ITS, such as ISO with its Communications Access for Land Mobiles (CALM) architecture [47], or IEEE with its WAVE architecture [48], describing a set of normative requirements for ITS communications beyond the lowest network layers.

TABLE II
MAJOR MILESTONES IN V2X DEVELOPMENT

Year	Milestone
1926	First radio-related patent for a traffic safety system.
1933	First car-fitted radio availability.
1984	The standardization of the Radio Data System, for digital transmission of important road information for motorists.
1989	Japanese scientists propose the road/automobile communication system (RACS) for navigation assistance and information distribution.
1991	CEN (Followed by ISO in 1992) establishes the first technical committee concerned with ITS.
1999	The US allocates 75 MHz of spectrum in the 5.9 GHz band to ITS-specific DSRC communications.
2004	Work begins on the IEEE 802.11p standard 2006 IEEE begins work on the related IEEE 1609 family of standards.
2008	70 MHz of spectrum are allocated by ETSI 2012 Work is finished on the IEE 802.11p standard, and it is officially incorporated into IEEE 802.11.
2016	USDOT proposes rule-making, potentially mandating DSRC roll-out by 2021.

Over the following decade, as standards developed in the aforementioned standards bodies, a variety of real-world implementations and trials were conducted, largely concerning the provision of driver-assist warning services. Utilizing communications based on the well-developed IEEE 802.11p standard (part of the same IEEE 802.11 family of technologies as Wi-Fi), coupled with the IEEE 1609-based WAVE architecture, DSRC promised to deliver what many had long been hoping for: a world of pervasive inter-vehicle communication.

While much of the global progress toward V2X was internationally coordinated, the conflict between openly developed international standards and proprietary protocols has persisted, and slightly different communications protocols have emerged in different regions, as exemplified by the adoption of the Cooperative Awareness Message and Decentralized Environmental Notification Message in the EU and the Basic Safety message in the U.S. Nonetheless, research into DSRC-based communication continues, and initial roll-outs of rudimentary DSRC systems have already begun. Toyota released its first inter-vehicle communication-enabled vehicles (operating on the 760 MHz band) in 2015 [49], and GM plans to soon follow suit with its first DSRC enabled vehicles in 2017 [50]. Looking ahead, the United States Department of Transportation released a plan which could potentially mandate the partial roll-out of DSRC-enabled vehicles starting as early as 2021, with all cars manufactured for use in the U.S. required to comply by 2024 [8].

As the DSRC standard has undergone a long evolution from concept to prototype, other wireless technologies have advanced significantly. Of particular relevance to the V2X use case are the advances made in both the mobile cellular network and the rapid expansion of the Wi-Fi industry.

Mobile networks available around the start of the DSRC standardization process were insufficient to support the stringent requirements necessary for V2X communication. However, much has changed in the last two decades. With the advent of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), also known as LTE [16], cellular networks with high throughput for both uplink and downlink traffic, low latency, and high reliability have become widely available. While the LTE and LTE-Advanced networks still do not support the ultra-low latency and ultra-high reliability required by the most demanding V2X applications, such an advance of capabilities is expected with the forthcoming 5G network. Unlike the DSRC case, which assumes the future construction of an enormous network of supporting infrastructure, LTEs infrastructure is already widespread, supporting traffic between the enormous number of users of the lately ubiquitous smart phone, among other cellular devices. Many on-board vehicular services already support cellular network access through 3G and LTE through an on-board unit typically referred to as a telematics system, which also covers other long-range communications technologies, like GPS. These systems are used today for applications including navigation assistance, fleet management, and infotainment.

However, the traffic load already being handled by mobile operators networks as well as an inherently centralized architecture pose a significant hurdle for the adoption of LTE as a V2X technology. Indeed, as will be explored later in this paper, it seems unlikely that the LTE network as it exists in 2017 could support the full range of V2X applications. In particular, tests have found LTE to fall critically short of the latency guarantees necessary for certain time-critical applications like pre-sense crash handling and cooperative platooning. But development across a number of components of the mobile network, often grouped under the somewhat ambiguous umbrella 5G, hold much promise for overcoming many of the shortcomings of LTE.

The 3GPP standardization body, in charge of the standards for 3G, LTE, and other future mobile network developments, has released a dedicated set of criteria for supporting V2X applications in future cellular networks [51], with specific reference to frequently cited requirements like sub 100 ms latency and 10Hz message frequency. Similarly, the METIS (an acronym for the somewhat unwieldy Mobile and wireless communications Enablers for the Twenty-twenty Information Society) project, part of a partnership between a large number of cellular industry players, has specifically targeted support for the V2X use case, aiming for end-to-end latency as low as 5ms for messages falling into the traffic efficiency and safety categories [52]. Though much of the 5G technology necessary to enable this performance remains in the research and prototype stages, mobile network operators and vendors of related technology have shown a strong intention to meet the constraints of the V2X use case by the year 2020.

At the same time, an explosion of consumer demand for Wi-Fi technologies, particularly faster, greater bandwidth variants like those using the 802.11n and 802.11ac standards, has resulted in significant regulatory pressure to open more spectrum for the use of unlicensed wireless technologies in both the U.S. and Europe. Such pressures have resulted in proposals to share spectrum between U-NII (Unlicensed National Information Infrastructure) and other currently licensed technologies, including DSRC. The particular point of contention is the 5.9 GHz band (5.850-5.925 GHz in the U.S. case, 5.855-5.925 GHz in the European case), currently allocated exclusively for use by vehicular applications, the sharing of which would allow Wi-Fi technologies to leverage additional high-throughput 80 MHz and 160 MHz channels. Of especial interest to Wi-Fi stakeholders is that favourable spectrum sharing overlapping with the DSRC spectrum would allow for significant gains when compared to the relatively restrictive sharing allowed with radar systems in the 5.250 GHz −5.750 GHz band. Sharing within that band requires implementation of Dynamic Frequency Selection (DFS), involving among other things, a 30 minute back off period upon detection of channel use by licensed applications [53]. While proponents of DSRC assert that prevention of interference with safety-critical V2X applications should be paramount, many critics claim under-utilization to-date of the 75 MHz band by actual V2X applications is stifling wireless innovation.

In order to address these concerns, a team of technical experts, consisting of members from both the Wi-Fi and automotive industries determined that the most promising means of implementing spectrum sharing was the Detect and Vacate (DAV) protocol. Though not as restrictive as DFS, DAV is similar in requiring Wi-Fi technologies making use of the DSRC band first ensure that the desired channel is clear before use, enforcing a back off period in the event such traffic is detected [54]. Though auto-makers have committed to carrying out testing on the feasibility of DAV, the regulatory dispute has, as of this writing, not yet been settled. Wi-Fi stakeholders are continuing to pursue a variety of means of freeing the DSRC spectrum for use by unlicensed applications, including the Wi-Fi Innovation Act resolution introduced in the U.S. House of Representatives, the passage of which would require opening the spectrum through legislative means [55].

B. *V2X Applications and Requirements*

V2X applications cover a wide variety of potential consumer needs and business models. In order to reason more effectively about the fulfillment of application requirements, it is common to group potential use-cases together by their purpose and minimum requirements. Accordingly, applications for V2X are often classified into one of four major categories.

1) Infotainment: Infotainment (a portmanteau of information and entertainment rather than an obscure typographical error) comprises a number of services intended to provide general, typically non-driving related, informative or entertaining services to drivers and passengers. These services include things like general media transfer, instant messaging between vehicle passengers, and the delivery of geo-specific advertisements. A dashboard embedded system for streaming Internet video is one example of an infotainment service, an embedded point of service for a car rental service being another. Infotainment services are characterized by relatively low minimum latency requirements (latency on the order of 500 - 1000 ms, minimum transmission frequency on the order of 1 Hz) and throughput comparable to conventional mobile broadband services, up to around 80 Mbps [56], [57].

2) Traffic Efficiency: The traffic efficiency category covers a broad range of applications intended to optimize the

TABLE III
HIGH LEVEL OVERVIEW OF V2X USE CASES AND THEIR REQUIREMENTS

Category	Use Case Examples	Latency	Throughput	Communication Frequency
Infotainment	Video Streaming, Music	500-1000 ms	80 Mbps	1 Hz
Traffic Efficiency	Navigation System, Stationary Vehicle Warning	100-500 ms	10-45 Mbps	1 Hz
Traffic Safety	Pre-sense crash warning, Vulnerable Road User Warning	20-100 ms	0.5-700 Mbps	10Hz
Cooperative Driving	Cooperative Adaptive Cruise Control, Cooperative Overtake	2-10 ms	5 Mbps	10Hz

flow of road traffic. The term 'traffic efficiency' here should not be interpreted as over-the-air efficiency of data transfer, but the efficiency of vehicular traffic over a network of roads. This can mean anything from system-level coordination of intersection timing and route planning to environmentally friendly coordination of engine use (in the case of hybrid vehicles) and the exchange of floating car data, which includes general information about geographical location, road conditions, car speed, and congestion. An on-board GPS which automatically reroutes based on traffic conditions might be one concrete example of a traffic efficiency application with relatively loose requirements. Some over-the-road traffic efficiency applications may require low-latency, robust network connections, but others should be able to degrade gracefully in the presence of network trouble, and requirements tend to fall somewhere between the traffic safety and infotainment categories (as defined in [56]), with moderate latency and throughput requirements.

3) Traffic Safety: Traffic safety applications are aimed at reducing the frequency and severity of vehicle collisions, property damage, and human casualties. This includes applications concerned with critical decision making, like coping with abnormal vehicular behaviour, protection of vulnerable road users like cyclists and pedestrians, and making allowances for the passage of emergency vehicles. The most oft-cited and perhaps the most important potential use of V2X, particularly as concerns regulatory bodies, traffic safety applications are characterized by their very strict requirements in terms of round trip latency, broadcast frequency, and packet error rate. Pre-sense crash warning, which involves the detection of an unavoidable crash and the coordination of crash mitigation among one or more vehicles, is the application in this category with the most stringent requirements. As defined by ETSI, pre-sense crash warnings require minimum round-trip latency of 50ms with 10Hz broadcast frequency [56], while the U.S. Department of Transportation defines the minimum allowable latency as 20ms [58]. While many modern implementations of traffic safety systems rely on on-board recognition systems and thus do not require an overwhelming amount of throughput to function, future applications relying on remote processing for real-time event handling may require orders of magnitude more bandwidth, further increasing the need for a network capable of robust, extremely high-throughput data transmission. For instance, some research suggests that the physical transmission of data necessary to support certain traffic safety services, like road sign and obstacle recognition, could require up to 700 Mbps of throughput between nodes in the VANET [59]. Consequently, depending on the traffic safety services which are ultimately supported, requirements for throughput may vary significantly, as reflected in Table III.

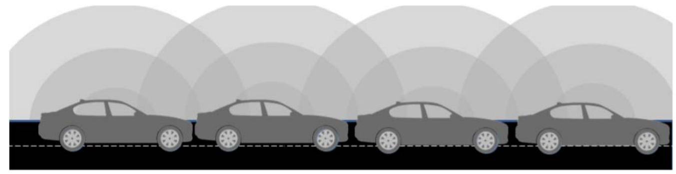

Fig. 2. Cooperative Driving use case example: Platooning.

4) Cooperative Driving: Among the applications considered by this paper, some (adaptive cruise control, cooperative platooning, etc.) are sometimes counted as part of traffic safety, above, and sometimes as a distinct fourth category: cooperative autonomous driving (see [60]). Though the case could be made that the requirements for these services are similar enough to traffic safety to merit inclusion in that category, because their requirements are particularly stringent and their applications uniquely suited to autonomous vehicle operation, we choose here to treat them separately. Co-operative platooning (the very tight packing of a group of vehicles travelling in the same direction in a lane, see Figure 2), sometimes also captured under the label of Cooperative Adaptive Cruise Control (CACC), is a cooperative driving application with very strict requirements in terms of communication latency and frequency. Supporting cooperative driving services requires throughput on the order of 5 Mbps and latency as low as 2-10 ms [57], [61].

A general accounting of use cases classified as above can be found in Table III. More detailed information about minimum requirements by service can be found in [56]–[58].

C. CAM, DENM, and BSM: V2X Message Types

While much of the technology involved in V2X communication has been well-coordinated internationally, a number of regional differences have arisen. One of the most pointed difference between the U.S. and EU V2X standards are the message sets defined for communication between vehicles. More concretely, the EU has defined two separate classes of message for vehicle safety applications: the Cooperative Awareness Message and the Decentralized Environmental Notification Message (CAM and DENM, respectively), which each serve a separate, specific purpose. In contrast, in the United States, the Society of Automotive Engineers (SAE) has defined one major class of message for V2V safety applications, the Basic Safety Message (BSM) [62]. There are also additional message classes in each region, defined for particular activities like traffic light coordination (SPAT), road sign signalling (IVI), and awareness of vulnerable road users (PSM), but we limit our scope here to describing the most essential message sets for inter-vehicle coordination. Following is a brief overview of the features of each message class, though those interested in more detail are advised to reference the CAM [63], DENM [64], or DSRC message set [65] (see also: [62]) standards.

1) Cooperative Awareness Message: The cooperative awareness message, CAM, is the message format standardized by ETSI for the regular broadcast of real-time vehicle data. This data includes information about vehicle heading, position, general information about the vehicle itself, as well as data collected from vehicle sensors, and is sent at a rate between 1 and 10 Hz, as defined in the ETSI standard. Through broadcast and reception of CAM messages, vehicles are able to keep track of their immediate environment, as well as receive information about possible, but not urgent, road hazards. Though it is specifically intended for safety, the information transmitted in the CAM is also potentially usable with non-safety related applications. Vehicle position and movement data would be essential for many traffic optimization solutions, for example.

One of the major issues with CAM distribution is the frequency at which a vehicle broadcasts beacons. Though CAM broadcast frequency defaults to 1 Hz, the broadcast rate is adjusted based on a number of criteria. This includes changes in car heading, speed, and location (a change of heading more than 4 degrees, a change in speed of more than 0.5 m/s, or a change in position exceeding 4m). The default transmission rate for CAMs is defined in the ETSI standard as 1Hz, though one can easily see that for a car travelling at highway speeds (e.g., around 100 km/h or 27.8 m/s), the vehicle will exceed the 4m change of position threshold very frequently, resulting in a de-facto transmission rate of closer to 6 or 7 Hz.

To ameliorate the effects of such frequent broadcasting on potential channel congestion, broadcast rate is additionally bounded an interval set by the Decentralized Congestion Control (DCC) function, described in [66]. DCC adjusts broadcast frequency based on occupancy of one of three states (RELAXED, ACTIVE, and RESTRICTIVE), imposing increasingly severe limits on maximum broadcast rate (as well as transmission power and data rate) as congestion increases. State transitions are the result of a measurement of channel busy rate (CBR), with greater detected congestion resulting in more restrictive states. In practice, this means that vehicles in congested areas will broadcast with significantly less frequency, decreasing congestion and allowing more vehicles to communicate.

In order to guarantee trusted message origins, CAM messages include a public key infrastructure (PKI) based certificate system, described in [67]. The security certificate attached to each CAM also includes an application identifier (ITSAID) and service specific permissions (SSP), which identify the application in use and the specific permissions of the broadcasting node, respectively. This system is in place to ensure that, for example, only verified emergency services vehicles are able to use certain functions of emergency service related applications; it stops clever, morally-flexible civilian vehicles from clearing the roadway for a faster commute.

D. Decentralized Environment Notification Message

The Decentralized Environment Notification Message, as defined by ETSI, is the event-driven counterpart to the CAM, carrying information about sudden or catastrophic road events like imminent collisions, abnormal vehicle operation, or detection of hazardous conditions. Unlike the CAM, the DENM is not broadcast on a regular basis, and so is not subject to many of the same mechanisms regulating message transmission, though it is also regulated by DCC. DENMs can be forwarded between vehicles upon receipt, allowing for the percolation of event-based information beyond the immediate neighbourhood of the originating entity. Support for this multi-hop forwarding somewhat complicates the process, as it must be ensured that the most up-to-date messages are the ones which are passed onwards, in the event of receipt of multiple DENMs regarding the same event. As an event-based message class, circumstances requiring the transmission of a DENM are not included in the DENM standard; it is left to the application layer to determine when and how to transmit it. One example of when a DENM might be utilized is in the event of the discovery of a collision blocking the movement of traffic along a particular roadway: the vehicle which first discovers the blockage would transmit a DENM including details about the location and passability, and this message would be passed to nearby vehicles within a relatively large area. Because such a road hazard would be likely to change in the near-term, the information in the message may quickly become stale. In addition to the simple broadcast of a DENM, members of a VANET can also update, cancel, or negate DENMs based on the context as judged by the application and the transmitting vehicle. DENMs make use of a certificate system very similar to that used by the CAM.

E. Basic Safety Message

Only one of many message formats described in the SAE J2735 DSRC message set standard [65], the Basic Safety Message has the fundamental role of supporting all types of V2X safety applications. Like ETSI's CAM, the BSM is broadcast with a predetermined frequency, and like the CAM, part I of the BSM contains information germane to the general operation of the vehicle such as heading, speed, position, and other vehicle-specific properties. The information transmitted in part I of the BSM is included with every transmission, and is meant to be useful to a very broad range of safety applications.

Part II of the message, on the other hand, is relatively loosely defined, intended for use with an arbitrary variety of safety applications. Accordingly, elements included in part II of the BSM are not of any particular defined order or length, and do not need to include related header information. Rather, it is meant to be used flexibly to fulfill the requirements of a given V2X application. Most commonly discussed in conjunction with Part II, as per [62], is a part of the data frame referred to as the VehicleSafetyExtension. This frame is not required to be part of a BSM, but when included, conveys information covering path history, future path predictions, GPS correction data, and one of a large set of event flags, indicating some context.

Unlike the CAM, the broadcast rate for the BSM is set to 10 Hz, rather than being adjusted based on changes in vehicular position, heading or speed. Also unlike CAM, channel congestion for the BSM is regulated with linear message rate integrated control (LIMERIC), a function which adaptively adjusts the beacon transmission rate, smoothly converging to a fair rate between vehicles [68]. The LIMERIC function linearly adjusts message transmission frequency as a function of the number of nearby transmitting nodes, avoiding the sudden and potentially congestion-inducing state changes of DCC. This means that, much like the CAM case, vehicles occupying increasingly congested areas will broadcast with decreasing frequency, but unlike CAM DCC, the rate can change smoothly, allowing for a broader range and less all-or-nothing transition from state-to-state. Though this congestion control protocol is distinct from that employed by V2X transmission in Europe, research has shown both to operate acceptably in mixed VANETs including vehicles employing a mix of both protocols [69].

III. V2X Access Technologies

Any V2X access technology must be capable of a few basic functions, namely, the transmission of basic safety and service messages between vehicular and infrastructural nodes. The most frequently studied family of wireless access technologies used in conjunction with V2X are based on DSRC and IEEE 802.11p. But there is no inherent link between DSRC and V2X communication, and, as is already the case today, much of the data passed to and from the connected car can also make use of the cellular network. Indeed, many in the telecommunications industry have already made strong overtures of support toward the V2X use-case, including industry partnership groups like 3GPP [51], METIS [52], and the 5G Automotive Association (5GAA) [70]. Choice of wireless technology need not be an either-or proposition; many analyses have shown that a heterogeneous solution can outperform either technology alone (see [17], [18], or [30] for a thorough survey).

In order to better understand the relative benefits and drawbacks of DSRC and the cellular network, it would be useful to first consider a high level view of each technology.

A. IEEE 802.11p and WAVE

IEEE 802.11p is an amendment to the IEEE 802.11 Wi-Fi specification for PHY/MAC (Physical and Medium Access Control) layer communications. Submitted to IEEE for addition to the standard in 2010 by IEEE 802.11 Task Group p [71], the 11p amendment made several changes to the IEEE 802.11 standard to accommodate inter-vehicular communications. Specifically these amendments defined the functions that are controlled by the 802.11 MAC and the functions and services that are required to operate in a dynamic environment without having to join a traditional BSS (Basic Service Set, a set of intercommunicating Wi-Fi nodes). More specific details about this amendment and the research it is founded upon can be found in [72] and [73].

The 802.11 standard does not itself define the spectrum in which DSRC communication must occur, merely describing how communication over an abstract channel must be executed. The spectrum utilized by VANETs is instead defined by various regional bodies.

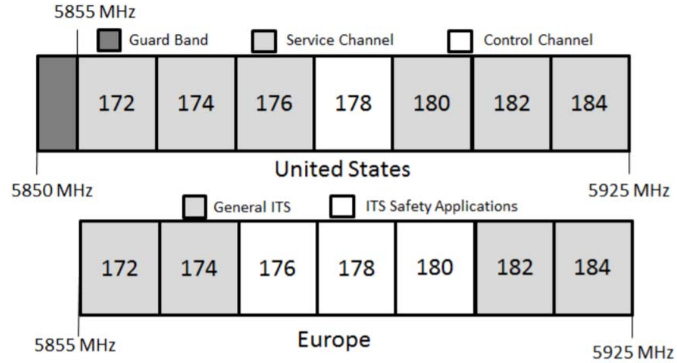

Fig. 3. Spectrum allocations for V2X in North America and Europe.

Europes ITS-G5 reserves 70 MHz (5855 MHz - 5925 MHz) for general V2X communications, of which 30 MHz (5875 MHz - 5905 MHz) is dedicated to traffic safety applications [74]. The Federal Communication Commission of the United States allocates 75 MHz of the 5.9 GHz band for V2X applications (5850 MHz - 5925 MHz), reserving one 10 MHz İControl Channelİ band (5885 MHz - 5895 MHz) specifically for vehicle safety traffic, another (5915 MHz - 5925 MHz) for public safety communication, and leaving the rest for more general use [75]. The spectrum allocations for the United states and Europe can be seen in Figure 3. Unlike its European and American counterparts, Japans ARIB allocates a single channel of the 700 MHz band (755.5 MHz - 764.5 MHz) for ITS communications [15], though the 5.8 GHz band, currently partially reserved for electronic toll collection (ETC) and similar ITS services, is a potential candidate for advanced ITS use [76]. While ETC is also under the umbrella of ITS and V2X and an important model for recent connected car technology, its V2I-specificity and relatively short range (30m) render it out of scope for the purposes of this survey.

IEEE 802.11p is further supplemented by the IEEE 1609 family of standards, collectively referred to as WAVE. The 1609 standards define interfaces and features of the V2X communication stack above the PHY and MAC layers defined by 802.11. This includes standards describing overall architecture and how to manage security (1609.2), routing (1609.3), multichannel operation (1609.4), and communications (1609.5), among other things [48]. ISO defines its own set of standards for accomplishing analogous goals, but both sets of standards apply most specifically to the vehicular security case, deferring to TCP/IP for handling other, less essential services [77].

Vehicles use IEEE 802.11p-based technology to form a VANET, which rapidly changes as vehicles come together and move apart. Vehicles regularly broadcast messages, as described in Section II-C1 above, exchanging basic information about position and movement, passing that information additionally to road-side stations and other more vulnerable road users.

The IEEE 802.11p standard makes allowances for collision avoidance based on Tiered Contention Multiple Access (TCMA), which is an extension of Carrier Sense Multiple Access with collision avoidance (CSMA/CA) which gives higher priority messages a smaller back-off time in the event that a channel is determined busy. Basically, participating network nodes listen for activity on a channel between transmissions, as defined by an inter-frame space parameter. Upon the detection of traffic on a particular channel, nodes pause for a random length back-off period, with a duration between predefined minimum and maximum back-off times. In the case of higher priority traffic, these back-off times are shorter, privileging the transmission of high priority traffic.

In order to allow vehicles with only one radio to take advantage of both safety and service-related communications, the WAVE standard allows for multi-channel operations. Described in the IEEE 1609.4 standard, channel switching allows a vehicle with a single radio to divide transmissions between the control channel (CCH), used for safety-related messages, and the service channel (SCH). These divisions are enforced over a repeating interval of 100ms, beginning at the start of a UTC second [78]. Synchronization is necessary; all vehicles must be able to transmit and receive CCH messages simultaneously, less critical messages not be received. These intervals are further buffered by a guard interval, during which transmission is disallowed to account for various timing errors and inaccuracies between vehicles.

Network composition is highly dynamic within VANETs: nodes are added to and removed from the network as quickly as member vehicles enter and leave relative proximity. This lends VANETs a topological instability, with implications for network functions like routing and addressing. This also means that many connections are severed before they can be used, particularly for multi-hop delivery [79].

In order to allow authentication between vehicles, the IEEE 1609.2 standard describes a private key infrastructure (PKI, sometimes referred to as vehicular PKI or VPKI). Already considered for a regulatory mandate by the USDOT [8], VPKI would require vehicles to carry a set of temporary pseudonymous certificates, which can be used to digitally sign V2X communications, assuring other vehicles of the authenticity of the transmitting vehicle and the validity of transmitted data. These temporary certificates are guaranteed by a Root Certificate Authority defined by the Security Credential Management System (SCMS), and are distributed on a regular basis to the vehicular fleet. The organization that will play the role of the Root Authority is as yet undetermined.

Because malicious vehicles cannot be known a priori and will initially possess a valid set of certificates, there must be a mechanism for invalidating active certificates. If a vehicle is determined to be a malicious actor, compromised, or otherwise rendered untrustworthy by the system, its certificates can be revoked by the Misbehaviour Authority (MA), thereby blacklisting it from the system. In order to distribute an up-to-date list of valid and invalid certificates, vehicles must regularly download a Certificate Revocation List (CRL), a relatively large file containing all certificate revocations, which has implications for necessary throughput and possible costs associated with data transmission [13]. It is as yet unclear what entity or entities would be in charge of running either the MA.

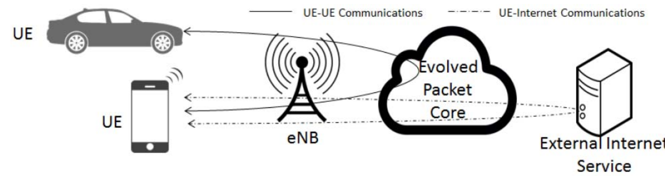

Fig. 4. A high-level view of LTE-based communications.

B. LTE and LTE-A

Compared to an ad-hoc network like one based on IEEE 802.11p, the mobile network is more centralized and less dynamic, with centralized coordination of resource allocation, mobility, and network operation. This centralization allows for relative efficiency in the coordination of transport resources, but also requires a message to traverse a number of core network nodes before reaching a destination UE (see, for example, Figure 4, with consequences for end to end latency. While the current LTE network does not provide latency guarantees sufficient to support use cases with requirements as stringent as traffic safety, forthcoming innovations like sidelink D2D communication and network slicing are set to change what is possible over the mobile network.

Sometimes referred to as 3.9G [80], LTE is the culmination of cooperative standardization efforts conducted by partner organizations across the telecommunications industry, under the auspices of the 3rd Generation Partnership Project (3GPP). Initiated in 2004, the standardization process for the initial LTE architecture was frozen in 3GPP Release 8, in 2008 [81]. Deployment of LTE began near the end of 2009 [82], and adoption of the technology quickly spread throughout the telecommunications world, with global implementation continuing today. LTE brought with it a number of important benefits, not the least of which was finally uniting carriers which had previously made use of different, incompatible 3G standards (namely, UMTS, largely used in Japan, Europe, and China, and CDMA2000, used by carriers in North America and South Korea). Though spectrum allocations for LTE differ by region, and LTE-TDD (LTE-Time Division Duplexing) and LTE-FDD (LTE-Frequency Division Duplexing) employ different transmission schemes, it is economically feasible to produce User Equipment (UE) which can operate in multiple frequencies, using either LTE-FDD or LTE-TDD. This means that phones can be manufactured for use in the global market, and has significantly positive implications for global roaming capabilities. LTE draws its improved performance from a number of enabling technologies, including an IP-based architecture comprising relatively few core network nodes (called the Evolved Packet core, or EPC) and innovations in the radio access network. Thanks to these technologies, LTE allows for both higher overall data throughput and significantly lower latency than its predecessors. Based on the 4G requirements defined by the International Telecommunication Union Radio Communications Sector (ITU-R) in the International Mobile Telecommunications Advanced (IMT-Advanced) specification, however, LTE did not meet the requirements of a true 4G network [83]. Satisfying these requirements meant increasing throughput, efficiency, and reliability when compared to LTE networks. In order to meet these increased requirements, the LTE-A, or LTE-Advanced, standard supports new communications technologies, like carrier aggregation, Multiple Input, Multiple Output (MIMO) based spatial multiplexing, and the use of small, low power relay nodes to service cell edges and improve overall coverage. Unlike 802.11p, which handles scheduling and congestion control at each device, LTE employs a centralized model, where an infrastructural base station (an evolved Node B, or eNB), coordinates the allocation of radio resource blocks. In order to initiate a connection, LTE UEs utilize the Random Access Channel (RACH), a special channel shared by UEs and used specifically to request the allocation of radio resources. At a system level, UEs communicate with the EPC in order to request service, like the establishment of a connection with an external server. In the case of establishing a data connection, the EPC, while also handling book-keeping for tasks like user mobility and user authentication, establishes a dedicated bearer, which can be thought of as a dedicated stream of IP-based traffic, between the UE and a gateway to an external network. This bearer is maintained by the EPC for the duration of the connection, then released when the connection is complete. While the LTE network was designed for use largely with conventional mobile devices, development of the capabilities of the mobile network continues, both for the specific purposes of V2X and more generally. As of this writing, according to 3GPP Technical specification 22.185 [51], standards-compliant cellular networks supporting V2V applications are required to offer end-to-end latency below 100ms, with some support for V2X communications being included in 3GPP release 14 [84], and further support forthcoming in release 15 [85]. The major focus of these new standards is supporting V2V communication via sidelink device to device communication. Sidelink device to device Proximity Services (ProSe) [86] involve the transmission of data directly from device to device, not unlike the peer-to-peer communication which occurs under the DSRC paradigm. The advantages of this technology, as opposed to traditional ad-hoc or cellular signalling, are improved spectrum utilization, energy consumption, and network throughput, as well as lower best-case latency. Unlike DSRC, ProSe-enabled UEs can establish a direct connection either through a direct negotiation of transport resources between devices or in a way intermediated by infrastructural nodes. This allows for the flexible leverage of the spectrum efficiency made possible by centralized coordination and of the reliability of ad-hoc, direct communication when infrastructural connectivity is not available.

C. 5G and Beyond

5G, unlike LTE or LTE-A, does not refer to a particular standard, but rather a collection of requirements and new technologies that are seen as the next step for mobile cellular networks. The Next Generation Mobile Network (NGMN) Alliances 5G White Paper is one of the most frequently cited sources for 5G requirements [87]. While it does not have the force of a standard, many mobile network operators and vendors are using these requirements as a target for research and development efforts. The requirements given by the 5G White Paper involve improvement along eight key KPIs: Latency, Mobility, Data-rate, Spectrum Efficiency, Capacity, Peak Data-rate, Energy Efficiency, and Support for Connection Density, most by one or two orders of magnitude. A number of technologies are vying to fulfill the promise of 5G, both in terms of wireless access capability, and core network architecture. While research into these technologies is currently ongoing, and it is difficult to make definitive statements about the capabilities of these technologies, it will be useful to survey a few of the most prominent technologies with potential application to V2X communications.

1) Millimeter Wave: Millimeter Wave (mmWave), one of the technologies currently under investigation as a key enabler of 5G wireless access, refers to communications utilizing the Extremely High Frequency (EHF) band occupying the 30-300 GHz band of the radio frequency spectrum. Prior to its application to 5G, mmWave has had a history of use in the automotive industry; for example, the 77 GHz band has already been used in the context of Long Range Radar (LRR) in automatic cruise control and other car sensor applications [88]. While it has traditionally been used in lower throughput sensing applications, mmWave is capable of providing a data rate up to several Gbps [89]. In order to reap this benefit, however, few formidable challenges remain. Common to high radio frequencies, mmWave has a very strong directional characteristics. Specifically, it requires a Line-of-Sight (LoS) connection between a transmitting and receiving car, or infrastructure element. This is difficult to achieve in mobile scenarios across different road infrastructure and geographic settings. Specifically, this means trouble for pre-sense crash warning systems that rely on wireless communication occurring in non-LOS conditions. Further, the car roof is unsuitable for antennas capable of the 360 coverage necessary for V2X applications, due to a combination of low antenna height, strong directional properties of the mmWave band, and the car itself blocking transmission [90]. A more comprehensive study focusing on the progress of mmWave data communication applications in the context of V2X services can be found in [38].

2) Network Slicing and Mobile Edge Computing: Not all requirements of V2X services need be fulfilled at the simultaneously; for example, separate virtual networks might fulfill different subsets of the 5G requirements, depending on their intended use case. One enabling technology for the fulfillment of the strict requirements of V2X, network slicing, draws on recent advancements in network function virtualization (NFV) and software-defined networking (SDN) [91]. Using network slicing, virtual, logically isolated, network slices can be created on top of physical infrastructure in a dynamic manner, allowing network operators to customize network capabilities as required by an application. Because the network slices themselves consist of virtual machines (VMs) connected over a virtualized network, the introduction of additional network resources can be executed very quickly, as it involves only the repartitioning of physical network resources, be they network links, compute cycles, or memory. These slices can be configured with the minimal set of functions necessary for a particular service: for example, a network of stationary wireless sensor nodes would not need mobility management, and thus have no need to include such functionality in the network. One specific way this technology is applicable to V2X is in the potential for the targeted application dedicated mobile edge computing (MEC) resources, sometimes referred to as the distributed cloud or 'fog' computing [92]. Such an architecture would include pools of nearby compute resources dedicated to performing processing for specific mobile services used by local mobile terminals; in the case of V2X, cars would be able to leverage these nearby resources to perform potentially costly computations involving environmental hazards without incurring the latency penalties involved in consulting a larger and more centralized, but distant, cloud. More generally, network slicing would allow for the mobile network serving vehicular terminals to be tailored specifically to the needs of V2X services, allowing for a potential solution to some of the problems (latency, capacity) associated with using the mobile network for V2X. As operators proceed with the implementation of LTE-A and look toward 5G, the capabilities of the mobile network continue to increase.

Millimeter wave, network slicing, and mobile edge computing do not, of course, comprise the full suite of technologies expected to debut for 5G networks. 3GPP is still in the process of defining New Radio for use in 5G mobile communications, and it is yet to be determined exactly what the capabilities of this new radio will be. It is likely that such developments will significantly improve the cell network's ability to handle the high capacity, throughput, and ultra low latency required for V2X. Time will tell how quickly vendors and network operators will be able to standardize, implement, and begin commercial roll-out of 5G technologies, but significant effort is being invested in beginning deployment around the year 2020.

D. Other Potential Access Technologies

Outside of cellular and 802.11p-based technologies, many other potential wireless access technologies have been considered as candidates for at least a subset of V2X services. While we cannot provide exhaustive coverage of every technology which has been or is being considered for use in a vehicular communication, a survey of some of major contenders follows, below.

1) 802.15.1/Bluetooth: IEEE 802.15.1, widely known as Bluetooth, is one of the most well-known wireless standards for short-range communication [93]. Bluetooth has already seen wide adoption as a solution for intra-vehicle infotainment systems, where external devices like mobile phones and music players can be connected to in-car entertainment systems, allowing for a variety of services to be utilized directly through an in-car interface, including phone calls, music playing, and GPS navigation. Unfortunately for potential inter-vehicle application, while the ideal maximum range of Bluetooth is 100 meters, the Personal Operating Space (POS) [93], which defines the sphere in which Bluetooth devices form networks, is limited to 10 meters. Further, while much research (e.g., [94] and [95]) has been performed toward the end of using Bluetooth for vehicular applications, it lacks many of the basic mobility support features which are required to maintain a short-range ad-hoc network in the highly dynamic context of V2X, like quickly establishing new connections with approaching vehicles. Because of this issue, and the extremely limited operational radius, it is difficult to imagine Bluetooth as a viable medium for generalized V2X communications.

2) Satellite Radio: In the context of V2X, satellite radio links have mainly been investigated to complement or augment other wireless access technologies [96], [97]. No conventional communication infrastructure is sufficient to provide coverage in all scenarios, including natural disasters and remote locations out of the range of both cellular coverage and the range of other vehicular terminals. Satellite connections are one potential solution to closing coverage gaps. However, satellite communication is quite expensive, and incurs far more unavoidable latency then most terrestrial communication methods, in the order of hundreds of milliseconds [98]. This makes satellite links explicitly unsuitable for safety applications, where a much lower latency is an explicit requirement. Additionally, despite research into antenna design suitable for use in vehicular communications [99], [100], fitting a satellite antenna without an unacceptable impact to a vehicles aesthetics or cost is also a challenge, as is the case in mmWave-based vehicular communications. Because of these limitations, it is unlikely that satellite radio will be adopted as a general-purpose medium for V2X communication.

3) Visible Light Communications: As the terminology suggests, Visible Light Communications (VLC) make use of visible frequencies of light, using the 430-790 THz band to transmit and receive information [101]. The high frequency of the spectrum allows for extremely high throughput; at present, a 10 Gbps of high speed data communication has been demonstrated using VLC [102]. One of the major benefits of VLC is that it does not cause interference with and is not affected by the already-crowded lower-frequency spectrum. The advent of Light Emitting Diodes (LEDs) has greatly facilitated research progress in VLC, and a number of different standards using visible light are already available (see [103]). Producing light consumes much less energy relative to energy consumption in radio frequency-based communication systems, and equipping a car with a VLC system has less of an adverse effect on the vehicular aesthetics and economics, since many light sources available in the car can already be used with minor visible modifications. Despite these advantages, VLC is beset to a number of problems, ranging from annoyance caused by flickering lights during data transmission, adjustment of the light source to the brightness of the transmission environment, noise from ambient and other irrelevant light sources from the surroundings, and inoperability in non-LOS conditions between the transmitter and receiver [101].

E. Heterogeneous Wireless Access

Another frequently proposed solution for V2X connectivity is a heterogeneous combination of both IEEE 802.11p and cellular access technologies. Some approaches, covered in detail in [30], use the heterogeneous approach to network connectivity for all applications, safety included, to draw upon the strengths of each respective wireless technology while tempering their weaknesses. Other approaches foresee the division of services between radio technologies, with the cellular network handling high-throughput entertainment services while DSRC handles vehicle safety. Two significant obstacles stand in the way of a heterogeneous network implementation: technical and practical considerations. From a technical perspective, operation over the composition of multiple network interfaces is a non-trivial problem. Zheng *et al.* [30] propose a solution to this problem involving the abstraction of radio access into virtual resources, mediated by a Heterogeneous Link Layer, which dispatches transmissions through appropriate technologies, but admit that the task is very complex. In practical terms, the implementation of a heterogeneous solution would require cooperative standardization efforts across a large number of industry stakeholders, including the DSRC, telecommunications, and automotive industries. While this is not an impossible task, it is certainly no mean feat, and it may introduce additional delay into a process that many stakeholders are already viewing with impatience. Nonetheless, such cooperation may be necessary for the satisfactory implementation of ITS.

IV. Challenges for IEEE 802.11p/WAVE and Cellular V2X

There are several key challenges that any candidate technology for a commercial C-ITS deployment must overcome. While, as discussed in the previous section, many technologies are in contention for use in V2X communications, we focus here on the challenges specific IEEE 802.11p and Cellular V2X, which are the most well-studied candidates for adoption by the automotive industry. While we do not offer an in-depth analysis of the challenges faced by other candidate V2X technologies discussed in Section III, challenges for each of those technologies are given in brief above, and interested readers are encouraged to refer to the given sources for a more thorough treatment of each technology. Due both to the strict requirements for latency and communication frequency, and to the safety-related nature of any C-ITS operation, we focus on several major KPIs: Capacity, latency, security, privacy, and economic considerations. Because the technical details of each potential access technology differ significantly, the challenges they face and strengths they bring to bear are often very different.

A. IEEE 802.11p/WAVE

Because IEEE 802.11p-based DSRC involves relatively short-range peer-to-peer communications, the context over which a VANET is established differs significantly from the larger scale and more centralized mobile network. This approach has many benefits thanks in large part to an independence from infrastructure and a reduction in overhead involved in authenticating with and passing through the core network. But with these strengths come weaknesses. The shorter range of communication and the lack of pre-existing DSRC equipped infrastructure means that connectivity can be unavailable in the case of sparse network density. A lack of centralized infrastructure also introduces problems with coordination, particularly in terms of channel utilization, and consequent issues with scalability of vehicular networks in congested situations. Intermittent connectivity and lack of a centralized architecture also creates problems from a security perspective, requiring each individual vehicle to be able to judge the validity and authenticity of signals received from all other vehicles. In order to better understand these challenges, it would be helpful to first take a closer look at the performance of DSRC as reported in the literature.

1) Scalability, Latency, and Reliability: Though DSRC provides reliable and ultra-low latency communication for medium-sized VANETs in LOS conditions, suboptimal conditions can quickly result in degraded performance. This degradation can be due to a number of causes, from physical impediments, like obstructions between transmitters and receivers, to inefficient coordination of radio resources.

One of the challenges faced by DSRC is a mismatch between packet length and channel coherence time, potentially resulting in elevated packet loss due to fading [104]. Line of sight conditions have also been a point of concern for VANET implementations, especially in urban environments where significant LOS obstructions are the norm rather than the exception. Huang *et al.* [105] found through empirical road testing of actual vehicles equipped with DSRC transmitters that LOS obstructions, including buildings, foliage, and other vehicles, can cause significant problems with message transmission.

Given that vehicles must coordinate safety messages over a single safety channel with finite spectrum, there is an upper bound to how many nodes can effectively communicate at a single time. Because, like other IEEE 802.11 devices, DSRC nodes are not coordinated by a central entity, they must coordinate their use of radio resources in an ad-hoc manner. Previous research has shown that when local VANETs reach sizes in the hundreds of vehicles, the delivery of messages is severely inhibited by channel congestion [9], [104], [106]. This problem is compounded by the suboptimal performance of the MAC protocol, resulting in severe degradation of network quality in terms of latency, packet error rate (PER), and consequently, throughput [107].

For example, in an early analysis of the WAVE standard, Eichler [106] show that while delay remains acceptably low for all message classes in VANETs of 150 nodes or fewer, cases involving 250 or more nodes experience an average delay of greater than 1 second, even for messages of the highest (safety-related) priority. Similarly, Hafeez *et al.* [108] demonstrate both through an analytical model and simulation results that vehicle density varies inversely with reliability, as measured by metrics like latency, effective communication range, and PER, though they did find that increasing carrier sense range relative to transmission range markedly improves the behaviour of the system. Given that real-world road situations allow for the sufficient proximity of as many as 800 road vehicles [13], it is essential that any safety-supporting technology be able to handle potentially very large numbers of vehicles.

TABLE IV
CHALLENGES FOR EACH V2X WIRELESS ACCESS CANDIDATE, IN BRIEF

KPI	802.11p-based DSRC	Cellular V2X
Latency	Not a cause for concern for 802.11p-based DSRC under normal operating conditions. An elevated packet error rate and the consequent need to retransmit messages can cause increased latency under sub-optimal conditions	When operating through infrastructural nodes (e.g. eNB, EPC), processing delay is potentially problematic. Sidelink D2D and the provision of local edge resources are potential solutions to the problem of high latency.
Capacity	Vehicular traffic congestion (several hundred vehicles within a 300m radius) can quickly cause high channel congestion and severely impact packet error rate. A potential path toward solving congestion issues may lie in improved congestion control schemes and controlling rate of transmission. Optimal data-rates in the ballpark of 6 to potentially 27 Mbps are troublingly low, and may be insufficient to support many forthcoming V2X applications	Depending on the size of the cell, frequent unicast transmission via eNB from hundreds of vehicles can cause significant congestion. Using eMBMS or sidelink D2D may solve this problem. 5G aims to support data-rates measured in Gbps, which should be sufficient for all considered V2X applications
Coverage	LOS and relatively short communication range have implications for effective coverage for 802.11p-based DSRC. Communication through intermediate infrastructural nodes (e.g. RSUs) is one potential solution to the LOS communication problem.	Coverage, particularly in mountainous and rural areas, can be inconsistent. Sidelink D2D is one potential solution to providing ubiquitous V2V coverage.
Security	Due to its ad-hoc nature, DSRC is vulnerable to a number of potential attacks on availability authenticity, confidentiality, and integrity. Some of these problems may be ameliorated by the implementation of VPKI and decentralized misbehavior detection, but many theoretical attacks, like vehicular worms and wormhole attacks, remain hard to defend against.	Cellular V2X, the outgrowth of a centralized and long-commercialized communications technology, is somewhat less vulnerable to many security problems. Some attacks, particularly attacks on availability like jamming, remain difficult to defend against.
Privacy	The use of temporary pseudonymous certificates for authenticating V2V communication provide a measure of privacy for DSRC nodes. Sophisticated eavesdropping and data interception may still pose a risk to driver privacy.	The association of cellular communications with a subscriber ID represents a potential compromise of UE privacy, particularly regarding authorities and network operators.
Infrastructure & Cost	The lack of existing DSRC infrastructure and requirement for an extra DSRC-capable module in each vehicle stand to incur significant costs, both for municipal authorities and end users.	The existing cellular infrastructure eases potential costs on municipal authorities, but high mobile data rates and cellular radios in each vehicle mean potentially high costs for end users.

The issue with congestion is at least partially the result of inefficiency at the MAC layer. Besides suffering from general issues like susceptibility to hidden and exposed terminals, the EDCA-based protocol in use with VANETs demonstrably struggles with efficient resource allocation [36]. There are a number of possible solutions to this problem of channel congestion. For example, the use of TDMA-based MAC protocols shows significant improvement over the relatively low performance of contention-based CSMA/CA conditions [35]. Alternatively, centralized control messaging could take place over a separate communication channel (e.g., the cellular network), allowing for significantly improved QoS for V2V communication.

Another challenge in the regulation of medium access is the stable adaptation of message rate, particularly for vehicles utilizing CAM DCC, standardized for use in the EU. Rostami *et al.* [109] simulated a ‘winding highway’ under LIMERIC, CAM DCC, and no-congestion-control scenarios. They found that while LIMERIC converges to approximately the target CBR, CAM DCC never actually converges, bouncing erratically between three CBR states ranging from 2 This instability in CBR results not from state-changes in the DCC algorithm, which remains in the RESTRICTIVE state for the duration of the simulation, but from the distribution of transmissions over time. That is, because vehicles tend to change states simultaneously, and because there are a relatively limited number of possible message rates, vehicles utilizing DCC for congestion control tend to produce clustered transmissions, resulting in brief spikes of CBR followed by periods of relative calm. Adjustments made to the standard show that resolution is feasible, but as ITS-G5 stands, unstable performance in congested scenarios may be the norm.

Channel switching based on IEEE 1609.4 has been suggested as one way for vehicles to access both service and safety channels, but there are many potential issues with this system. First, for the purposes of coordination, because all vehicles must transmit their messages during the interval designated for CCH use, congestion, which is already a harsh constraint under dedicated channel-use conditions, is potentially multiplicatively increased, based on the relative size of the CCH interval. Analysis by Wang and Hassan [110] shows that in order to ensure at least 95 At the very least, dynamically adjusting the CCH and SCH intervals using an algorithm like that described in [111], depending on measurements of local congestion, will be necessary in order to preserve the reliability of DSRC-based safety message dissemination.

Further, and perhaps more essentially, the standard defined in IEEE 1609.4 as a part of WAVE does not allow for a transition to cars using multiple radios [78]. Though the standard allows vehicles to stay consistently tuned to the CCH, it requires the broadcast of safety-messages during the period in which all vehicles are listening on that channel. This means that, for reasons of backwards compatibility, the presence of single-radio vehicles utilizing channel switching require even vehicles with multiple radios, capable of accessing both the SCH and CCH simultaneously, to limit broadcasting to within a shorter CCH interval, bottlenecking communications for all cars. As long as vehicles employing the channel switching strategy are on the road and supported users of DSRC communications, this problem will persist.

Multi-hop broadcast induced broadcast storms are another frequently cited concern for DSRC-based VANETs. While CAMs and BSMs are single-hop broadcasts at regular time intervals, event-triggered DENMS are intended to be distributed through the VANET over several hops. In order handle DENM distribution, vehicles forward messages upon receipt, keeping each message alive for a non-trivial length of time, until conditions have sufficiently changed or the DENM has been cancelled. A broadcast storm, a well explored property of general mobile ad-hoc networks [112], arises when a broadcast message, originating at a single node, is rebroadcast by all receivers, then rebroadcast by all of the receivers of the rebroadcast, and so on. These redundant broadcasts quickly result in severe channel congestion, stopping new messages from being reliably sent and received.

Though certainly still a concern, analysis like that in [113] has shown that regulation as simple as preventing rebroadcast by an individual node is sufficient for full message penetration with very low delay, despite potentially high collision rate. More pressing are concerns about collision with normal CAM messages, potentially impeding the normal functionality of the VANET during broadcast of event-based messages. The analysis in [114] shows that congestion can be minimized by giving DENM messages sending priority over CAMS, since doing so allows the event-based congestion to quickly finish propagating through the network, but does show an effect on CAM reception, introducing effective delays of 200 ms or greater. It is essential that DENMs be effectively and quickly disseminated through the VANET, but interference with the delivery of CAMs may be a cause for concern.

Some solutions for the issue of unreliable CAM delivery have been proposed. Xiao *et al.* [115] construct a method of error correction wherein vehicles in a VANET stochastically retransmit a subset of the broadcast messages they have received to allow their neighbours to recover messages that may have been lost due to network connectivity issues. This is demonstrated to significantly reduce the probability of packet loss, but it seems likely that these additional transmissions may have deleterious implications for already congested scenarios, in addition to increasing the actual transmission time of each broadcast. Other potential solutions, like that in [108] suggest modifying transmission power in such a way as to reduce local congestion. Still, such solutions, whether or not they are effective in practice, have not yet been incorporated into vehicular standards, meaning that early adopters of DSRC-equipped vehicles will likely be unable to reap the related benefits. While DSRC offers essentially zerocost transmissions between participating nodes in a VANET, channel congestion, Internet availability, and a relatively low ideal data-rate contribute to low availability of data for in-car services.

One additional, and particularly troubling, issue with DSRC lies in the throughput possible via the technology. In optimal conditions maximal supported data-rates top out around 27 Mbps, and optimal performance is found at 6 Mbps, to say nothing of potential congestion which would further restrict data transfer. As shown in Section II-B, Infotainment and Traffic Efficiency, and Traffic Safety applications can require upwards of 45-80 Mbps to function, at conservative estimates, and the rise of high definition and 4K video streaming may require orders of magnitude greater data-rates. Further, traffic safety applications which are now housed in-vehicle, like object recognition and automated driving, may eventually have reason to move to the local cloud, which would additionally increase the amount of data throughput required for V2X communications to function. While issues with channel congestion may be ameliorated, it is currently unclear that, even under optimal conditions with no interference, DSRC will provide communications capacity sufficient to host a large proportion of potential V2X applications.

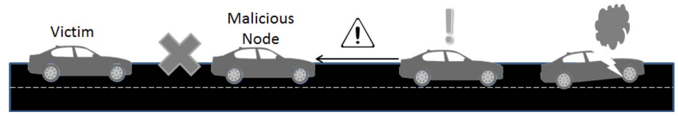

Fig. 5. Black hole attack in a VANET. In this case, a malicious node chooses not to transmit information about a road hazard ahead to following vehicles, exposing them to risk.

2) Privacy & Security: Another issue with which IEEE 802.11p-based DSRC must come to grips is the provision of secure, validated and authenticated messaging, under strict privacy-conserving constraints. This is particularly important in the case of V2V communications, where mis-calibrated sensors or maliciously spoofed data can result in congestion, elevated fuel consumption, property damage, or loss of life. The potential causes of such behaviour are multifarious; misbehaving vehicles may gain some benefit by way of tampering, or may simply intend to cause chaos among other vehicles on the road. Because the stakes are high for C-ITS, the security systems employed must be subject to accordingly high levels of scrutiny. A general taxonomy of threats to VANET security is presented below; a full review of potential VANET security vulnerabilities and their solutions are out of the scope of this more general overview, but a more thorough treatment of the subject can be found in [60] or [116].

Attacks on VANETs can be generally classified as attacks on one of five vulnerability categories: Availability, Identification and Authenticity, Confidentiality and Privacy, Integrity and data trust and Non-Repudiation and Accountability [60].

Attacks on availability, like the jamming, black hole (see Figure 5, and Sybil [117] attacks, involve interfering with the transmission and routing of packets, such that the VANET cannot function within operational constraints, degrading service and endangering lives. This category of attacks also encompasses things like vehicular malware [118]–[120] and the consequent potential for vehicular botnets [121], which could have a catastrophic impact on a fully ad-hoc V2X solution. The insecurity of the standard in-car network itself is a potential attack surface for denials of availability, as the compromise of any one component of the car is potentially enough to comprimise all other interconnected systems [122], [123]. These attacks are difficult to prevent, and though there are a number of strategies for vehicles to collaboratively detect and stem such tampering (see [124], [125]), it remains to be seen to what extent such strategies will be adopted and whether they will be practical in a real-world environment.

Attacks on authenticity, like falsified entity attacks and global navigation satellite system (GNSS) spoofing attacks, involve vehicles counterfeiting information like valid certificates or GNSS data, manipulating traffic and potentially causing injury or death to vehicle passengers. Preventing attacks on authenticity requires a strong method of authentication, not just for V2V messages, but also for other essential sources of data, like that collected from the GNSS system.

Attacks on confidentiality and privacy, like eavesdropping and data interception attacks, involve typically passive observers listening to vehicular transmissions, extracting data about nearby vehicles. This data may be used both to monitor traffic for undisclosed reasons, as well as to violate the privacy of drivers themselves, potentially deanonymizing vehicular UEs and opening drivers up to the possibility of having their movements tracked and recorded or their data used commercially. Because such listeners are not active and thus exceedingly difficult to identify or stop, only a robust system for ensuring driver privacy can defend against these attacks. Pseudonym schemes, like those planned for deployment with DSRC in the system envisioned by the USDOT ameliorate some privacy concerns, but still leave open the possibility of compromised user identity [32], [126].

Attacks on integrity are similar to attacks on authenticity, in that they involve vehicles using false identities, to rebroadcast messages with altered contents, potentially disrupting the flow of traffic. These attacks can potentially be prevented with sufficiently encrypted communication, such that the content of a message cannot be changed without invalidating it.

It is possible to identify at least a subset of misbehaving nodes [127], [128], and by so doing prevent them from perpetuating further attacks. But such a solution requires the trustworthy and reliable operation of a centralized VPKI infrastructure, as discussed in Section III-A, above. It is yet unclear what entity or entities will operate such an infrastructure, and how to ensure that this infrastructure is not itself the victim of compromise.

3) Infrastructural and Economic Considerations: One additional, less technical, challenge for the widespread implementation of DSRC is the economic proposition of installing and maintaining a DSRC-compatible infrastructure and vehicular fleet (see [13]). While the marginal cost estimated for consumers to add DSRC compliant systems to their vehicles is non-negligible, predicted as between 245 and 347 USD [8], the costs for the construction and operation of both road-side units and the VPKI is likely to present one of the strongest obstacles to full deployment. Though it remains unclear who will be responsible for the construction and maintenance of road-side units, it must be determined before any model including roadside maintenance can be considered a viable possibility.

B. Cellular V2X

The mobile cellular network has a number of advantages when compared to DSRC. As the backbone of a mature telecommunications industry, the infrastructure for providing cellular coverage is already largely in place. Because scheduling and supporting the transmissions of large numbers of UEs in small areas is one of the central problems facing cellular network providers, such problems are well studied and many solutions are already implemented in the commercial network. Similarly, security is already a high priority for mobile network carriers, and the centralized nature of the mobile network renders the treatment of misbehaving UEs much simpler than in an ad-hoc network.

But likewise does the mobile network face a number of obstacles not shared by DSRC. Without support for broadcast transmission, traditional LTE networks struggle with the volume of unicast signalling in densely congested scenarios. Designed to support conventional voice and data services, the network requires the traversal of a number of core network nodes, rendering the latency constraints of the most stringent V2X safety applications out of reach of conventional LTE [129]. Further, because communication via the mobile network requires authentication via subscription-specific identification credentials, privacy and anonymity are difficult to guarantee. Finally, economic considerations like the pricing structure for mobile data and the need for uninterrupted nationwide coverage present significant practical obstacles.

1) Latency and Capacity: Compared to DSRC, LTE has been shown to scale more stably, though it is still subject to overload in congested situations. Unlike the relatively small range over which VANETs are defined in IEEE 802.11p-based communications, congestion control for ITS communications over LTE must take into account cell-wide vehicular density. Analysis in [130] estimates that, depending on the amount of background traffic originating from unrelated UEs, an LTE cell should be able to handle somewhere between 1700 and 3400 CAM transmissions per second. In the case of sparse traffic or relatively dense cell distribution this may be sufficient to handle V2X traffic, but in heavily congested, larger-scale cells, this may cause an unacceptable violation of latency and reliability constraints. Simulation in [9] reports that, as estimated, LTE retains acceptably low latency for up to 150 vehicular users broadcasting at 10 Hz, without employing any regulation of broadcast frequency. Analyses like those in [40] and [131], however, confirm that as the number of vehicles in a given cell exceed a few hundred, beacon delivery rates for unicast CAMs reach unacceptably low levels.

Broadcast messages, on the other hand, have been shown to be significantly more scalable, though research consensus is uncertain. Calabuig *et al.* [132] show that the use of eMBMS (evolved Multimedia Broadcast Multicast Service) for broadcasting safety messages is significantly more efficient than unicast in congested scenarios. Though 100 vehicles easily overload the network in the unicast condition, eMBMS using QPSK 0.44 encoding is able to handle broadcast delivery with sub-50ms delay, potentially sufficient for even pre-crash sensing applications. The threshold for service degradation also depends largely on the ratio of downlink to uplink transmissions. In the simulations performed in [40], downlink broadcast delivery is shown to be very reliable for up to 800 vehicles per cell when uplink transmissions are allowed a relatively large portion of each LTE frame (3:2 downlink:uplink ratio), but suffer significantly (bottlenecking around 300 vehicles) when subject to 9:1 downlink:uplink bandwidth constraints.

Kato *et al.* [131] show that CAM delivery via eMBMS broadcast can support up to 300 vehicles (the maximum density simulated) with sub-100 ms latency. They note that though earlier simulations [133] report congestion on the uplink with as few as 150 vehicles, they did not observe such a bottleneck. The authors attribute this to two order-of-magnitude reductions of control traffic, first by aggregating CAMs of nearby vehicles into a single downlink update, then further by switching from unicast to broadcast downlink transmission. With these two techniques, they find that downlink control traffic is reduced from 16,000 messages per second to a mere 232 [131].

Another potential remedy to the higher latency of communication over the mobile network is the forthcoming support of direct ProSe D2D communication. Though both broadcast and unicast transmissions require both the presence and traversal of infrastructural nodes, ProSe communications can allow direct vehicle to vehicle transmission even outside of cellular coverage. This will both lower latency bounds for communication between UEs and allow for continuity of service even outside of the range of infrastructural nodes [134], [135].

2) Privacy: One issue shared by both DSRC and cellular V2X regards user expectations of privacy. As user acceptance and high market penetration is instrumental for the benefits of V2X to be realized, it is essential that, in the absence of a regulatory mandate, consumer preferences be strongly considered in the design of a V2X architecture. A 2016 survey by Schmidt *et al.* found that while the safety benefits of V2X are accepted by the general public, the loss of privacy, particularly through the revelation of personal data, is seen as unacceptable [136]. This includes not just the loss of data to potentially malicious eavesdroppers and commercial entities, but also the possession and use of vehicular data by infrastructure providers and governmental authorities. Because the mobile network is designed to incorporate secure authentication and billing by way of subscription-specific identification, it is unclear to what extent such anonymity and privacy can be guaranteed.

3) Infrastructural and Economic Considerations: While the infrastructure for the mobile network is already in operation, offering a wide coverage area, high throughput, and high capacity, there are still economic barriers to supporting uninterrupted V2X coverage via the cellular network. One such obstacle is the necessity of uninterrupted nation-wide network coverage. While forthcoming solutions like ProSe D2D offer alternatives to ensuring cell coverage of all terrestrial road networks, the prospect remains economically daunting for mobile carriers. Without the ability to guarantee the absence of dead spots, where vehicles are unable to communicate, regulatory agencies may resist the adoption of cellular V2X as an alternative to DSRC [8]. Further, while the use of adhoc technology like V2X is more-or-less free, the mobile network charges a significantly higher rate for data usage, which has long been a major obstacle to the consideration of a cellular-network based solution [1]. To this end, the U.S. DOT estimates that, at current rates for data charging, even the implementation of a hybrid solution, using the mobile network only for the management of VPKI certificates, incurs a per vehicle cost almost three times as high as using only DSRC-based communications [8].

Research into both cellular V2X and DSRC-based communications is still very active, including a great wealth of research on all of the challenges covered here. Both technologies offer significant promise for the real world implementation of V2X communications, but each also offers a host of obstacles which must be overcome before implementation is practical. We give a general accounting of strengths, challenges, and potential solutions in Table IV.

V. Conclusion

At present, it seems likely that the first connected cars to make their way onto the worlds public roadways will make use of DSRC technology. The subject of decades of research and already considered by the United States Department of Transportation for a regulatory mandate in the near term, DSRC is a mature technology that will be essential in supporting the earliest users of V2X communication. The suitability of DSRC for highly congested scenarios in the real world remains untested, however, as does the potential for achieving the throughput and connectivity necessary for delivery of non-safety related services. Similarly, the robustness and practicality of the security measures proposed for use with the technology remains in question, from both economic and operational perspectives.

The mobile network, on the other hand, offers a variety of advantages, not the least of which being a pre-existing infrastructure already offering significant coverage of terrestrial roadways. The centralized nature of the cellular network, high throughput, and long history of successful commercial deployment operation offer a strong foundation on which to build future V2X services. Further, forthcoming technologies, like eMBMS broadcast service and ProSe D2D communications offer promising solutions to issues with latency and coverage which pose significant obstacles for implementation over LTE and LTE-A networks. At present, however, latency constraints, economic obstacles, and pressure to accelerate the roll-out of V2X services make early adoption of the mobile network for the purposes of V2X unlikely.

Each wireless access technology offers a unique set of pros and cons for application in the context of V2X. DSRC provides the low latency necessary for the provision of Traffic Safety and Cooperative Driving services, while it struggles with both the throughput necessary for Infotainment and Traffic Efficiency, as well as the capacity necessary to deal with particularly congested traffic situations. The present-day cellular network, in contrast to DSRC, struggles to provide extremely low latency without direct D2D communication, but excels in its proven ability to support high throughput, reliable data transmission, even in highly congested situations, making it an appropriate for both Infotainment and Traffic Efficiency applications.

No single technology has demonstrated the capacity, throughput, latency, and security necessary to support the overwhelming amount of high-priority traffic that will arise as V2X communication becomes prevalent. New ideas and new technologies will be required before such demands can be satisfactorily met. With regards to the present, the authors believe that the most functional and robust implementation lies not in the exclusive choice of one or the other technology, but a heterogeneous solution which draws upon the strengths of each. By turning each technology toward the applications at which it excels, compensating for their respective weaknesses, it seems likely that a robust, reliable, and capable fleet of V2X capable vehicles is within reach. Such a solution could provide the extremely low latency and dynamicity of DSRC while also leveraging the centralized scheduling, high throughput, and robust security of the mobile network.

The onus for moving toward a final V2X solution lies on the shoulders of a number of stakeholders, from automotive manufacturers to governmental authorities and mobile network operators. Whether and to what extent co-operation between stakeholders across so many disparate fields will be realized remains an open question. Only time will tell which technology or technologies are chosen for the long-term support of V2X communications.

REFERENCES

[1] C. Bettisworth *et al.*, "Status of the dedicated short-range communications technology and applications: Report to congress," U.S. Dept. Transp., Washington, DC, USA, Rep. FHWA-JPO-15-218, 2015.

[2] A. Assad, "Fuel-efficient heavy-duty vehicle platooning," Ph.D. dissertation, Dept. Autom. Control, KTH Roy. Inst. Technol., Stockholm, Sweden, 2014.

[3] A. Karapantelakis and J. Markendahl, "The role of mobile network operators in intelligent transport systems: Situation analysis, challenges and suggested approach," in *Proc. Regional Conf. Int. Telecommun. Soc.*, Los Angeles, CA, USA, 2015, pp. 25–28.

[4] C2C-CC, "Car to car communication consortium manifesto: Overview overview of the C2C-CC system," Car Car Commun. Consortium, Rep. Version 1.1, 2007.

[5] E. Paikari, S. Tahmasseby, and B. Far, "A simulation-based benefit analysis of deploying connected vehicles using dedicated short range communication," in *Proc. IEEE Intell. Veh. Symp.*, Dearborn, MI, USA, 2014, pp. 980–985.

[6] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Standard 802.11p-2010, 2010.

[7] *Standards for Wireless Access in Vehicular Environments (WAVE)*, IEEE Standard 1609, 2016.

[8] "49 CFR part 571, notice of proposed rulemaking (NPRM), federal motor vehicle safety standards; V2V communications," document NHTSA-2016-0126, Nat. Highway Traffic Safety Admin., Dept. Transp., Washington, DC, USA, 2016.

[9] Z. H. Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: A performance evaluation," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 89, Dec. 2014.

[10] H. La Vinh and A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, 2014.

[11] O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, "Understanding, modeling and taming mobile malware epidemics in a large-scale vehicular network," in *Proc. World Wireless Mobile Multimedia Netw. (WoWMoM)*, vol. 2013. Madrid, Spain, 2013, pp. 1–9.

[12] Z. H. Mir and F. Filali, "Simulation and performance evaluation of vehicle-to-vehicle (V2V) propagation model in urban environment," in *Proc. 7th Int. Conf. Intell. Syst. Model. Simulat. (ISMS)*, Bangkok, Thailand, 2016, pp. 394–399.

[13] D. Wilkie, "Letter report: Review of the status of the dedicated shortrange communications technology and applications," Nat. Acad. Transp. Res. Board, Washington, DC, USA, Rep., 2015.

[14] "CENELEC and ETSI in the field of information and communication technologies to support the interoperability of cooperative systems for intelligent transport in the European community," European Commision, Brussels, Belgium, Standardisation Mandate M/453. Oct. 2009.

[15] "T109: 700 MHz band intelligent transport systems," ARIB Standard. Association of Radio Industries and Businesses, Tokyo, Japan, 2012.

[16] *Evolved Universal Terrestrial Radio Access (E-UTRA); Long Term Evolution (LTE) Standards*, 3GPP, Sophia Antipolis, France, Dec. 2007.

[17] K. Katsaros, M. Dianati, R. Tafazolli, and X. Guo, "End-to-end delay bound analysis for location-based routing in hybrid vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7462–7475, Sep. 2016.

[18] N. M. Sadek, H. H. Halawa, R. M. Daoud, H. H. Amer, and N. A. Ali, "Heterogeneous LTE/Wi-Fi architecture for ITS traffic control and infotainment," in *Proc. IEEE Int. Conf. Elect. Syst. Aircraft Railway Ship Propulsion Road Veh. (ESARS)*, 2015, pp. 1–6.

[19] Z. H. Mir, J. Kim, Y.-B. Ko, and F. Filali, "Improved multi-hop routing in integrated VANET-LTE hybrid vehicular networks," in *Proc. 10th Int. Conf. Ubiquitous Inf. Manag. Commun.*, Da Nang, Vietnam, 2016, p. 76.

[20] E. Abd-Elrahman, A. M. Said, T. Toukabri, H. Afifi, and M. Marot, "A hybrid model to extend vehicular intercommunication V2V through D2D architecture," in *Proc. Comput. Netw. Commun. (ICNC)*, Garden Grove, CA, USA, 2015, pp. 754–759.

[21] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: A survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013.

[22] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[23] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[24] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[25] K. Tanuja, T. Sushma, M. Bharathi, and K. Arun, "A survey on VANET technologies," *Int. J. Comput. Appl.*, vol. 121, no. 18, 2015, pp. 1–9.

[26] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 2, pp. 88–105, 2nd Quart., 2008.

[27] M. Alsabaan, W. Alasmary, A. Albasir, and K. Naik, "Vehicular networks for a greener environment: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1372–1388, 3rd Quart., 2013.

[28] R. S. Bali, N. Kumar, and J. J. P. C. Rodrigues, "Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions," *Veh. Commun.*, vol. 1, no. 3, pp. 134–152, 2014.

[29] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014.

[30] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

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

[32] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," *Wireless Sensor Networks (WSN) for Vehicular and Space Applications: Architecture and Implementation*. Norwell, MA, USA: Springer, 2015.

[33] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[34] F. D. D. Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. A. Loureiro, "Data communication in VANETs: A survey, challenges and applications," Ph.D. dissertation, INRIA Saclay, INRIA, Rocquencourt, France, 2014.

[35] M. Hadded, P. Muhlethaler, A. Laouiti, R. Zagrouba, and L. A. Saidane, "TDMA-based MAC protocols for vehicular ad hoc networks: A survey, qualitative analysis, and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2461–2492, 4th Quart., 2015.

[36] R. F. Atallah, M. J. Khabbaz, and C. M. Assi, "Vehicular networking: A survey on spectrum access technologies and persisting challenges," *Veh. Commun.*, vol. 2, no. 3, pp. 125–149, 2015.

[37] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," *Veh. Commun.*, vol. 3, pp. 43–57, Jan. 2016.

[38] V. Va, T. Shimizu, G. Bansal, and R. W. Health, Jr., "Millimeter wave vehicular communications: A survey," *Found. Trends® Netw.*, vol. 10, no. 1, pp. 1–118, 2016.

[39] M. Saini, A. Alelaiwi, and A. E. Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Comput. Surveys*, vol. 48, no. 2, p. 29, 2015.

[40] A. Vinel, "3GPP LTE versus IEEE 802.11p/WAVE: Which technology is able to support cooperative vehicular safety applications?" *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 125–128, Apr. 2012.

[41] M. Annoni and B. Williams, "The history of vehicular networks," in *Vehicular Ad Hoc Networks*. Cham, Switzerland: Springer, 2015, pp. 3–21.

[42] H. Flurscheim, "Radio warning system for use on vehicles," U.S. Patent 1 612 427, Dec. 1926.

[43] D. Kopitz and B. Marks, *RDS: The Radio Data System*. Boston, MA, USA: Artech House, 1999.
[44] B. Violino, "The history of RFID technology," *RFID J.*, Jan. 2005, accessed: Nov. 17, 2016. [Online]. Available: http://www.rfidjournal.com/articles/view?1338
[45] K. Takada, Y. Tanaka, A. Igarashi, and D. Fujita, "Road/automobile communication system (RACS) and its economic effect," in *Proc. IEEE Veh. Navigation Inf. Syst. Conf. Conf. Rec.*, Toronto, ON, Canada, 1989, pp. A15–A21.
[46] T. Iwadate *et al.*, "Communication system design of RACS (road/automobile communication system)," in *Proc. Veh. Navigation Inf. Syst. Conf.*, vol. 2, 1991, pp. 247–256.
[47] *ISO/TC 204 Intelligent Transport Systems*. Accessed: Feb. 27, 2017. [Online]. Available: https://www.iso.org/committee/54706.html
[48] *1609 WG—Dedicated Short Range Communication Working Group*. Accessed: Sep. 16, 2016. [Online]. Available: http://standards.ieee.org/develop/wg/1609
[49] *Weekly Brief: Toyota Brings First V2I and V2V Tech to Mass Market*. Accessed: Aug. 26, 2016. [Online]. Available: http://analysis.tu-auto.com/auto-mobility/weekly-brief-toyota-brings-first-v2i-and-v2v-tech-mass-market
[50] *General Motors Promotes DSRC for Connected Vehicle (V2X) Technology Development in China*. Accessed: Mar. 1, 2017. [Online]. Available: http://media.gm.com/media/cn/en/gm/news.detail.html/content/Pages/
[51] *Service Requirements for V2X Services*, 3GPP Standard TS 22.185, 2016.
[52] S. E. El Ayoubi *et al.*, "Deliverable D1.1: Refined scenarios and requirements, consolidated use cases, and qualitative technoeconomic feasibility assessment," Mobile Wireless Commun. Enablers Twenty twenty Inf. Soc., Jan. 2016, accessed: Nov. 17, 2016. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pd
[53] Wi-Fi Alliance, *Spectrum Sharing in the 5 GHz Band DFS Best Practices*, Spectr. Regul. Committee, Austin, TX, USA, 2007.
[54] J. B. Kenney, "Spectrum sharing in the 5.9 GHz DSRC band," in *Proc. 22nd ITS World Congr.*, 2015, pp. 1–12.
[55] R. Latta, "H.R.821—Wi-Fi Innovation Act," United States Federal House Resolution, House Energy and Commerce, Washington, DC, USA, 2015.
[56] "Intelligent transport systems (ITS) vehicular communications; basic set of applications; definitions," ETSI, Sophia Antipolis, France, Rep. ETSI TR 102 638 V1.1.1, 2009.
[57] *Perspectives on Vertical Industries and Implications for 5G*. Next Gener. Mobile Netw., Frankfurt, Germany, 2016.
[58] Crash Avoidance Metrics Partnership and Vehicle Safety Communications Consortium, "Vehicle safety communications project: Task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC," Nat. Highway Traffic Safety Admin., U.S. Dept. Transp., Washington, DC, USA, Rep. DOT HS 809 859, 2005.
[59] J. Choi *et al.*, "Millimeter-wave vehicular communication to support massive automotive sensing," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 160–167, Dec. 2016.
[60] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.
[61] G. P. Fettweis, "The tactile Internet: Applications and challenges," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 64–70, Mar. 2014.
[62] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," in *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
[63] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI Standard 302 637-2 v1.3.1, Sep. 2014.
[64] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, ETSI Standard 302 637-2 V1.3.1, Nov. 2014.
[65] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE Standard J2735, 2016.
[66] *Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems Operating in the 5 GHz Range; Access Layer Part*, ETSI Standard TS 102 687, 2011.
[67] *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, ETSI Standard TS 103 097 V1.2.1, 2013.
[68] J. B. Kenney, G. Bansal, and C. E. Rohrs, "LIMERIC: A linear message rate control algorithm for vehicular DSRC systems," in *Proc. 8th ACM Int. Workshop Veh. Inter Netw.*, 2011, pp. 21–30.
[69] B. Cheng *et al.*, "Performance evaluation of a mixed vehicular network with CAM-DCC and LIMERIC vehicles," in *Proc. IEEE 16th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, 2015, pp. 1–6.
[70] 5G Automotive Association, "The case for cellular V2X for safety and cooperative driving," Accessed Feb. 14, 2017. Nov. 2016. [Online]. Available: http://www.5gaa.org/pdfs/5GAAwhitepaper23Nov2016.pdf
[71] L. Armstrong and W. Fisher, "Status of Project IEEE 802.11 Task Group p, Wireless Access in Vehicular Environments (WAVE)" IEEE P802.11 Task Group p. Accessed: Aug. 26, 2016. [Online]. Available: http://www.ieee802.org/11/Reports/tgp_update.htm
[72] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM Standard 2213-03, 2010.
[73] W. Fisher, *Development of DSRC/WAVE Standards*. Annapolis, MD, USA: IEEE Press, 2007.
[74] "The European table of frequency allocations and applications in the frequency range 8.3 kHz to 3000 GHz (ECA table)," Eur. Res. Council, Brussels, Belgium, Rep. 25, 2016.
[75] "Amendment of parts 2 and 90 of the commissions rules to allocate the 5.850–5.925 GHz band to the mobile service for dedicated short range communications of intelligent transportation services," ET Docket 98-95, FCC, Washington, DC, USA, pp. 95–98, 1999.
[76] "Dedicated short-range communication system, version 1.0," document STD-T75, Assoc. Radio Ind. Bus., Tokyo, Japan, 2001.
[77] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Proc. Veh. Technol. Conf.*, Singapore, 2008, pp. 2036–2040.
[78] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC multi-channel operations and its implications on vehicle safety communications," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Tokyo, Japan, 2009, pp. 1–8.
[79] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): Challenges and perspectives," in *Proc. 6th IEEE Int. Conf. ITS Telecommun.*, Chengdu, China, 2006, pp. 761–766.
[80] M. F. L. Abdullah, J. Abdullah, A. Z. Yonis, and M. F. Ghanim, "Comparison study on 3.9G and 4G evolution," in *Proc. Int. Conf. Inf. Commun. Manag. (IPCSIT)*, 2011, pp. 181–186.
[81] *LTE*. Accessed: Dec. 11, 2017. [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte
[82] *Nationwide 4G/LTE Rollout for Teliasonera in Norway and Sweden*. Accessed: Feb. 27, 2017. [Online]. Available: https://www.ericsson.com/news/1372929
[83] *Requirements Related to Technical Performance for IMT Advanced Radio Interface(s)*, Int. Telecommun. Union, Geneva, Switzerland, ITU-Recommendation 2134, 2008.
[84] *LTE-Based V2X Services*, document RP 161874, 3GPP, Sophia Antipolis, France, 2016.
[85] *3GPP Release-15: Further LTE Enhancements and 5G Normative Work Kick-Off*. Accessed: Dec. 11, 2017. [Online]. Available: https://www.grandmetric.com/2017/04/26/3gpp-release-15-further-lte-enhancements-and-5g-normative-work-kick-off/
[86] "Study of LTE device to device proximity services," 3rd Gener. Partnership Project, Sophia Antipolis, France, Rep. 3GPP TR 36.843, Jun. 2014.
[87] NGMN Alliance, *5G White Paper*, Next Gener. Mobile Netw., Frankfurt, Germany, White Paper, 2015.
[88] J. Hasch *et al.*, "Millimeter-wave technology for automotive radar sensors in the 77 GHz frequency band," *IEEE Trans. Microw. Theory Techn.*, vol. 60, no. 3, pp. 845–860, Mar. 2012.
[89] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: Opportunities and challenges," *Wireless Netw.*, vol. 21, no. 8, pp. 2657–2676, 2015.
[90] C. F. Mecklenbrauker *et al.*, "Vehicular channel characterization and its implications for wireless system design and performance," *Proc. IEEE*, vol. 99, no. 7, pp. 1189–1212, Jul. 2011.
[91] M. R. Sama, X. An, Q. Wei, and S. Beker, "Reshaping the mobile core network via function decomposition and network slicing for the 5G era," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Doha, Qatar, 2016, pp. 90–96.

[92] S. Singh, Y.-C. Chiu, Y.-H. Tsai, and J.-S. Yang, "Mobile edge fog computing in 5G era: Architecture and implementation," in *Proc. Int. Comput. Symp. (ICS)*, Chiayi, Taiwan, 2016, pp. 731–735.

[93] ICSLMS Committee, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-1997, 1997.

[94] A. Sugiura and C. Dermawan, "In traffic jam IVC-RVC system for ITS using Bluetooth," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 3, pp. 302–313, Sep. 2005.

[95] H. Sawant, J. Tan, Q. Yang, and Q. Wang, "Using Bluetooth and sensor networks for intelligent transportation systems," in *Proc. 7th Int. IEEE Conf. Intell. Transp. Syst.*, Washington, WA, USA, 2004, pp. 767–772.

[96] B. Kloiber, T. Strang, H. Spijker, and G. Heijenk, "Improving information dissemination in sparse vehicular networks by adding satellite communication," in *Proc. IEEE Intell. Veh. Symp. (IV)*, 2012, pp. 611–617.

[97] J. Hu and T.-C. Song, "A vehicle-mounted communication system integrating satellite and terrestrial networks," in *Proc. 7th Int. Conf. Comput. Converg. Technol. (ICCCT)*, Seoul, South Korea, 2012, pp. 767–771.

[98] S. Sasaki and T. Okazaki, "Feasibility study for telexistence on a ship—Measurement of delay time of satellite communication," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Budapest, Hungary, 2016, pp. 001477–001482.

[99] W. Shen, L. Chen, and X. Yang, "A design of phased arrays carried on vehicles for ku band satellite communication," in *Proc. Int. Symp. IEEE Antennas Propag. Soc.*, Albuquerque, NM, USA, 2006, pp. 545–548.

[100] M. Vicente-Lozano, G. Franceschetti, F. J. Ares-Pena, and E. Moreno-Piquero, "Analysis and synthesis of a printed array for satellite communication with moving vehicles," *IEEE Trans. Antennas Propag.*, vol. 50, no. 11, pp. 1555–1559, Nov. 2002.

[101] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digit. Commun. Netw.*, vol. 3, no. 2, pp. 78–88, 2017.

[102] A. Sarkar, S. Agarwal, and A. Nath, "Li-Fi technology: Data transmission through visible light," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 3, no. 6, pp. 1–12, 2015.

[103] S. Hranilovic and F. R. Kschischang, "Short-range wireless optical communication using pixilated transmitters and imaging receivers," in *Proc. IEEE Int. Conf. Commun.*, vol. 2. Paris, France, 2004, pp. 891–895.

[104] X. Wu *et al.*, "Vehicular communications using DSRC: Challenges, enhancements, and evolution," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 399–408, Sep. 2013.

[105] X. Huang, D. Zhao, and H. Peng, "Empirical Study of DSRC Performance Based on Safety Pilot Model Deployment Data," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2619–2628, Oct. 2017.

[106] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proc. IEEE 66th Veh. Technol. Conf.*, Baltimore, MD, USA, 2007, pp. 2199–2203.

[107] W. Sun, H. Zhang, C. Pan, and J. Yang, "Analytical study of the IEEE 802.11p EDCA mechanism," in *Proc. Intell. Veh. Symp. (IV)*, Gold Coast, QLD, Australia, 2013, pp. 1428–1433.

[108] K. A. Hafeez, L. Zhao, B. Ma, and J. W. Mark, "Performance analysis and enhancement of the DSRC for VANET's safety applications," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3069–3083, Sep. 2013.

[109] A. Rostami *et al.*, "Stability challenges and enhancements for vehicular channel congestion control approaches," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 10, pp. 2935–2948, Oct. 2016.

[110] Z. Wang and M. Hassan, "How much of DSRC is available for non-safety use?" in *Proc. 5th ACM Int. Workshop Veh. Inter Netw.*, San Francisco, CA, USA, 2008, pp. 23–29.

[111] K. A. Hafeez, A. Anpalagan, and L. Zhao, "Optimizing the control channel interval of the DSRC for vehicular safety applications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3377–3388, May 2016.

[112] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wireless Netw.*, vol. 8, nos. 2–3, pp. 153–167, 2002.

[113] I. K. Virdaus, M. Kang, S. Shin, and G.-R. Kwon, "A simulation study: Is the broadcast storming really harmful for emergency delivery in VANETs?" in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, 2015, pp. 666–670.

[114] A. Bohm, M. Jonsson, and E. Uhlemann, "Co-existing periodic beaconing and hazard warnings in IEEE 802.11 p-based platooning applications," in *Proc. 10th ACM Int. Workshop Veh. Inter-Netw. Syst. Appl.*, Taipei, Taiwan, 2013, pp. 99–102.

[115] G. Xiao, H. Zhang, Z. Huang, and Y. Chen, "Decentralized cooperative piggybacking for reliable broadcast in the VANET," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, Nanjing, China, 2016, pp. 1–5.

[116] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[117] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer Peer Syst.*, Cambridge, MA, USA, 2002, pp. 251–260.

[118] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[119] O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, "Worm epidemics in vehicular networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2173–2187, Oct. 2015.

[120] S. A. Khayam and H. Radha, "Analyzing the spread of active worms over VANET," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw. ACM*, Philadelphia, PA, USA, 2004, pp. 86–87.

[121] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, "Congestion attacks to autonomous cars using vehicular botnets," in *Proc. NDSS Workshop Security Emerg. Netw. Technol. (SENT)*, San Diego, CA, USA, 2015, pp. 1–9.

[122] C. Miller and C. Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle*, Black Hat, San Francisco, CA, USA, 2015.

[123] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[124] V. Bibhu, R. Kumar, B. S. Kumar, and D. K. Singh, "Performance analysis of black hole attack in VANET," *Int. J. Comput. Netw. Inf. Security*, vol. 4, p. 11, Oct. 2012.

[125] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in VANET," in *Proc. Glob. Telecommun. Conf. (GLOBECOM)*, Honolulu, HI, USA, 2009, pp. 1–5.

[126] J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, *Connected Vehicles: Surveillance Threat and Mitigation*, Black Hat, San Francisco, CA, USA, 2015.

[127] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter Netw. Syst. Appl.*, 2012, pp. 73–82.

[128] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[129] P. Luoto *et al.*, "System level performance evaluation of LTE-V2X network," in *Proc. 22nd Eur. Wireless Conf.*, 2016, pp. 1–5.

[130] T. Mangel, T. Kosch, and H. Hartenstein, "A comparison of UMTS and LTE for vehicular safety communication at intersections," in *Proc. Veh. Netw. Conf. (VNC)*, Jersey City, NJ, USA, 2010, pp. 293–300.

[131] S. Kato, M. Hiltunen, K. Joshi, and R. Schlichting, "Enabling vehicular safety applications over LTE networks," in *Proc. Int. Conf. Connected Veh. Expo (ICCVE)*, Las Vegas, NV, USA, 2013, pp. 747–752.

[132] J. Calabuig, J. F. Monserrat, D. Gozalvez, and O. Klemp, "Safety on the roads: LTE alternatives for sending ITS messages," *IEEE Veh. Technol. Mag.*, vol. 9, no. 4, pp. 61–70, Dec. 2014.

[133] M. A. Phan, R. Rembarz, and S. Sories, "A capacity analysis for the transmission of event and cooperative awareness messages in LTE networks," in *Proc. 18th ITS World Congr.*, 2011, pp. 1–5.

[134] H. Seo, K.-D. Lee, S. Yasukawa, Y. Peng, and P. Sartori, "LTE evolution for vehicle-to-everything services," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 22–28, Jun. 2016.

[135] H. Cao, S. Gangakhedkar, A. R. Ali, M. Gharba, and J. Eichinger, "A 5G V2X testbed for cooperative automated driving," in *Proc. Veh. Netw. Conf. (VNC)*, Columbus, OH, USA, 2016, pp. 1–4.

[136] T. Schmidt, R. Philipsen, P. Themann, and M. Ziefle, "Public perception of V2X-technology—Evaluation of general advantages, disadvantages and reasons for data sharing with connected vehicles," in *Proc. Intell. Veh. Symp. (IV)*, Gothenburg, Sweden, 2016, pp. 1344–1349.

Zachary MacHardy received the B.S. degree in computer science from the University of North Carolina Chapel Hill, Chapel Hill, NC, USA, and the M.S. degree in computer science from the University of California at Berkeley. He joined NTT DOCOMO in 2015, as a Research Engineer. He was with DOCOMO, where he was involved in the design of 5G core network architecture, with a particular focus on V2X and edge computing applications. He currently works as a Software Engineer for IXL Learning Inc., San Mateo, CA, USA.

Ashiq Khan received the Ph.D. degree in computer science from the University of Tsukuba. He is an Assistant Manager with NTT DOCOMO, where his present work focuses on the research and development of the 5G mobile network for 2020. He has ten years of work experience in network virtualization, and was involved in ETSI NFV standardization, NFV-based mobile network development, and the consequent commercial roll-out of the world's first multivendor virtualized evolved packet core mobile system by DOCOMO in 2016. He served in the OPNFV TSC as a Founding Member, and initiated the Doctor and Promise projects, leading to their successful implementation in OpenStack. He is currently the Chairman of the ETSI ZSM Network Operator Council and an OPNFV Ambassador.

Kazuaki Obana (M'98) received the B.E. and M.E. degrees in electrical engineering from Waseda University, Tokyo. He is a Senior Research Engineer and a Supervisor with Ubiquitous Service Systems Laboratory, NTT Network Innovation Laboratories. After joining NTT, he was engaged in research and development for 21 years on priority queuing by time and place information, proxy design with shaping functions, fast transmission system with multilane aggregation, home ICT system on customer premises equipment, programmable nodes, SDN, and NFV. From 2014 to 2017, he worked on NFV standardization with NTT DOCOMO. Since 2017, he has been with NTT Network Innovation Laboratories. His current interests and responsibilities are in IoT and related areas. He is a member of IEICE. He was a recipient of the Achievement Award 2017 from IEICE.

Shigeru Iwashina received the B.E. and M.E. degrees from the Tokyo Institute of Technology in 1993 and 1995, respectively. He is an Executive Research Engineer with the Smart ICT Platform Research Group, NTT DOCOMO. In 1995, he joined DOCOMO, where he has been engaged in various research and development activities, including the PDC cellular systems, the core network of IMT2000, and the core network of the LTE system. His current research interests are NFV-based mobile core network virtualization and 5G network architecture.