Dedicated Short-Range Communications (DSRC) Standards in the United States

Article *in* Proceedings of the IEEE · August 2011

DOI: 10.1109/JPROC.2011.2132790 · Source: IEEE Xplore

1 author:

John B. Kenney
Toyota InfoTechnology Center
44 PUBLICATIONS **1,421** CITATIONS

INVITED PAPER

Dedicated Short-Range Communications (DSRC) Standards in the United States

IEEE and SAE Standards for Wireless Access in Vehicular Environments (WAVE), most of which have been published in the past 12 months, are described in detail in this paper.

By John B. Kenney, *Member IEEE*

ABSTRACT | Wireless vehicular communication has the potential to enable a host of new applications, the most important of which are a class of safety applications that can prevent collisions and save thousands of lives. The automotive industry is working to develop the dedicated short-range communication (DSRC) technology, for use in vehicle-to-vehicle and vehicle-to-roadside communication. The effectiveness of this technology is highly dependent on cooperative standards for interoperability. This paper explains the content and status of the DSRC standards being developed for deployment in the United States. Included in the discussion are the IEEE 802.11p amendment for wireless access in vehicular environments (WAVE), the IEEE 1609.2, 1609.3, and 1609.4 standards for Security, Network Services and Multi-Channel Operation, the SAE J2735 Message Set Dictionary, and the emerging SAE J2945.1 Communication Minimum Performance Requirements standard. The paper shows how these standards fit together to provide a comprehensive solution for DSRC. Most of the key standards are either recently published or expected to be completed in the coming year. A reader will gain a thorough understanding of DSRC technology for vehicular communication, including insights into why specific technical solutions are being adopted, and key challenges remaining for successful DSRC deployment. The U.S. Department of Transportation is planning to decide in 2013 whether to require DSRC equipment in new vehicles.

KEYWORDS | Dedicated short-range communication (DSRC); networks; safety; standards; vehicles; WAVE; 5.9 GHz

I. INTRODUCTION

Vehicles utilize a variety of wireless technologies to communicate with other devices. This paper focuses on one specific technology, dedicated short-range communication (DSRC) [1], which is designed to support a variety of applications based on vehicular communication. DSRC is under active development in the United States and in other countries. The goal of the paper is to explain the content and status of the major standards that support interoperable DSRC in the United States [2]–[7].

The primary motivation for deploying DSRC is to enable collision prevention applications. These applications depend on frequent data exchanges among vehicles, and between vehicles and roadside infrastructure. The U.S. Department of Transportation (DOT) has estimated that vehicle-to-vehicle (V2V) communication based on DSRC can address up to 82% of all crashes in the United States involving unimpaired drivers, potentially saving thousands of lives and billions of dollars. The National Highway Traffic Safety Administration (NHTSA) within the U.S. DOT plans to decide in 2013 whether to use regulations to require or encourage deployment of DSRC equipment in new vehicles in the U.S. [8].

The basic paradigm of DSRC-based collision avoidance is illustrated in Fig. 1. Each DSRC-equipped vehicle broadcasts its basic state information, including location, speed, and acceleration, several times per second over a range of a few hundred meters. Each vehicle also receives these "safety messages" from DSRC-equipped neighbors. A receiving vehicle uses these messages to compute the

Manuscript received December 2, 2010; revised February 22, 2011; accepted February 26, 2011. Date of current version June 17, 2011.
The author is with Toyota InfoTechnology Center, Mountain View, CA 94043 USA (e-mail: jkenney@us.toyota-itc.com).
Digital Object Identifier: 10.1109/JPROC.2011.2132790

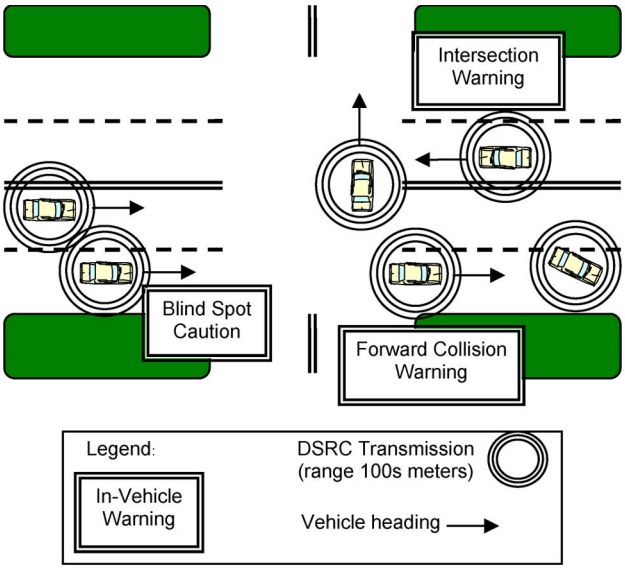

Fig. 1. ***Vehicles sending safety messages, displaying in-vehicle warnings.***

trajectory of each neighbor, compares these with its own predicted path, and determines if any of the neighbors poses a collision threat. In addition to V2V communication, vehicles may also communicate to and from DSRC roadside units (RSUs) using safety messages and other types of message. Examples of information a vehicle may learn from an RSU include: the geometry of an approaching intersection, the state of the signals at an intersection, and the existence of a hazard (e.g., disabled vehicle, emergency vehicle, ice, fog).

If a vehicle determines that a potential collision or other hazard (e.g., violating a red light) exists, the onboard system can take action to warn the driver, or even to assist in controlling the vehicle. Feedback to a driver can be conveyed audibly, visually (e.g., heads-up-display, dashboard screen, mirror signal), and haptically (e.g., shaking seat or steering wheel), and can range in intensity from inform to caution to warning. While the communication between DSRC devices must follow carefully designed interoperability standards, the internal threat computation and warning system employed by a vehicle is determined by the automobile manufacturer.

The U.S. Department of Transportation and several automakers in the United States have teamed up to study DSRC-based collision avoidance. The Vehicle Safety Communications—Applications project, completed in 2009, demonstrated the feasibility of several V2V safety applications [9], including:

- forward collision warning (stopped vehicle ahead);
- emergency electronic brake lights (hard-braking vehicle ahead);
- blind spot warning;
- intersection movement assist;
- do not pass warning;
- control loss warning;

A few of these are illustrated in Fig. 1.

DSRC can be used for many other applications beyond collision avoidance. Most of these involve communication to and from RSUs. For example, DSRC can be used to assist navigation, make electronic payments (e.g., tolls, parking, fuel), improve fuel efficiency, gather traffic probes, and disseminate traffic updates. It can also be used for more general entertainment and commercial purposes.

The word "Dedicated" in DSRC refers to the fact that the U.S. Federal Communications Commission has allocated 75 MHz of licensed spectrum in the 5.9 GHz band for DSRC communication [10], [11]. This spectrum is divided into several channels. V2V safety messages are expected to be exchanged on Channel 172, a specific channel designated for safety [12]. The term "Short Range" in DSRC is meant to convey that the communication takes place over hundreds of meters, a shorter distance than cellular and WiMax services typically support.

II. OVERVIEW OF DSRC STANDARDS

DSRC communication relies fundamentally on standards-based interoperability among devices from different manufacturers. This paper provides a description of the core DSRC standards under development for use in the United States. Most of these standards are either recently published or in the final stages of specification. The U.S. DOT and a consortium of automotive manufacturers (Vehicle Safety Communications 3—VSC3) have begun a project to test the interoperability and scalability of DSRC technology [13]. The first phase of this V2V-Interoperability project focuses on whether the emerging standards are clear and comprehensive enough so that independent implementations will be able to communicate. Testing to date has shown that DSRC equipment from four suppliers can communicate effectively, with no significant gaps in the standards identified [14].

This overview provides a brief description of the DSRC protocol stack. The sections that follow examine the major standards for each of the layers in turn: Physical (PHY), Data Link (including medium access control—MAC), Network/Transport, and Application. A few of the abbreviations used frequently in this paper are defined in Table 1.

Fig. 2 illustrates the protocol stack for DSRC communication, including shorthand names of protocols and standards intended for use at the various layers. At the PHY and MAC layers DSRC utilizes IEEE 802.11p Wireless Access for Vehicular Environments (WAVE), a modified version of the familiar IEEE 802.11 (WiFi) standard. In the middle of the stack DSRC employs a suite of standards defined by the IEEE 1609 Working Group: 1609.4 for Channel Switching, 1609.3 for Network Services (including the WAVE Short Message Protocol—WSMP), and

Table 1 Frequently Used Abbreviations

Abbreviation	Definition
AP	Access Point
BSS	Basic Service Set
CCH	Control Channel
DSRC	Dedicated Short Range Communication
GPS	Global Positioning System
MAC	Medium Access Control
OCB	Outside the Context of a BSS
PLCP	Physical Layer Convergence Procedure
QoS	Quality of Service
RSU	Roadside Unit
STA	Station
V2V	Vehicle to Vehicle
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement
WSM	WAVE Short Message
WSMP	WSM Protocol

1609.2 for Security Services. DSRC also supports use of well-known Internet protocols for the Network and Transport layers, i.e., Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). These protocols, defined by the Internet Engineering Task Force (IETF), are stable and well documented in other places, so they are not further discussed in this paper. The choice between using WSMP or IPv6+UDP/TCP depends on the requirements of a given application. Single-hop messages, like those upon which collision prevention applications are based, typically use the bandwidth-efficient WSMP, while multi-hop packets use IPv6 for its routing capability.

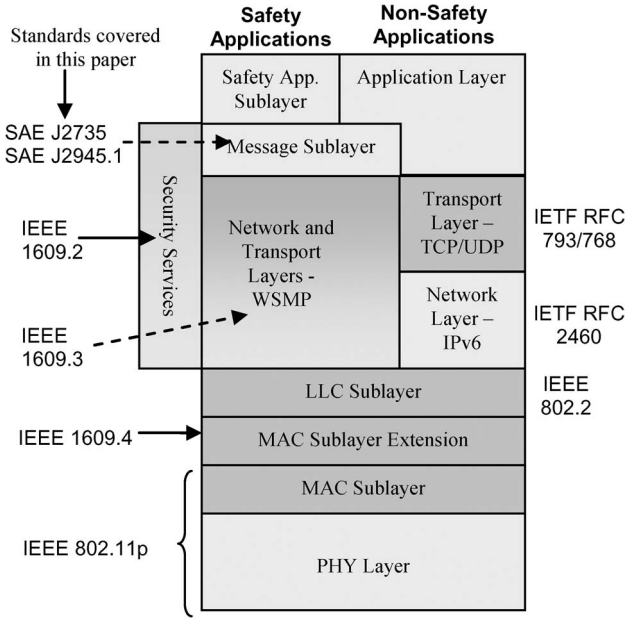

Fig. 2. ***Layered architecture for DSRC communication in the US.***

At the top of the stack, the SAE J2735 Message Set Dictionary standard specifies a set of message formats that support a variety of vehicle-based applications. The most important of these is the basic safety message (BSM), which conveys critical vehicle state information in support of V2V safety applications. Vehicles exchanging frequent BSMs can track each other's position and movement, and take action to prevent potential collisions. SAE J2735 defines message syntax, but leaves other norms for V2V safety to be specified in the emerging SAE J2945.1 communication minimum performance requirements standard. Among the topics to be addressed in SAE J2945.1 are BSM transmission rate and power, accuracy of BSM data elements, and channel congestion control.

Some of the material in this paper draws on the standards discussion in [15, ch. 10], with significant new content reflecting the evolving standards. A reader seeking additional details is encouraged to consult that reference.

Geographic Scope: The IEEE and SAE standards described in this paper have international scope, but have been developed in close coordination with U.S. automotive and governmental strategic plans. Efforts to develop standards for collision avoidance based on vehicular communication are also underway in regional standards organizations in other parts of the world, most notably the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), and the Japanese Association of Radio Industries and Businesses (ARIB). Harmonization efforts among government and standards organizations have also begun, particularly between the U.S. and Europe. It remains to be seen how the standards described here will be used outside of the United States. It appears that the protocols at the bottom of the stack, especially IEEE 802.11p, are most likely to be used elsewhere, with a decreasing probability for protocols higher in the stack. Note also that in some regions the term DSRC is either not used or carries a narrower, nonsafety connotation.

III. DSRC PHYSICAL LAYER STANDARD

The next several sections examine the various layers of the DSRC protocol stack (Fig. 2) in detail, working from bottom to top, and starting with the Physical layer. The DSRC PHY protocol is defined in IEEE 802.11 [16] (specifically clause 17), as amended by IEEE 802.11p [2]. It is divided into two sublayers: the *physical medium dependent (PMD)* sublayer and the *physical layer convergence procedure (PLCP)* sublayer. As the name suggests, the PMD interfaces directly with the wireless medium. It utilizes the familiar orthogonal frequency division multiplexing (OFDM) technique, originally added to 802.11 in the 802.11a amendment. The PLCP defines the mapping between the MAC frame and the basic PHY layer data unit, the OFDM symbol.

In 2003 an earlier version of the DSRC PHY was published under the auspices of ASTM International in the

ASTM E2213-03 [17] standard, which was also based on IEEE 802.11. In 2004 interested parties obtained approval to create the IEEE 802.11p WAVE amendment for DSRC within the IEEE 802.11 Working Group (WG). The amendment was published in 2010. The deviations from the main 802.11 standard were minimized to encourage 802.11 silicon vendors to add support for 802.11p, which would help keep costs down by leveraging the large volume of 802.11 chips produced annually. There are orders of magnitude more WiFi equipped cell phones sold every year than new vehicles. The automotive industry considers the PHY and MAC portions of ASTM E2213-03 to be deprecated in favor of IEEE 802.11 and 802.11p. The United States Federal Communication Commission (FCC) regulations for DSRC [18], [19], however, still incorporate by reference rules contained in ASTM E2213-03. It is anticipated that the FCC regulations will eventually be updated to instead require conformance to IEEE 802.11 and 802.11p.

The IEEE 802.11 WG periodically integrates its amendments into a new baseline standard. As this paper is written, the WG is undertaking this integration for all amendments completed since the prior integration effort in 2007. The integrated standard will be referred to as 802.11-2012 if it is published as planned in 2012. At that point the 802.11p amendment will no longer exist as a separate document, but the features it added to the baseline standard will informally still be referred to as 802.11p (as we still refer to 802.11a, b, and g, for example). It is also possible that in the integration process minor modifications will be made to the WAVE capabilities described in this paper.

The concept and theoretical basis of OFDM are well documented in other sources [15], so the present discussion focuses on the specific OFDM protocol defined in 802.11, including the modifications in the WAVE 802.11p amendment.

A. OFDM Physical Medium Dependent (PMD) Function

The OFDM protocol used in 802.11 is defined for three channel widths: 20, 10, and 5 MHz. While most 802.11a implementations use the 20 MHz channel, DSRC will more commonly use the 10 MHz channel. The basic parameters of the 802.11 10 MHz OFDM channel are shown in Table 2.

Table 2 IEEE 802.11 10 MHz OFDM Channel Basic Parameters

Parameter	Value
Number of data subcarriers	48
Number of pilot subcarriers	4
Total number of subcarriers	52
Subcarrier frequency spacing	156.25 KHz
Guard interval (GI)	1.6 μsec
Symbol interval (including GI)	8 μsec

Table 3 Data Rate Options in a DSRC 10 MHz OFDM Channel

Modulation Technique	Coded Bit Rate (Mbps)	Coding Rate	Data Rate (Mbps)	Data Bits per OFDM Symbol
BPSK	6	1/2	3	24
BPSK	6	3/4	4.5	36
QPSK	12	1/2	6	48
QPSK	12	3/4	9	72
16-QAM	24	1/2	12	96
16-QAM	24	3/4	18	144
64-QAM	36	2/3	24	192
64-QAM	36	3/4	27	216

Four modulation techniques are available for use on a subcarrier, each of which corresponds to a different number of bits encoded per subcarrier symbol. *Forward error correction (FEC)* coding is applied to the user bits, which reduces the effective user bit rate but also improves the probability of successful decoding. Eight combinations of modulation rate and FEC coding rate are specified in IEEE 802.11, as shown in Table 3. For example, binary phase shift keying (BPSK) uses one bit per subcarrier symbol and thus 48 bits per OFDM symbol. With 1/2 rate coding, there are 24 data bits and 24 coding bits per OFDM symbol. With 24 data bits per OFDM symbol and an 8 μs symbol period, the resulting data rate is 3 Mb/s.

PMD Transmitter: When the PLCP requests the PMD to transmit a frame, it supplies the coded bits that make up each OFDM symbol (the contents of which include MAC data and PLCP overhead described below). It also provides the data rate and the transmit power. The PMD sublayer performs the OFDM modulation, including Inverse Fast Fourier Transform calculation, Guard Interval (cyclic prefix) insertion, wave shape filtering, RF modulation, and power amplification. An 802.11 device (a.k.a. "station" or STA) implementing the OFDM 10 MHz PHY must support transmission and reception of the 3, 6, and 12 Mb/s data rates. The other rates are optional in 802.11. Most DSRC testing in the U.S. has utilized the 6 Mb/s configuration (Quadrature PSK with rate 1/2 coding), since it seems to provide a good compromise between channel load and signal-to-noise requirement [20], but it remains an open question whether other rates will also be supported. For example, perhaps a higher rate will be useful to reduce channel load in high vehicle density environments. The rules concerning which bit rates to use for DSRC V2V safety will likely be standardized in SAE J2945.1.

The FCC defines four classes of device, labeled A–D. As shown in Table 4, each class is associated with a maximum allowed transmit power at the antenna and a desired range (CFR 47 §90.375 [18]).

Devices participating in V2V safety will normally be in Class C. Each device class is also associated with a transmit

Table 4 FCC Device Classification

Device Class	Max. Output Power (dBm)	Communication Zone (meters)
A	0	15
B	10	100
C	20	400
D	28.8	1000

spectral mask, defined in IEEE 802.11p, which limits the out-of-band energy of a transmitter. A given mask specifies a frequency dependent upper bound on the permitted power spectral density (PSD) of the transmitted signal (with 100 KHz resolution bandwidth). The PSD limits are specified at certain frequency offsets from the signal center frequency, and are relative to the peak PSD of the signal (i.e., in dBr). The mask is defined as the piecewise linear function passing through the specified points. Table 5 shows the spectral mask PSD limits at the break-points between the linear segments for each of the four FCC device classes. Progressing from Class A to Class D, each class allows a higher maximum transmit power and enforces a tighter spectral mask.

Mask C, is shown graphically in Fig. 3 for a 10 MHz channel.

PMD Receiver: The PMD receiver performs the demodulation steps, including automatic gain control (AGC), clock recovery, RF demodulation, guard interval removal, and Fast Fourier Transform. When the PMD sublayer passes a received frame up to the PLCP sublayer, it also makes available the received signal strength indication (RSSI).

Receiver performance is specified in IEEE 802.11 in terms of minimum sensitivity and channel rejection. Minimum sensitivity is defined as the minimum absolute signal energy for which a reference 1000 byte packet must be correctly received at least 90% of the time. IEEE 802.11 specifies minimum sensitivity levels as a function of the modulation technique and FEC coding rate, and thus of the data rate of the packet. For the 10 MHz OFDM signal these levels vary from −85 dBm at 3 Mb/s to −68 dBm at 27 Mb/s (802.11p does not modify the sensitivity requirements).

Table 5 Power Spectral Density Limits for 10 MHz DSRC Channels in the United States (Standardized in IEEE 802.11p [2])

Freq. Offset	±4.5 MHz	±5.0 MHz	±5.5 MHz	±10.0 MHz	±15.0 MHz
Class A	0 dBr	-10 dBr	-20 dBr	-28 dBr	-40 dBr
Class B	0 dBr	-16 dBr	-20 dBr	-28 dBr	-40 dBr
Class C	0 dBr	-26 dBr	-32 dBr	-40 dBr	-50 dBr
Class D	0 dBr	-35 dBr	-45 dBr	-55 dBr	-65 dBr

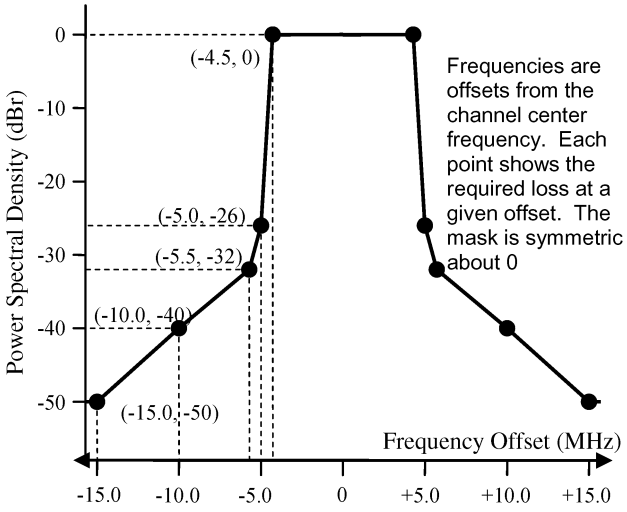

Fig. 3. ***Transmit Spectral Mask C. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)***

Channel rejection is an indication of a receiver's ability to filter out energy that is outside the 10 MHz channel of interest. There are different specifications depending on whether the interfering transmitter is in an adjacent channel or not. The IEEE 802.11 standard defines *adjacent channel rejection (ACR)* and *nonadjacent channel rejection (NACR)* requirements for each bit rate and channel bandwidth. The WAVE 802.11p amendment supplements the required ACR and NACR levels with more stringent optional enhanced channel rejection levels. These were introduced to compensate for the more challenging communication environment associated with rapidly moving vehicles, but they remain optional out of deference to the goal of encouraging WiFi silicon vendors to support the amendment.

DSRC Spectrum: The FCC has allocated the spectrum from 5.850 GHz to 5.925 GHz, i.e. the "5.9 GHz band," for DSRC operation in the United States [10], [11]. This spectrum is divided into seven 10 MHz channels with a 5-MHz guard band at the low end, as illustrated in Fig. 4. Pairs of 10 MHz channels can also be combined into a 20 MHz channel. Testing of DSRC in the U.S. has focused on 10 MHz channels, based on the desire to support many parallel types of applications, and on physical testing that suggests this width is well suited to the delay and Doppler spreads likely to be encountered in the vehicular environment [21]. However, it remains an open question whether concerns for channel congestion, particularly in the channel used for V2V safety communication (probably Channel 172), might be better addressed with the increased capacity of a 20 MHz channel. A frame with a given modulation and coding (Table 3) takes approximately half as long to transmit on a 20 MHz channel as on a 10 MHz channel, thus reducing the collision probability for a given number of

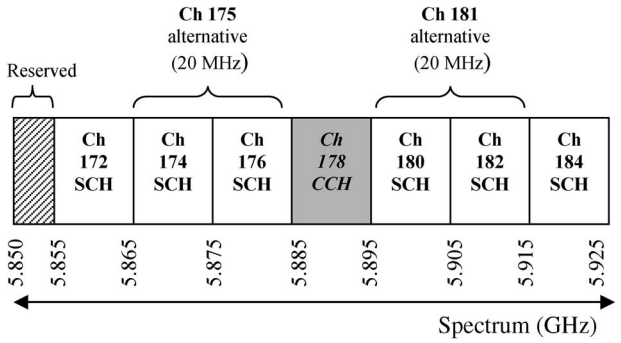

Fig. 4. *United States DSRC Band Plan channel designations. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)*

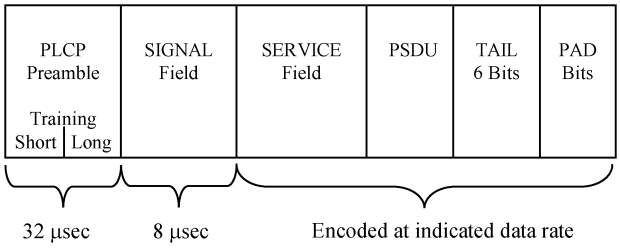

Fig. 5. *Physical Protocol Data Unit format. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)*

frame transmissions per second. On the other hand, a 20 MHz channel has more noise for a given background spectral density and may pose a greater challenge for some environments, e.g., inter-symbol interference due to a delay spread that exceeds the shortened cyclic prefix length.

The FCC has also designated each channel as either a Service Channel (SCH) or as the Control Channel (CCH). These designations, as well as more specific rules for use of individual channels by application type, are discussed below in Section V-A, which addresses the IEEE 1609.4 standard.

Cross-Channel Interference (CCI): The multichannel nature of the United States band plan heightens the concern about cross-channel interference (CCI), which the transmit mask and channel rejection requirements are meant to control. CCI testing has demonstrated the potential problems caused by simultaneous operation, particularly on adjacent channels, in a given region [22]. Many stakeholders in the automotive and IEEE 802.11 communities believe that stricter transmit mask or channel rejection constraints would be cost-prohibitive. The channel switching mechanism described in Section V-A uses time division to largely insulate CCH traffic (e.g., service advertisements) from SCH interference. CCI between two SCHs may result in some performance degradation if a receiver and an adjacent channel transmitter are in close proximity (especially if they are on the same vehicle). For non-safety related information, the performance penalty of CCI is likely to be tolerable. This leaves CCI involving BSM receptions on the safety channel (likely Channel 172, see discussion in Section V-A) as the biggest concern. It may be necessary to adopt additional constraints, either in standards or regulations, for the adjacent Channel 174. For example, transmissions on Channel 174 could use reduced power, could be limited to RSUs, or could be prohibited altogether.

In addition to addressing the transmit mask and channel rejection requirements, the IEEE 802.11p amendment also explicitly specifies OFDM operation in the 5.9 GHz band in the United States, as well as in a similar band defined for use in Europe.

B. OFDM Physical Layer Convergence Procedure (PLCP) Function

In a transmitter, the PLCP function is to process the bytes in a MAC frame so that they can be transformed into OFDM symbols for transmission over the air by the PMD. The PLCP adds PHY layer overhead to the MAC frame to create the PHY Protocol Data Unit (PPDU). The MAC sublayer passes three parameters to the PLCP along with the MAC frame: length of the MAC frame, transmit data rate (see Table 3), and transmit power. In a receiver the PLCP performs essentially the inverse function to extract a MAC frame from the PPDU. In addition to passing the received MAC frame up to the MAC sublayer, the PLCP also provides the RSSI. The PPDU format is shown Fig. 5.

The details of these fields have been stable in the IEEE 802.11 standard for a long time, and are not altered in the IEEE 802.11p amendment, nor are these fields used in any novel ways in DSRC. The *Preamble* is used to synchronize and equalize the signal at the receiver. A receiver operating on a 10 MHz channel must classify the channel as "busy" within 8 μsec after detecting the start of the *Preamble*. The *SIGNAL* field conveys the data rate and frame length. Since the data rate is unknown prior to reception of the *SIGNAL* field, the *Preamble* and *SIGNAL* are sent at a predetermined rate, more specifically at the lowest rate in Table 3, corresponding to BPSK and rate 1/2 coding. The lowest data rate is specified to maximize the probability that a receiver will successfully decode that portion of the frame. Even if the remainder of the frame cannot be decoded, reception of the *Preamble* and *SIGNAL* allows a receiver to estimate when the frame will end. The remainder of the PPDU uses the data rate indicated in the SIGNAL field. The *SERVICE* and *TAIL* fields facilitate bit scrambling. The *PAD* field ensures that the final OFDM symbol encodes the proper number of user bits from Table 3. The payload of the PPDU, the PHY Service Data Unit (PSDU), is the MAC frame.

IV. DSRC DATA LINK LAYER STANDARD (MAC AND LLC)

Like the PHY layer, the Data Link layer is commonly divided into sublayers. The lower of these is the *medium-*

access control (MAC) sublayer, which defines the rules by which STAs compete to share a wireless medium. The upper sublayer is the simpler *logical link control (LLC)*. The DSRC Data Link sublayers are described in the sections immediately following.

A. Medium-Access Control (MAC) Sublayer

The purpose of the MAC sublayer is to establish rules for accessing the common medium so that it can be shared efficiently and fairly among a set of STAs. The IEEE 802.11 rules fall into two categories: the session-based rules that define steps a STA must take before it is allowed to communicate information on behalf of Layer 3, and the frame-by-frame rules governing an individual transmission. The IEEE 802.11p amendment [2] makes significant changes to the session-based rules, while using the frame-by-frame rules as defined in the baseline IEEE 802.11 standard [16].

Session-Based Rules: The 802.11 standard defines a concept called the *Basic Service Set (BSS)*. A BSS is a set of STAs that agree to exchange data plane information. There are two types of BSS: *infrastructure* and *independent*. The infrastructure BSS is more common. It has a special *Access Point* (AP) STA that announces the BSS, and establishes some parameters and constraints for using the BSS. The AP serves as a gateway to a *distribution system* (DS) that provides access to additional networks beyond the wireless LAN, for example to the public Internet. Before a STA can transmit user plane data to the AP it first must hear the BSS announcement, in a beacon or probe response frame, and then go through a series of "setup" steps: Joining (which includes synchronizing with the AP STA's clock), Authenticating, and Associating.

The *independent* BSS has no AP or DS to provide backhaul connectivity; the STAs interact directly as peers. These STAs collectively shoulder the responsibility of announcing the existence of the BSS along with its parameters. Communicating within an independent BSS requires that the BSS first be announced, via a beacon frame, and that other STAs synchronize with the announcing STA.

For DSRC there are concerns about the delays attendant to following the setup steps outlined above, especially in the case of communicating through an AP. In a highly mobile vehicular environment, the opportunity to communicate may be fleeting, lasting only a few seconds, so there is a desire to define alternate, "lightweight" rules for accessing the medium.

That desire is in fact the primary motivation for the 802.11p WAVE amendment. The result of this effort is the definition of a new type of 802.11 communication "outside the context of a BSS" (abbreviated here "OCB"). In traditional 802.11, all data frames are sent between STAs that belong to the same BSS. By contrast, communication of data frames OCB is limited to STAs that do not belong to a BSS. There is no MAC sublayer setup required before STAs exchange data frames OCB.

The 802.11 frame header includes a 6-byte BSS identifier (BSSID) field. Each BSS is assigned an identifier by the STA that sends the beacon, for example in an infrastructure BSS the BSSID is the MAC address of the AP. Each frame sent within the context of a BSS includes the BSS's identifier in its header. The BSSID field of a frame sent OCB is set to all 1 s, i.e., 0xFFFFFF in hex notation, which is called the *wildcard* value. The purpose of the BSSID is to allow a receiver to easily distinguish frames that should be passed up the stack from frames that should be ignored. A receiver with the OCB capability enabled will configure the MAC to pass up any data frame with the wildcard value in the BSSID field, and to ignore any data frame sent by a STA in a coexistent BSS, i.e., with a non-wildcard BSSID. The OCB capability in IEEE 802.11p is designed to permit this type of coexistence with BSSs generally. However, the standard is more restrictive with respect to operation for DSRC. A STA operating in the 5.9 GHz DSRC band in the United States and in Europe is required by IEEE 802.11p to operate using the OCB capability, which means there will be no coexistent BSS in that band. This restriction might be relaxed in the future, e.g. , BSS operation might be permitted on a DSRC channel that does not support critical safety applications. The restriction in IEEE 802.11p might also be codified for United States operation in FCC regulations when they are updated to reflect the changing standards (see Section III).

A data frame sent OCB may carry an individual (unicast) or group (multicast or broadcast) destination address. The Basic Safety Message (see Section VI-A) will generally be encapsulated in a WAVE short message (WSM—see Section V-B) and then sent OCB to the broadcast destination address.

The IEEE 802.11p amendment introduces a new management frame, the *Timing Advertisement (TA)* frame, which can be used to announce information about the sender's time source. The 802.11p amendment also modifies the definition of the 802.11 *Vendor-Specific Action (VSA)* frame so that it can be used by organizations that have either a 24-bit or a 36-bit Organization Identifier (assigned by IEEE). The IEEE 1609 WG has a 36-bit identifier, and when the VSA is sent with this identifier, the payload of the frame may be used to convey a WAVE Service Advertisement (WSA—see Section V-B) on behalf of the management plane. The VSA frame could thus be used, for example, by an RSU that has a tolling service, traffic service, or commercial service to offer to passing vehicles.

There are few MAC-sublayer rules governing OCB communication. The most important is that a STA cannot engage in OCB communication while it belongs to a BSS. Management Frames must be of subtype TA or Action (including VSA). The definition of OCB communication is notable more for what it leaves out than for what it adds, and this proved somewhat controversial among

long-time 802.11 WG members. In particular, OCB communication does not:

- use a beacon frame;
- require one STA to synchronize with another before they can communicate;
- use authentication at the MAC sublayer; or
- include any notion of the STAs "associating" before they communicate.

Here are some reasons why these omissions are acceptable in the vehicular environment.

Lack of beacon: The 802.11 beacon periodically announces the existence of a BSS, and conveys parameters important to its correct operation, including the BSSID. The OCB type of communication does not utilize a BSS, and so does not need most of the beacon contents (see [16, Tabs. 7 and 8]). Some beacon contents, however, e.g., supported data rates or Quality of Service (QoS) parameters, are relevant and so alternative means of specifying them are needed for OCB communication. This can be within the 802.11p amendment (e.g., it specifies a distinct default set of QoS parameters for OCB communication), in another standard (e.g., SAE J2945.1), or via higher layer or management plane communication (e.g., the VSA frame carrying a WSA defined in IEEE 1609.3 can convey information about allowed data rates).

Synchronization: MAC sublayer synchronization between STAs is used within a BSS primarily to facilitate "power management" whereby a STA may alternate between "awake" and "doze" states. DSRC devices frequently have access to adequate power, and furthermore may wish to monitor a channel continually, so power management is not used with OCB communication, and MAC sublayer synchronization is not required. Vehicles engaged in V2V safety communication are assumed to have GPS for positioning, so they are inherently synchronized at the application layer. A device without GPS can synchronize via reception of a TA frame, if desired.

Authentication: Like synchronization, the need for authentication in OCB communication is determined at higher layers. In the DSRC model, a means of authenticating messages is provided by the IEEE 1609.2 standard [3]. This method, which is further discussed in Section V-C, is preferable to that defined in 802.11 for efficiency and privacy reasons. OCB communication that uses IPv6 rather than the 1609 upper layers can utilize a variety of well-established techniques for authentication, if desired.

Association: The association of STAs in an infrastructure BSS has a specific purpose, to help the AP bridge frames between a non-AP STA within the BSS and a node on the other side of the DS. V2V safety messages have no need of bridging. Many other DSRC messages (V2V or between a vehicle and an RSU) also reach their destinations in a single hop. If multihop forwarding is desired using an RSU as an intermediate node between a vehicle and a server, it can be achieved by layer 3 routing (e.g., using IPv6) or by bridging if the forwarding address is provided through other means (e.g., management frame, configuration). The OCB type of communication would only be used on the wireless link between the vehicle and the RSU. Multi-hop forwarding is beyond the scope of IEEE 802.11 for OCB communication; in particular it does not use the "To DS" and "From DS" bridging indicators that are available for communication to and from an AP [16].

In summary, the traditional 802.11 functions of beaconing, synchronization, authentication, and association are not needed at the MAC sublayer for OCB communication. The TA frame offers an optional, lightweight alternative to the beacon for synchronization. The other functions are optionally implemented at higher layers, either as part of a separate standard or via proprietary means.

The IEEE 802.11 WG has recently established a new task group (TGai) to develop an amendment for "Fast Initial Link Setup," [23] for scenarios in which the BSS AP hierarchy is still desired. It remains to be seen if this can be utilized for DSRC communications that are more "session-based," e.g., a service provided by an RSU. The OCB capability, however, is clearly preferred for V2V safety exchanges in which there is no AP. When the FCC updates its rules for DSRC operation, it may require OCB communication for the entire band, or for individual channels (e.g., the safety channel 172) within the band.

Medium Access Rules: IEEE 802.11 defines a complex set of rules that allow STAs to efficiently share the wireless medium. The most important points are summarized here. IEEE 802.11p does not alter these rules; they apply identically to frames sent within and outside of the context of a BSS. The basic medium access paradigm of IEEE 802.11 is "carrier sense multiple access/collision avoidance," or CSMA/CA. The simplest communication scenario under CSMA/CA is as follows:

1) A STA that has a frame to send first senses the wireless medium.
2)
   a) If the medium is idle the STA begins transmission of its frame.
   b) If the medium is busy, the STA performs a random "backoff" by choosing a number of idle time slots to wait before transmission. The countdown begins when the medium becomes idle, is interrupted during any non-idle interval, and resumes when the medium returns to idle.
3) The sender of a unicast frame waits for an acknowledgment (ACK) from the recipient; if it does not receive the ACK within a timeout interval it retransmits the frame after another random backoff. A frame sent to a group address is not acknowledged and is sent only once.

The *Enhanced Distributed Channel Access (EDCA)* QoS mechanism [16] provides different priorities of wireless

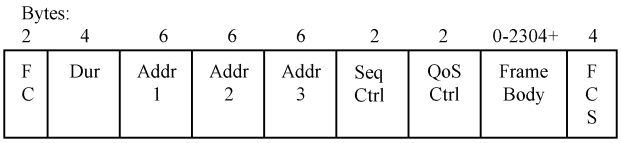

Fig. 6. *IEEE 802.11 MAC header, frame body, and FCS (most common form). (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)*

access primarily through selection of the idle time and backoff range parameters. There are many excellent papers that describe IEEE 802.11 EDCA in detail [24], [25], so it is not further discussed in this paper.

802.11 MAC Frame Format: Every 802.11 MAC frame consists of a *header*, *frame body*, and a *Frame Check Sequence (FCS)*. The frame body is passed into the MAC sublayer from a higher layer or from the management plane. The frame header can have a variety of formats, depending on the frame type (control, data, management).

The most common frame format is shown in Fig. 6 and briefly summarized here. The *Frame Control* field (shown as *FC* in the figure) includes a protocol version, a frame type and subtype, and several other bit fields. The *Duration* field (shown as *Dur* in the figure) indicates frame's time duration, possibly including some overhead beyond the physical transmission time. For a frame sent OCB, *Addresses 1, 2, and 3* contain respectively the MAC address of the sending device, the MAC address of the destination device, and the wildcard BSSID. The *Frame Check Sequence* field (shown as *FCS* in the figure) carries a 4-byte Cyclic Redundancy Code (CRC) computed over the header and frame body, which is used for detecting bit errors. The other fields, *Sequence Control* and *QoS Control* are outside the scope of this paper.

B. Logical Link Control (LLC) Sublayer

The LLC sublayer of the DSRC protocol stack uses the standard IEEE 802.2 [26] protocol supplemented with the *subnetwork access protocol (SNAP)* [27]. IEEE 1609.3 requires support of the LLC *unacknowledged connectionless (Type 1) service* with *unnumbered information (UI)* frames. With LLC SNAP [28], the protocol associated with the LLC payload is indicated by the EtherType. In DSRC the two recognized EtherType values are 0x88DC (WAVE Short Message Protocol) and 0x86DD (IPv6). Fig. 7 shows the LLC PDU format for DSRC, including the LLC and SNAP headers. This becomes the frame body of the MAC frame.

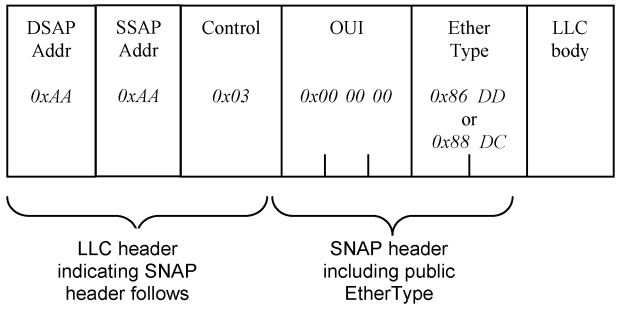

Fig. 7. *IEEE 802.2 LLC frame format used in DSRC. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)*

V. DSRC MIDDLE LAYERS

This section describes the architecture and standards that specify the middle portion of the DSRC protocol stack, as envisioned by the IEEE 1609 WG. Three principal functions are covered: *multichannel operation* (IEEE 1609.4 [5]), *networking services* (IEEE 1609.3 [4]), and *security services* (IEEE 1609.2 [3]).

The IEEE 1609 architecture (see IEEE 1609.0 [29]) generalizes the MAC sublayer of Fig. 2 into a set of one or more instances of the IEEE 802.11p MAC defined above, plus a channel switching protocol that defines how a given device can operate efficiently on multiple DSRC channels, one channel at a time. This multichannel operation concept [5] is described in more detail below.

As shown in Fig. 2, the DSRC protocol stack splits into two branches above the LLC sublayer. The first uses the WAVE Short Message Protocol (WSMP) defined in IEEE 1609.3 [4], which is optimized for the non-routed data exchanges that are common to vehicular networks, e.g., V2V safety messages. The second uses traditional internet protocols, principally IPv6, UDP, and TCP. In general, a service can choose to run over WSMP or IPv6, depending on its requirements. IEEE 1609.3 also defines the WAVE Service Advertisement (WSA).

The third major function defined within the IEEE 1609 suite is Security. Optional message authentication and encryption protocols are standardized in IEEE 1609.2 [3]. IEEE 1609.3 and 1609.4 were published in December 2010. IEEE 1609.2 is expected to be balloted and published in 2011.

In addition to the IEEE 1609.2, 1609.3, and 1609.4 standards, the IEEE 1609 WG is also developing the following standards (not discussed in detail in this paper):

- IEEE 1609.1—Remote management (e.g., for simple WAVE devices);
- IEEE 1609.11—Electronic Toll/Fee Collection;
- IEEE 1609.12—Defines Provider Service ID (PSID) allocations; [30]. The PSID is described later.

A. MAC Extension for Multichannel Operation: IEEE 1609.4

IEEE 1609.4 is applicable when DSRC is operating in a multi-channel environment, as it will in the U.S. 5.9 GHz band (see Fig. 4). IEEE 1609.4 defines a management extension to the MAC that allows a system with one or more radios to effectively switch among those channels.

Under this extension, a system maintains a separate logical instance of the IEEE 802.11p MAC, including queues and state variables, for each channel on which it operates. IEEE 1609.4 channel switching is optional; in particular a DSRC device is permitted to remain tuned to a single channel all the time.

The goal of IEEE 1609.4 is to define a mechanism by which devices that are switching among multiple channels will find each other, i.e., tune to the same channel at the same time. The problem is especially challenging for devices that have a single radio. The IEEE 1609.4 solution involves two concepts: the *control channel (CCH)* and *time division*. The CCH concept designates one channel (Ch. 178 in the US) as a special "rendezvous" channel that the devices will tune to on a regular basis. All other channels in the band plan are designated *service channels (SCH)*. The time division concept assumes that all devices have access to Universal Coordinated Time (UTC), e.g., from a GPS signal. IEEE 1609.4 defines a division of time into alternating CCH intervals and SCH intervals. During a CCH interval devices wishing to find each other rendezvous on the CCH. There they may hear WSAs announcing the availability of any services offered in the immediate area. The WSA provides information about one or more services, and indicates the SCH on which each is offered. During an SCH interval devices may switch to one of the SCHs.

Fig. 8 illustrates the basic time division concept defined in IEEE 1609.4. Time is segmented into "sync periods," which by default are 100 ms each. Each sync period consists of one CCH interval followed by one SCH interval. The default division is 50 ms for each.

Each CCH and SCH interval begins with a 4 ms guard interval, which is used by a switching device to transfer control from one virtual MAC to another. The device may begin receiving frames as soon as it is ready within the guard interval, but it normally will not transmit until the guard interval is complete because it will assume that its neighbors are still performing their own transitions. The guard interval also accounts for small errors in a device's representation of UTC. A device that does not switch channels is permitted to send at any time, including a guard interval. However, it cannot assume that a channel switching neighbor will be capable of receiving its transmissions during a guard interval.

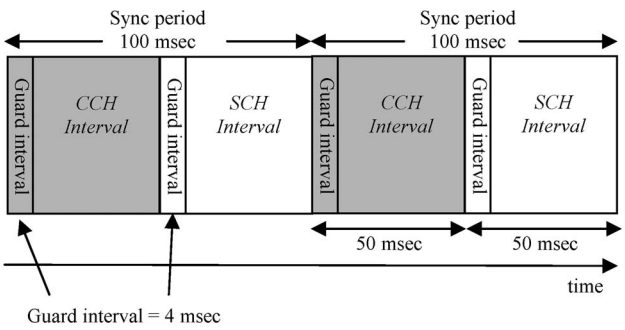

Fig. 8. ***Division of time into CCH Intervals and SCH Intervals. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)***

Switching to an SCH: If a device determines via a WSA that it is interested in accessing an advertised service (more on this process in the next subsection), it will switch to the relevant SCH. Normally it will switch at the end of the CCH interval and return to the CCH at the start of the next CCH interval. However, IEEE 1609.4 provides for an *immediate* departure option, in which the switch to the SCH can occur as soon as the WSA is received. It also provides for an *extended access* departure option in which the device remains on the SCH through one or more sync periods until service delivery is completed.

A device might also remain on the CCH during the SCH interval, e.g., if there is no WSA or the services advertised in a WSA are not currently of interest. A device tuned to the CCH during the SCH interval may transmit and receive, but in general its neighbors cannot be assumed to hear any transmissions, because they may be tuned to an SCH.

Synchronized Frame Collisions: The rendezvous time on the CCH is the 46 ms from the end of the CCH guard time to the end of the CCH interval. If a frame intended to be sent during the rendezvous time is enqueued during the other 54 ms of the sync period (i.e., during the SCH interval or CCH guard time), IEEE 1609.4 requires that the frame treat the channel as busy and enter back-off when the guard time expires. Within a transmission area, any two devices whose frames choose the same back-off time slot (by default a 1 in 16 probability) will experience a frame collision. If there are many such devices, the probability that any given time slot is chosen by exactly one frame will be quite small. This problem is referred to as "synchronized collisions." This is a significant concern if BSMs are constrained to be sent on the CCH during the CCH interval, since there could be hundreds of devices in a given area. However, synchronized collisions are relatively easy to avoid if the message generation function in the higher layers is provided with a signal indicating the start of a sync period. Then it can choose to enqueue its message at the MAC layer during a random time within the 46 ms interval. It may still find the channel busy and enter back-off, but at reasonable channel loads it is far less likely to suffer a collision. Synchronized collisions can also occur on an SCH at the start of the SCH interval. Annex B of IEEE 1609.4 recommends, but does not require a device to take steps to avoid this phenomenon.

Channel Switching and Safety Communication: An early version of IEEE 1609.4 required all DSRC devices to participate in channel switching, and in particular to visit the CCH during the CCH interval. Under that paradigm, V2V safety messages would also be exchanged during the 46 ms rendezvous time, and the capacity of the system for safety messages would be less than half that of a system that utilized a full-time channel. Concerns about the

reduced capacity for safety messages prompted research into other approaches, and led to the decision to make IEEE 1609.4 optional. An analysis of the performance associated with the channel switching safety paradigm and with several alternatives can be found in [31].

A consensus is developing in the industry to send all collision avoidance safety messages (specifically the BSM, Map Data, and Signal Phase and Timing messages, see Section VI-A) on Service Channel 172, with no time division. However, this implies that a vehicle desiring to participate in both safety and non-safety applications will require two DSRC radios, one that remains tuned to Channel 172 and one that participates in IEEE 1609.4 channel switching. A single-radio safety system will only send and receive on Channel 172. Congestion remains a concern even with a dedicated safety channel [31], and congestion control is one of the most important open research problems for DSRC [13], [32]–[35]. Since some vehicles might have only one DSRC radio, one can imagine that many stakeholders will desire their applications to also use Channel 172. The U.S. FCC has designated Channel 172 "exclusively for vehicle-to-vehicle safety communications for accident avoidance and mitigation, and safety of life and property applications" [12]. The balance between Channel 172 congestion and access is an outstanding DSRC policy issue, which must be addressed in future standards (e.g., SAE J2945.1) and government regulation (U.S. DOT and FCC).

Notwithstanding the removal of safety messages, there are still concerns about CCH congestion. Due to these concerns, only WSMs, WSAs, and other management frames are allowed on the CCH; IP packets are not allowed. The IEEE 1609 standards impose no packet-type restrictions on the SCHs, but constraints might be added in other standards (e.g., SAE J2945.1) or in FCC regulations, if necessary to protect high priority applications like V2V safety.

B. Network Services for DSRC: Network and Transport Layers, IEEE 1609.3

The Internet Protocol (IP) has become the default Layer 3 protocol in many networks today, especially those that are interconnected with other networks as part of the public Internet. The primary service that IP offers to higher layers is connectivity, i.e., the ability to find a path to a node anywhere, based only on its public IP address. The IP connectivity service is achieved via a set of highly successful IP routing protocols.

In the vehicular environment, however, many packets are sent directly over the air from the source to the destination, so routing is less of an issue. In order to avoid the packet overhead associated with internet protocols, a minimum of 52 bytes for a UDP/IPv6 packet, the IEEE 1609 WG defined a new Layer 3 protocol that is efficient for these 1-hop transmissions: the *WAVE Short Message Protocol (WSMP)*. Packets sent using WSMP are referred to as *WAVE Short Messages (WSMs)*. The minimum WSM overhead is 5 bytes, and even with options and extensions it will rarely exceed 20 bytes. Channel congestion is a significant concern in DSRC, especially on the channel used for BSMs, so the efficiency of WSMP is quite valuable.

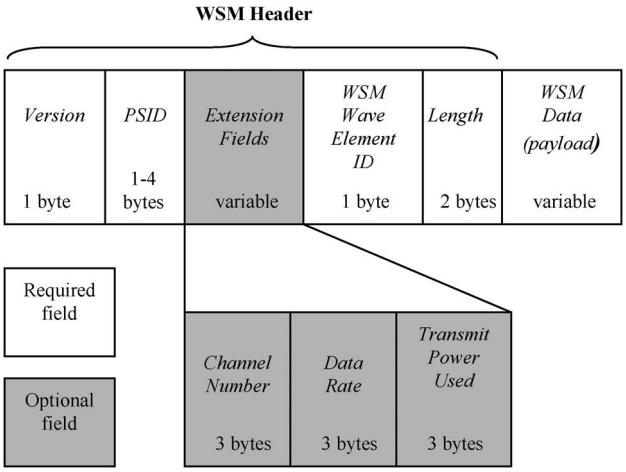

Fig. 9. *WAVE Short Message format. (Reproduced by permission of © 2010 John Wiley and Sons Ltd.)*

1) WAVE Short Message Format: The WSM format consists of a variable-length header followed by a variable-length payload, as shown in Fig. 9. The message format includes both mandatory and optional fields, defined later.

WSMP version: This mandatory one-byte field contains a 4-bit WSMP version number and 4 reserved bits. The version number associated with the current 1609.3 standard [4] is 2. A receiver will discard a WSM with a version number higher than it was designed to support.

Provider Service IDentifier (PSID): The mandatory PSID identifies the service that the WSM payload is associated with. A device creates a list of PSIDs that have active receive processes at higher layers. When a WSM arrives, if the PSID matches one of those on the list, the WSM payload is forwarded to that process. In this way, the PSID serves a purpose that is similar to a TCP or UDP Port.

For bandwidth efficiency, PSIDs are defined in a variable-length format. Leading bits are used to indicate the number of bytes in the PSID, as shown in Table 6.

Table 6 Provider Service Identifier (PSID) Lengths and Ranges

Leading bits in first byte of PSID	Length of PSID (bytes)	Range of PSID values for this length (hex representation)	Number of PSID values for this length
0	1	0x00-0x7F	2^7
10	2	0x8000-0xBFFF	2^{14}
110	3	0xC00000-0xDFFFFF	2^{21}
1110	4	0xE0000000-0xFFFFFFFF	2^{28}

A leading bit of 0 indicates a 1-byte PSID. Similarly, leading bits of 10, 110, and 1110, respectively, indicate a 2-byte, a 3-byte or a 4-byte PSID.

PSIDs are currently administered by the IEEE 1609 WG, with some values assigned at the request of other standards organizations (e.g. SAE). There is an effort underway to harmonize the PSID and a similar identifier used in some European standards, so that identifiers will be drawn from a common number space. The IEEE 1609.12 draft standard [30] was recently started to document allocations that have been made by IEEE 1609 and other standards organizations from this number space. The current draft IEEE 1609.12 reflects nine PSID values requested by SAE for application areas associated with the J2735 messages.

WSM Extension Fields: In IEEE 1609.3 there is a facility for including an optional "extension field" in a WSM or WSA header. This facility provides flexibility for the protocol to omit or include a field considered optional. It also provides extensibility so that new extension fields can be defined in future revisions.

An extension field consists of three fields: a one-byte *identifier*, a one-byte *length*, and a variable-length *contents* field whose size (in bytes) is indicated in the *length* field. Since a given extension field may or may not be present, its presence needs to be explicitly signaled. The *identifier* provides that indication, distinguishing one extension from another; *identifiers* are unique and are defined in the 1609.3 standard. The *length* field also supports flexibility and extensibility. An explicit *length* indicator allows the *contents* field to be variable length, which promotes bandwidth efficiency in longer fields. More importantly, the *length* indicator allows a legacy device to skip over an extension whose *identifier* it does not understand, and continue parsing the rest of the message. This will be important when extension fields are added in the future, after devices are deployed.

The current version of IEEE 1609.3 defines three extension fields for the WSM. The *contents* field of each uses one byte, so with the *identifier* and *length* each extension is three bytes long. Note that since each is fixed length and is defined in the original revision of the WSMP version 2 protocol, the *length* field could have been omitted as redundant, but it is included for consistency with future extensions, at the cost of one byte. The three WSMP extensions are:

- **Channel Number**: Interpreted in the context of a particular regulatory domain, e.g., see Fig. 4 for U.S. 5.9 GHz band channel numbers.
- **Data Rate**: Using an IEEE 802.11 format with resolution 500 Kbps.
- **Transmit Power Used**: A signed integer with resolution 1 dBm

WSMP WAVE Element ID: This mandatory one-byte field marks the end of the extension fields and indicates the format of the WSM Data field.

Length: This mandatory two-byte field is the final byte of the WSM header. Its value is equal to the number of bytes in the WSM Data field, which follows immediately. The valid range is 0–4095, but a smaller maximum length may be defined in the Management Information Base (MIB). The upper four bits of this field are reserved.

WSM Data: This is the payload of the WSM. Some or all of this data is provided by higher layers at the sender and is passed to higher layers at the receiver. In some cases additional protocol information is inserted in a "shim header" at the sending device. The format of the WSM Data field is indicated by the WSMP WAVE Element ID value. In the current version of IEEE 1609.3 three formats are defined, indicated by WSMP WAVE Element ID values 128, 129, and 130. In one format (ID = 128) all of the WSM Data belongs to the higher layer. The other two formats include a shim header pre-pended to the higher layer data. One of these shim headers (ID = 130) relates to remote management and is defined in IEEE 1609.1. The other shim header option (ID = 129) is the so-called WSMP Safety Supplement (WSMP-S) Control field. The use of WSMP WAVE Element ID 129 is optional if the higher layer data is safety-related; if ID 129 is not used then ID 128 is used and the WSMP-S Control field is not inserted. As noted above, there is an ongoing debate about which channel will be used for V2V safety messages. Some of the alternatives outlined in [31] rely on extra protocol information, and the WSMP-S Control field was defined to convey that information. However, the WSMP-S Control field is itself extensible. In the long term its utility may expand to include support of other functions related to improving DSRC safety, e.g., conveying information useful to an adaptive congestion control algorithm.

2) WAVE Service Advertisement Format: The WSA includes information about one or more DSRC services that are offered in an area. A service can be almost any information exchange that provides value to a vehicle's occupants. Example services include traffic alerts, tolling, navigation, restaurant information, entertainment, and Internet access. Most services are provided by an RSU, but a vehicle could also send a WSA. The information exchange within a service can be unidirectional or bidirectional. WSAs are sent on the CCH during the CCH interval. The services they advertise are offered on one or more of the SCHs. One type of DSRC communication that is not considered a service is the broadcast of Basic Safety Messages from a vehicle to its neighbors. Those broadcasts are not advertised via a WSA.

A WSA-sender may support more than one service offering. For efficiency, it can provide information about up to 32 services in a single WSA. Services can be supported by either the IPv6 or WSMP part of the protocol stack. The information passed in the WSA will vary depending on the service protocol, as shown below. The WSA is intended to

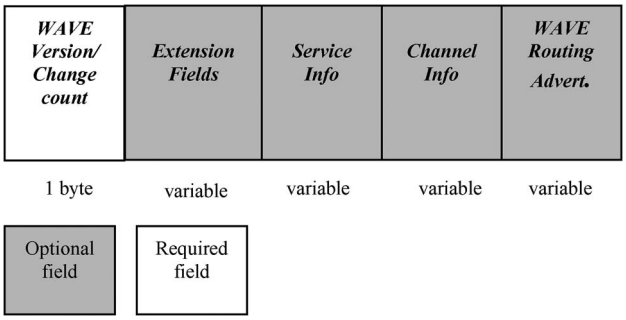

Fig. 10. *WAVE Service Advertisement format.*

be carried within an IEEE 802.11 Vendor Specific Action (VSA) management frame. The WSA is a management message; it originates in the management plane of the sender and is processed in the management plane of the receiver. The decision to access an advertised service is not standardized; typically it depends on factors including the type of service (indicated by PSID), the quality of the link to the service provider, the time since the vehicle most recently accessed this service, the availability of competing services, the cost of the service, etc. The WSA format is shown in Fig. 10.

WAVE version/Change count: This mandatory one-byte field conveys the 4-bit version number that defines the format of this WSA. The version number associated with the current standard is 1. This serves the same purpose for a WSA as the WSMP version serves in a WSM. The remaining four bits are a modulo-16 content change counter. The sender increments the counter when it updates the content of the WSA. This provides an efficient way for a receiver to filter out duplicate WSAs.

WSA header extension fields: As with the WSM, optional extension header fields are allowed in the WSA header, and they are encoded using the same *identifier/length/contents* format. The aggregate length of the WSA header extensions must not exceed 254 bytes. In the current standard six extensions are defined as follows.

- *Repeat Rate*: An 8-bit unsigned integer indicating the number of WSA broadcasts per five seconds. Monitoring the success rate of repeated broadcasts, along with other measures like received power level, provides a way to estimate link quality.
- *Transmit power used*: An 8-bit signed integer indicating the power with which the WSA's frame was transmitted, with resolution 1 dB.
- *2D Location*: An 8-byte field conveying the location of the transmitting device, encoded as a 32-bit latitude and 32-bit longitude, with 1/10 micro-degree resolution.
- *3D Location and confidence*: A 15-byte field conveying the 3D location of the transmitting antenna (32-bit latitude, 32-bit longitude, and 16-bit elevation), the position and elevation confidence (4 bits each), and a 4-byte position accuracy indication.
- *Advertiser Identifier*: a text string of 1 to 32 bytes associated with the WSA sender.
- *Country String*: a 3-byte field using a format defined in IEEE 802.11 to convey the country regulatory domain of the sender.

Service Info: The WSA header extensions are followed by 0 to 32 instances of a Service Info field. This is where services are actually advertised. Each Service Info field advertises one service. Each Service Info field has the following content.

- One-byte WSA WAVE Element ID. Value 0x01 indicates Service Info.
- 1-to-4-byte Provider Service Identifier (PSID), indicating the type of service being advertised, see WSM format above.
- One-byte Service Priority, with values restricted to the range 0–63 (0 is lowest priority). This priority is associated with the higher layer process initiating the advertisement. It is used to help arbitrate access to competing advertised services.
- One-byte Channel Index. Indicates which of the Channel Info fields that follow (see below) is associated with this service.
- Variable length Service Info Extension Fields. These extensions are specific to a service info field, and they utilize the same encoding format as other extensions. The Service Info Extensions defined in the current standard are as follows.
  - Provider Service Context (PSC)—a string of up to 31 bytes that provides additional information about the service. Each PSID has a unique PSC format, which is defined by the organization to which the PSID is assigned.
  - IPv6 address—a 16-byte address of the entity hosting the service, if the service is provided using IPv6 rather than WSMP.
  - Service Port—a two-byte port number for the transport layer protocol (UDP or TCP) if the service is provided using IPv6.
  - Provider MAC Address—a six-byte IEEE MAC address of the device hosting the advertised service, if different from the MAC address of the device sending the WSA.
  - RCPI Threshold—a one-byte Received Channel Power Indicator value indicating the minimum WSA received power recommended prior to attempting to access the service, with range 0 to −110 dBm.
  - WSA Count Threshold—a one-byte count indicating the minimum number of WSAs recommended to be received prior to attempting to access the service, with range 0 to 255 WSAs.

- WSA Count Threshold Interval—a one-byte time interval over which the WSA Count Threshold is measured, with range 0.1 to 25.5 seconds. If absent, the WSA Count is measured over 1 second.

Channel Info: The Service Info fields are followed by 0 to 32 instances of a Channel Info field. There is one Channel Info field for each channel on which an advertised service is offered. A Service Info field is linked to a Channel Info field by the Channel Index in the Service Info field. Each Channel Info field has the following content.

- One-byte WAVE Element ID. Value 0x02 indicates Channel Info.
- Two-byte Operating Class and Channel Number. These follow a format defined in IEEE 802.11. Together they indicate the channel to which the remaining information applies. In the U.S. this would normally be one of the channels shown in Fig. 4.
- One-byte Adaptable field, of which only one bit is used, as a bit flag. If the flag is 0, then the Data Rate and Transmit Power Level (see directly below) are fixed. If the flag is 1, then the Data Rate is a lower bound and the Transmit Power Level is an upper bound. In that case higher rates and/or lower power levels are allowed when accessing the service.
- One-byte Data Rate, a signed integer with resolution 500 Kbps, the allowed range is 1.0 to 63.5 Mbps.
- One-byte Transmit Power Level, applied to transmissions on the indicated channel. The resolution is 1 dB and the range is −128 dBm to +127 dBm.
- Variable length Channel Info Extension Fields: These extensions are specific to a Channel Info field, and they utilize the same encoding format as other extensions. There are two Channel Info extension fields in the current standard as follows.
  - EDCA parameter set: The format of the EDCA parameter set is defined in IEEE 802.11. The default EDCA parameter set for OCB communication is defined in IEEE 802.11p. This extension field provides an opportunity to advertise a non-default set for up to four different priority classes. Note: the IEEE 1609 WG plans to issue a corrigendum (correction) to [4] to clarify that when the EDCA extension field is included it may consist of parameters for between one and four EDCA access categories.
  - Channel Access: A bit flag within a one-byte field. The value 0 indicates that the service is available all the time, and the value 1 indicates that the service is available only during SCH intervals.

WAVE Routing Advertisement (WRA): This is an optional field within the WSA. It is only used when an advertising device offers a service that utilizes the IPv6 part of the protocol stack. The WRA provides information about how to connect to the Internet, which a receiver (e.g., a vehicle) can incorporate in its network configuration. Each WSA includes at most one WRA. If present, the WRA consists of a fixed-length mandatory part followed by a variable-length optional extension. Each extension includes an explicit length indicator, so it is not necessary to also explicitly indicate the length of the entire WRA.

- **WAVE Element ID**: a mandatory one-byte field set to 0x03. This distinguishes the WRA from a Channel Info field.
- **Router Lifetime**: a mandatory two-byte field indicating how long, in seconds, the Default Gateway information that follows is valid.
- **IpPrefix**: a mandatory 16-byte IPv6 subnet prefix.
- **Prefix Length**: a one-byte value indicating how many of the 128 bits in the preceding IpPrefix are significant.
- **Default Gateway**: a mandatory 16-byte IPv6 address of the default router used to achieve internet connectivity.
- **Primary DNS**: a mandatory 16-byte IPv6 address of a device that can serve as a Domain Name Server;
- **WRA Extension Fields**: optional extension fields using the normal format; the current standard defines two extension fields:
  - Secondary DNS: 16-byte IPv6 address
  - Gateway MAC address: 6-byte IEEE MAC address, if different than the MAC address of the WSA transmitter.

C. Middle Layer Security Services: IEEE 1609.2

The general topic of security in vehicular networks is a complex subject. This subsection explains how the basic principles are applied in the specific case of the IEEE 1609.2 [3] standard: Security Services for Applications and Management Messages. As this paper is being written the IEEE 1609.2 standard is in draft stage. Some changes are likely during the balloting process, which is expected to be completed in 2011. IEEE 1609.2 defines standard mechanisms for authenticating and encrypting messages, especially WSMs and WSAs. This subsection focuses on authentication of a vehicle safety message, i.e. a Basic Safety Message (BSM) carried in a WSM. In addition to the algorithm and frame formats currently defined in IEEE 1609.2, the general area of "DSRC security" involves other issues as well. A cooperative U.S. DOT and automotive industry project called V2V-Communications Security [36] is developing solutions related to the following open questions: a) type of wireless communication to be used between a vehicle and the security infrastructure [i.e., Certificate Authority (CA)], b) type of Public Key Infrastructure (PKI), e.g., policy regarding

certificate validity, certificate encryption, and certificate revocation, c) protecting the privacy of vehicle drivers and owners, d) physical security of DSRC devices, and e) detection and reporting of misbehaving DSRC devices. Some of the solutions to these open issues may eventually be reflected in the IEEE 1609.2 standard, while others will likely be documented in government regulations.

IEEE 1609.2 Authentication: An authenticated message carries a *digital signature* that can be used to verify that the sender had the authority to send the message and that the content has not been altered. IEEE 1609.2 authentication uses the Elliptic Curve Digital Signature Algorithm (ECDSA), which is an asymmetric cryptographic algorithm. Two different key lengths are specified, 224 bits and 256 bits. ECDSA is a relatively processor-intensive algorithm, which is a concern in the cost-sensitive vehicle market, especially given that a receiver might receive hundreds of safety messages per second. Signing or verifying a message with the 224-bit version of ECDSA takes about 60–80% as much processing time as the 256-bit version [37], so it has been the plan to sign BSMs using the 224-bit key. However, the emergence of the implicit certificate option (see below) has called that plan into question recently.

Certificate Content: To sign a message a sending device must have a private signing key and a certificate containing the public key associated with that private key. The receiver uses the public key to verify the signature. The certificate also includes information about how a receiver can check if the certificate has been revoked. For privacy reasons, the certificate a vehicle will use to sign safety messages will not carry information that is easily linked to permanent identifiers for that vehicle. The issuing Certificate Authority (CA) can identify the certificate holder, but even that capability can be split among multiple authorities to prevent abuse.

In addition, the certificate carries various scoping restrictions with regard to time, content, and location (location is more important in the case of an RSU certificate). With privacy again in mind, the vehicle will typically use a given certificate for a limited time (e.g., 5 to 10 min), so that the vehicle's movements cannot easily be tracked by its safety broadcasts over long intervals. When the vehicle changes certificates it also changes other identifiers in its safety messages, e.g., source MAC address, Temporary ID and Sequence Number in the BSM (see Section VI-A). A vehicle will typically be reloaded with new certificates infrequently (e.g., annually). To prevent a so-called Sybil attack in which an attacker gains access to multiple valid certificates and uses them simultaneously, only one certificate will be valid at any given time. For example, a vehicle might carry on the order of 100 000 certificates, each of which is valid for a different five minute period in the coming year. Even if all of those certificates are stolen, the attacker can only use one at a time to impersonate the certificate owner. This principle can be relaxed to allow a short (e.g., 30 second) overlapping validity interval between consecutive certificates, so that certificate transitions can be randomized for privacy, and so that a vehicle will have some flexibility to defer a transition during a critical safety event.

The certificate carries a list of PSIDs that the sender is authorized to use in its WSM transmissions. For example, a vehicle will have certificates authorizing it to send a WSM with the PSID that is associated with the Basic Safety Message. The certificate may also indicate content-specific permissions that the sender has. For example, an SAE J2735 emergency vehicle alert message (EVAM) might be sent by a number of emergency vehicle types, including police cars, ambulances, and tow trucks. A siren indication within the EVAM is permissible for an ambulance or police car, but not for a tow truck. The certificate attached to an EVAM will authorize the PSID value with which the EVAM is associated, and in addition will include a service specific permissions (SSP) field indicating which content within the message the sender is authorized to set. The format of the SSP field consists of a 1-byte length indicator followed by up to 31 additional bytes. The format of the SSP is specific to a given PSID value, and is defined by the organization that defines the meaning of that PSID value (i.e., defined by SAE in the case of the PSID associated with the J2735 EVAM). The SSP field can be absent, indicating that there are no content-specific restrictions for that PSID value.

Finally, the certificate carries its own authentication field, signed by the CA using the CA's private key. A recipient of the certificate can use the CA's public key to authenticate the certificate itself. The CA's public key is usually well known, and thus it does not need to be disseminated using DSRC. Since a CA's public key has a much longer lifetime than a DSRC sender's public key, it will normally utilize the 256-bit version of ECDSA for stronger security.

The sender's public key and the CA's authentication can be provided by a certificate in two ways. In an *explicit certificate* these are supplied in separate fields within the certificate, for example a 224-bit sender public key field and a 256-bit CA signature.

Alternatively, in an *implicit certificate* the sender's public key and the CA's authentication are supplied implicitly via a *reconstruction field*. A receiver can use the CA's public key and the reconstruction field value to recover the sender's public key, and in the process it can authenticate the certificate itself. An implicit certificate requires that the sender and CA use the same length key, so in the case of BSM certificates it would likely revert to the higher security 256-bit key. The length of the reconstruction field is equal to the key length. The replacement of explicit sender public key and CA signature fields with a single reconstruction field allows an implicit certificate to save on the order of 50 to 60 bytes compared to an explicit

certificate. This is a significant saving, and the IEEE 1609 WG is thinking about specifying this approach as an option [3]. The implications for processing burden depend somewhat on implementation choices, but generally implicit certificates are expected to represent roughly the same processing requirement as explicit certificates.

Certificate Digest: An explicit certificate can be on the order of a hundred bytes or more in length. Even the smaller implicit certificate is significant compared to the vehicle state content in a BSM (which varies between about 50 and 150 bytes). In order to reduce the security overhead, a WSM might carry a *certificate digest*, which is a short (e.g., 8 byte) hash of a certificate, in place of the certificate itself. A digest can be used in place of either an explicit or an implicit certificate. If a vehicle has once received a full certificate from another vehicle, it can recognize a certificate digest in a subsequent message and use the cached certificate to verify the signature. On the other hand, a vehicle cannot begin to verify messages from a given sender until it sees a full certificate. A sending vehicle might interleave BSMs carrying full certificates and BSMs carrying certificate digests, trading off the bandwidth consumed against the latency to verify a first message from that sender. The interleaving schedule is one of many open security issues for vehicle safety security. Use of certificate digests does not impact security processing significantly because the hash operation is very simple.

Other Security Overhead: In addition to the digital signature and the certificate (or certificate digest), a signed message may also include other security overhead. For example, it may optionally include a message generation time and validity period, or a location and validity region. These can be used, respectively, to prevent temporal or spatial replay attacks. In the case vehicle safety, the BSM already includes absolute generation location, and the recipient is able to judge whether the transmitter location is close enough to be relevant, so there is no need for location security overhead. Generation time in the BSM is only modulo-one minute, so an absolute generation time is included in the certificate.

IEEE 1609.2 Encryption: Though the focus of this subsection is authentication for vehicle safety messages, the IEEE 1609.2 standard also defines an encryption algorithm, which uses a combination of symmetric and asymmetric cryptography. In the current standard, one symmetric algorithm and one asymmetric algorithm are specified. The symmetric algorithm is the Advanced Encryption Standard with 128-bit keys in Counter with CBC MIC mode, i.e. AES-CCM. The asymmetric algorithm is the Elliptic Curve Integrated Encryption Scheme (ECIES). Since symmetric cryptography requires less processing, the sender will encrypt the message with a symmetric key, and then will encrypt the symmetric key using the asymmetric algorithm. The receiver does the inverse, decrypting first the symmetric key, and then the message. The bulk of the cryptography is done using the efficient symmetric algorithm. It is also possible for a message to be both signed and encrypted, in that order. IEEE 1609.2 security services will normally be invoked by the message sublayer (see Fig. 2), and the secured message will become the payload of a 1609.3 WSM.

VI. DSRC MESSAGE SUBLAYER

At the top of the protocol stack in Fig. 2, the Application Layer includes application processes and additional protocols that provide direct support to applications. An example of the latter is the SAE J2735 DSRC Message Set Dictionary standard, which defines fifteen messages that collectively enable a core set of DSRC applications. This section describes these messages, and examines the Basic Safety Message in detail. The SAE DSRC committee is also developing a complementary standard, J2945.1 [7], which defines additional rules for using BSMs to implement V2V safety systems.

A. SAE J2735 DSRC Message Set

In this section the names of data structures defined in the J2735 standard are represented in this font: `Sample`. Table 7 lists the fifteen message types that are defined in the SAE J2735 standard [6].

The SAE DSRC committee is developing additional message types that will appear in a future revision of J2735, for example a message to enable cooperative cruise control. In addition, the U.S. DOT is planning to propose additional content in SAE J2735 to solidify the systems engineering behind the standard, for example content related to concept of operations and development of requirements. That proposal is expected to be provided to the SAE in early 2012.

SAE J2735 defines the format of each of the message types listed in Table 7. Each message is defined as a collection of constituent data structures called *data elements* and *data frames*. A data element is the most basic data structure in the J2735 standard. A data frame is a more complex data structure, composed of one or more data elements or other data frames. The J2735 standard defines the syntax (length, format) and semantics of each data element and data frame.

An example of the relation between data elements and data frames can be seen in the `ApproachesObject` data frame, which is used as part of the description of an intersection. The `ApproachesObject` frame is made up of four constituent parts: a `Position3D` frame, a simple `LaneWidth` element, and two instances of a frame called `Approach`, one each for ingress and egress lanes. The `Approach` frames are each in turn composed of a collection of several data elements and data frames that describe a set of lanes. The `ApproachesObject` data frame is itself a constituent of a larger frame called `Intersection`. Ultimately, messages are composed of

Table 7 SAE J2735 DSRC Standard Message Types

Message Type	Purpose
A La Carte Message	Generic message with flexible content
Basic Safety Message	Conveys vehicle state information necessary to support V2V safety applications
Common Safety Request	A vehicle uses this to request specific state information from another vehicle
Emergency Vehicle Alert Message	Alerts drivers that an emergency vehicle is active in an area
Intersection Collision Avoidance	Provides vehicle location information relative to a specific intersection
Map Data	Sent by RSU to convey the geographic description of an intersection
NMEA Corrections	Encapsulates one style of GPS corrections – NMEA style 183
Probe Data Management	Sent by RSU to manage the collection of probe data from vehicles
Probe Vehicle Data	Vehicles report their status over a given section of road; aggregated to derive road conditions
Roadside Alert	Sent by RSU to alert passing vehicles to hazardous conditions
RTCM Corrections	Encapsulates a second style of GPS corrections – RTCM
Signal Phase and Timing Message	Sent by RSU at a signalized intersection to convey the signal's phase and timing state.
Signal Request Message	A vehicle uses this to request either a priority signal or a signal preemption.
Signal Status Message	Sent by RSU to convey the status of signal requests.
Traveler Information	Sent by RSU to convey advisory and road sign types of information

collections of data elements and data frames. The hierarchical structuring of data elements, data frames, and messages encourages reuse of data structures. A given message can be decomposed in a tree structure, with each branch ultimately ending in a data element. SAE J2735 defines approximately 150 data elements and 70 data frames.

The data elements, data frames, and message types in J2735 are defined in *Abstract Syntax Notation One (ASN.1)*, which is defined in the ITU-T X.680 series of standards. SAE J2735 also specifies the use of the *Distinguished Encoding Rules (DER)* to translate the ASN.1 into over-the-air bits and bytes. DER, a subset of the Basic Encoding Rules (BER), is defined in the ITU-T X.690 standard [38]. DER encodes each data item (element or frame) in a three-part structure consisting of an *identifier*, a *length*, and the *contents*. The encoding is recursive, i.e., the *contents* field of one frame consists of the entire *identifier*, *length*, and *contents* of each of the constituent parts. The use of ASN.1 and DER encoding has three principal advantages: interoperability of data types, efficient parsing using the *identifier, length, contents* structure, and extensibility while providing backward compatibility for legacy implementations. The DER encoding can also impose a data size (and therefore bandwidth) penalty, however. Each tag and length represents overhead, and if the value fields are short the overhead can be significant. In some cases, notably the `Basic Safety Message`, some of the flexibility of DER encoding is sacrificed in the name of bandwidth efficiency. The next subsection describes the Basic Safety Message use case in more detail.

Case Study—The Basic Safety Message: The BSM is perhaps the most important message in the J2735 standard. It conveys core state information about the sending vehicle, namely its position, dynamics, system status, and size. It also has the flexibility to convey additional information as needed. There has been extensive research into the content of safety messages for collision avoidance [9]. This research demonstrated that although there are many distinct collision avoidance applications, there is a significant overlap in the state information that each application in a receiving vehicle needs from its neighbors. This commonality led to the definition of the `BSM` for support of all V2V safety applications, rather than defining a group of application-specific messages.

The common requirements only go so far, however. The `BSM` has two parts. Part I includes critical state information that must be sent in every `BSM`. The data structure for Part I emphasizes compactness and efficiency. Part II is an optional area where additional data elements and frames can be included. Part II provides three forms of flexibility: 1) inclusion of some data types at a frequency less than the overall BSM rate; 2) evolution in the definition of new state information (e.g., from new types of sensor) and new applications; and 3) customization of messages to include company-specific features.

Table 8 lists the content of the `BSM` Part I, which is present in every `BSM` transmission. The first column of the table uses the official data structure terminology from the standard. The constituents of Part I are an exception to the recursive encoding rule mentioned above. There is a heightened sensitivity to the bandwidth consumed by `BSMs` in general and Part I of `BSMs` in particular. For that reason, the constituent pieces of the `BSM` Part I are not individually DER-encoded, since the identifier and length would add at least two bytes for each. The content shown in Table 8 consumes 39 bytes, and DER-encoding the individual items would add approximately equal overhead. So, instead DER-encoding is applied to just two items. The `DSRC_MessageID` must be separately DER-encoded because it is parsed independent of the rest of the content. The remainder of Part I is defined as one complex element (called the `BSM_blob`), to which one DER tag and length are applied. The components of the `BSM_blob` are of fixed length and known order, so there is no need for each component to have an explicit *identifier* and *length*.

Table 8 SAE J2735 DSRC Basic Safety Message Part I

Data item name, Element/Frame, and length	Description
DSRC_MessageID element, 1 byte	The first element in every message, used by the parser to determine how to parse the rest of the message
MsgCount element, 1 byte	A sequence number, incremented with each successive transmission of a **BSM** by a given vehicle, used primarily to estimate packet error statistics.
TemporaryID element, 4 bytes	A value chosen randomly and held constant for a few minutes, it helps a receiver correlate a stream of **BSMs** from a given sender.
DSecond element, 2 bytes	The current time, modulo one minute, with resolution 1 millisecond.
Latitude, Longitude 2 elements, 4 bytes each	Geographic latitude and longitude, with resolution 1/10 microdegree.
Elevation element, 2 bytes	Position above or below sea level, resolution 0.1 meter.
PositionalAccuracy frame, 4 bytes	Conveys the one-standard-deviation position error along both semi-major and semi-minor axes, and the heading of the semi-major axis.
TransmisionAndSpeed frame, 2 bytes	3 bits encode vehicle transmission (gear) setting. 13 bits convey unsigned vehicle speed, resolution 1 cm/second.
Heading element, 2 bytes	Compass heading of vehicle's motion, resolution 1/80 degree.
SteeringWheelAngle element, 1 byte	Current position of the steering wheel, resolution 1.5 degree. Clockwise rotation is a positive angle.
AccelerationSet4Way frame, 7 bytes	Provides longitudinal acceleration, lateral acceleration, vertical acceleration, and yaw rate.
BrakeSystemStatus frame, 2 bytes	Conveys whether or not braking is active on each of four wheels, also conveys the status of the following control systems: Traction Control, Anti-Lock Brakes, Stability Control, Brake Boost, and Auxiliary Brakes.
VehicleSize frame, 3 bytes	Vehicle length and width, resolution 1 cm.

There are four data items that are most often discussed for inclusion in Part II of the BSM. These are collected in a data frame called VehicleSafetyExtension, which is shown in Table 9. A given BSM may include the VehicleSafetyExtension frame or not, and a given VehicleSafetyExtension frame may be composed of any combination of the four data items shown. The first item reports the occurrence of one or more "events," and is included in the message only when there is at least one event. The remaining three items are considered necessary for the operation of some safety applications (see Annex C.8 of [6]), but they are not required to be updated as frequently as the Part I data, so they are not included in every BSM. The PathHistory and RTCMcorrections fields can also be quite lengthy. The sub-rate necessary for each of these items is an open research question, and is expected to be addressed in SAE J2945.1 (see below).

Table 9 VehicleSafetyExtension Data Frame, Required for Some Safety Applications, Sent in Part II of Some BSMs

Data item name, Element/Frame, and length	Description
EventFlags element, 2 bytes	An optional set of bit flags, each of which can convey the occurrence of a given "event." A given event may be flagged only if a set of minimum activation criteria are met. Examples include: Hard Brake, Hazard Lights, Emergency Response Vehicle, Stop Line Violation
PathHistory frame, variable length (typically on the order of 20 bytes for a straight path and less than 100 bytes for a curved path)	Used to convey where a vehicle has been, in the form of individual data structures sometimes called "Bread Crumbs." Each bread crumb includes a prior position, and optionally time and position accuracy. **PathHistory** is useful in identifying lane level information in the absence of map data. The number of bread crumbs in a frame is a function of the degree to which the actual path can be represented in piecewise linear fashion.
PathPrediction frame, 3 bytes	Indicates the path that a sender expects to traverse. 2-byte radius of curvature and 1-byte prediction confidence.
RTCMPackage frame, variable	Conveys GPS correction data in the RTCM style. Variable length depends on number of satellites in view.

B. SAE J2945.1 Minimum Performance Requirements

The SAE DSRC committee realized that specification of the message format was not sufficient to ensure interoperability of V2V safety applications. Additional rules are required, and the SAE J2945.1 *DSRC Vehicle BSM Communication Minimum Performance Requirements* (MPR) draft standard [7] is being developed to document those rules. This work is in its early stages. A first version is expected to be published as a "recommended practice" in 2011, with more complete "standard" versions to follow as V2V safety systems approach deployment. In the long term this is expected to be part of a series of J2945.x standards, each of which addresses MPR for a given message or group of similar messages.

The motivation for J2945.1 is to define additional constraints on a BSM sender, beyond syntax and semantics, such that a receiver will know enough to provide effective driver warnings for collision prevention. The initial areas that J2495.1 is expected to address are:

BSM Sending Rate: A key question is how often a vehicle should send BSMs. BSMs that are sent too frequently add to channel load with little marginal benefit. BSMs that are sent too infrequently may fail to provide information in a timely manner needed to provide driver warnings. Constraints may be needed for both a maximum and minimum message rate. This is complicated for a number of reasons:

- Ideally these constraints would be a function of safety application performance, but 1) there are no standardized safety applications, and 2) even for

prototype applications it is very difficult to translate application level performance into message rates (or into other J2945.1 constraints, like sensor accuracy). For example, some simple applications may be able to provide an effective driver warning based on the reception of a single message in a critical time window, while others may require receipt of two or more messages before providing a warning.

- The optimal message rate will depend on the physical characteristics of the communication channel, which vary widely and change rapidly.
- The optimal message rate will also depend on the ability of a receiver to model the sender's position between messages, and thus on the sender's dynamics. An approach to varying sending rate based on dynamics is described in [33].
- If a vehicle is running a standardized adaptive message rate control algorithm to control congestion [34], [35], it would be desirable to allow a wider range of rates than if the vehicle is permitted to choose any allowed rate at any time.

As noted in the J2735 discussion, Part I is included in every BSM, but Part II elements are optional in SAE J2735. The elements in the `VehicleSafetyExtension` (Table 9) are considered necessary for inclusion on either an event basis or at a rate below the nominal 10 Hz BSM rate. SAE J2945.1 will separately address the minimum and maximum constraints for including these elements in BSMs.

BSM Transmit Power: This is somewhat analogous to message rate in that it affects channel loading (and potential congestion) and application performance. The SAE J2945.1 standard will provide constraints for transmit power, ideally in a way that accounts for the operating environment (e.g., vehicle speed, relevance of application requirements as a function of road type, etc.)

Sensor Accuracy: Most of the data in a BSM represents the output of a sensor, e.g., speed, acceleration, three-dimensional position, time. The receiver uses this to model the sender's relative position. Constraints on sensor data accuracy are needed in order to enable the receiver to provide timely warnings with a sufficiently high probability while avoiding false negatives. This is again complicated by the fact that application performance is difficult to translate to individual sensors. A particularly challenging issue is the absolute accuracy of GPS position data, given that GPS errors may be expected to be correlated near a given location and that relative position is more critical than absolute position for collision prevention. It may also be necessary to specify requirements related to the maximum latency between the capture of sensor data and the transmission of a BSM that conveys that data.

Some additional requirements that may be included in later versions of J2945.1 include Security and Privacy, Certificate Management, BSM PSID assignments, BSM SSP definition, QoS (relative message priority and EDCA parameter selection), and Adaptive Congestion Control. As new interoperability requirements are discovered in other parts of the protocol stack, the J2945.1 standard will be a candidate document for addressing them.

Another open issue is whether J2945.1 will represent a single set of constraints for all BSM-sending devices, or whether it will recognize classes of devices some of which have greater capability (e.g., because they are factory installed and have greater sensor availability) than others. The U.S. DOT and automakers are investigating at least three classes of device in the Safety Pilot Model Deployment [39]: fully integrated, aftermarket, and "Here I Am" (HIA). The HIA devices have no access to internal vehicle state, and derive their safety message contents primarily from GPS signals; they do not have receivers or provide driver warnings. The aftermarket devices will both transmit and receive BSMs, and will have a variety of sensor data capabilities. The aftermarket and HIA devices are expected to accelerate the penetration of DSRC equipment compared to a new-car-only deployment approach, and thus to accelerate the benefits of DSRC.

One final note is that some aspects of V2V safety will likely not be standardized. In particular, automobile manufacturers will define and implement proprietary versions of the safety applications, including the threat assessment algorithms and the important driver-vehicle interface.

VII. CONCLUSION

DSRC technology in the 5.9 GHz band has the potential to support many different types of applications, including collision avoidance applications that can save tens of thousands of lives and billions of dollars in the United States. This technology depends fundamentally on standards-based interoperability. The core standards expected to be used in the U.S. are reaching a critical level of maturity. Several have been published within the past 12 months: IEEE 802.11p, IEEE 1609.3, and IEEE 1609.4 (see Fig. 2). The IEEE 1609.2 Security Services standard is likely to be published near the end of 2011. A preliminary version of SAE J2945.1 Minimum Performance Requirements may also be published in 2011, with more substantial revisions expected soon after. Recent testing of basic interoperability among independent DSRC implementations is encouraging [14].

NHTSA plans to decide in 2013 whether to use regulations to require or encourage deployment of DSRC safety systems in new vehicles in the United States [8]. That decision will be based on a variety of factors, including an objective benefits assessment. While the status of standards today is healthy, a number of challenges remain. Some of the most critical are as follows.

- Development of SAE J2945.1 Vehicle BSM Communication Minimum Performance Requirements,

to specify BSM rate and power constraints, as well as position and sensor accuracy requirements.

- Development of a "communications security" framework to supplement the algorithms and frame formats specified in IEEE 1609.2. This framework will define aspects of the public key infrastructure (PKI) over which vehicles will be provided security certificates and certificate revocation notices, as well as a means by which the security infrastructure can be notified if a vehicle detects a misbehaving device. Some aspects of this framework may be documented in IEEE 1609.2, while others will be captured in government regulations. The V2V-Communications Security project is investigating these issues and proposing solutions [36]. The proposals will be tested in the V2V-Interoperability project [13].
- Development of a Channel Congestion Control algorithm, especially for the safety channel. While DSRC congestion will not be a problem in the early stages of deployment, the long life cycle of vehicles suggests that even the initial in-vehicle devices have a capability to react to channel congestion by mitigating their own contribution. This capability can then be refined with experience. Congestion control is likely to be standardized eventually, perhaps in SAE J2945.1.
- Policy and Business issues, many of which will not require technical standardization but which nevertheless are important for deployment, including: enforcement of regulations and standards, certification of devices, clarification of use of Channel 172 (see Section V-A), field testing and analysis of field data to prove benefits, a decision regarding the potential subsidy of equipment to promote fast market penetration, and harmonization of standards between the United States and other regions of the world. ■

REFERENCES

[1] *Vehicle Safety Communications Project—Final Report*, U.S. Dept. Trans., Nat. Highway Traffic Safety Admin., Rep. DOT HS 810 591, Apr. 2006.

[2] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—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 Std. 802.11p, Jul. 2010.

[3] *Draft Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE P1609.2/D9.0, May 2011.

[4] *IEEE Standard for Wireless Access in Vehicular Environments—Networking Services*, IEEE Std. 1609.3-2010, Dec. 2010.

[5] *IEEE Standard for Wireless Access in Vehicular Environments—Multi-Channel Operation*, IEEE Std. 1609.4-2010, Dec. 2010.

[6] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE Std. J2735, SAE Int., DSRC Committee, Nov. 2009.

[7] *Draft DSRC Message Communication Minimum Performance Requirements—Basic Safety Message for Vehicle Safety Applications*, SAE Draft Std. J2945.1 Revision 2.2, SAE Int., DSRC Committee, Apr. 2011.

[8] R. Resendes, "Vehicle-to-vehicle and safety pilot," in *Proc. U.S. Department of Transportation Safety Workshop*, Jul. 20, 2010. [Online]. Available: http://www.its.dot.gov/presentations/Safety_workshop2010/Vehicle-toVehicle%20and%20Safety%20Pilot%20–%20R%20Resendes.pdf

[9] *Vehicle Safety Communications—Applications VSC-A, First Annual Report*, U.S. Dept. Trans., Nat. Highway Traffic Safety Admin., Rep. DOT HS 811 073. [Online]. Available: http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2008/811073.pdf

[10] *Intelligent Transportation Services Report and Order*, U.S. Federal Communications Commission, R&O FCC 99-305, Oct. 21, 1998.

[11] *Dedicated Short Range Communications Report and Order*, U.S. Federal Communications Commission, R&O FCC 03-324, Dec. 17, 2003.

[12] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850–5.925 GHz band (5.9 GHz band)*, U.S. Federal Communications Commission MO&O, FCC 06-110, adopted Jul. 20, 2006.

[13] *Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability), Project Order 0004, Technical Proposal Statement of Work*, U.S. Dept. Trans., Nat. Highway Traffic Safety Admin., Cooperative Agreement DTNH22-05-01277, Dec. 2009.

[14] *Draft First Annual Report: Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability); Vehicle Safety Communications 3 (VSC3) Consortium*, submitted to U.S. Dept. Trans., Jan. 2011.

[15] H. Hartenstein and K. Laberteaux, Eds., *VANET: Vehicular Applications and Inter-Networking Technologies*. Wiley, 2010.

[16] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11-2007, Jun. 2007.

[17] *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 E2213-03, ASTM International, Aug. 2003.

[18] *Code of Federal Regulations, Title 47, Part 90, Private Land Mobile Radio Services*, U.S. FCC, CFR 47 Part 90. [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx_08/47cfr90_08.html

[19] *Code of Federal Regulations, Title 47, Part 95, Personal Radio Services*, U.S. FCC, CFR 47 Part 95. [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx_08/47cfr95_08.html

[20] D. Jiang, Q. Chen, and L. Delgrossi, "Optimal data rate selection for vehicle safety communications," in *Proc. 5th ACM Int. Workshop on Veh. Inter-NETworking (VANET 2008)*, San Francisco, Sep. 2008.

[21] F. Bai, D. Stancil, and H. Krishnan, "Toward understanding characteristics of Dedicated Short Range Communications (DSRC) from a perspective of vehicular network engineers," in *Proc. Sixteenth Annu. Int. Conf. Mobile Comput. Networking (MobiCom)*, Chicago, IL, Sep. 2010.

[22] V. Rai, F. Bai, J. Kenney, and K. Laberteaux. (2007, Jul.). *Cross-Channel Interference Test Results: A Report From the VSC-A Project*, IEEE 802.11 WG submission 11-07-2133-00-000p. [Online]. Available: https://mentor.ieee.org/802.11/dcn/07/11-07-2133-00-000p-cross-channel-interference-test-results-a-report-from-the-vsc-a-project.ppt

[23] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment—Fast Initial Link Setup*, IEEE P802.11ai, Dec. 2010, Project Authorization Request (PAR).

[24] J. Hui and M. Devetsikiotis, "A unified model for the performance analysis of IEEE 802.11e EDCA," *IEEE Trans. Commun.*, vol. 53, no. 9, pp. 1498–1510, Sep. 2005.

[25] A. Banchs, A. Azcorra, C. Garcia, and R. Cuevas, "Applications and challenges of the 802.11e EDCA mechanism: An experimental study," *IEEE Network*, vol. 19, no. 4, pp. 52–58, Jul.–Aug. 2005.

[26] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements; Part 2: Logical Link Control*, IEEE Std. 802.2, May 1998, 1998 Edition (R2003), Also adopted by the ISO/IEC and redesignated as ISO/IEC 8802-2:1998.

[27] *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, IEEE Std. 802-2001, Feb. 2002.

[28] J. Postel and J. Reynolds, *A Standard for the Transmission of IP Datagrams Over*

IEEE 802 Networks, Internet Engineering Task Force RFC 1042, Feb. 1988.

[29] *Draft Standard for Wireless Access in Vehicular Environments—Architecture*, IEEE P1609.0/D0.9, Apr. 2010.

[30] *Draft Standard for Wireless Access in Vehicular Environments—Provider Service Identifier (PSID) Allocations*, IEEE P1609.12/D0.3, May 2011.

[31] K. Hong, J. Kenney, V. Rai, and K. Laberteaux, "Evaluation of multi-channel schemes for vehicular safety communications," in *Proc. 3rd IEEE Int. Symp. Wireless Veh. Commun. (WiVEC 2010)*, Taipei, May 2010.

[32] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: Fair Transmit Power Control for safety-critical information," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, Sep. 2009.

[33] C. Huang, H. Krishnan, R. Sengupta, and Y. Fallah, "Implementation and evaluation of scalable vehicle-to-vehicle transmission control protocol," in *Proc. Second IEEE Veh. Networking Conf. (VNC 2010)*, Dec. 2010.

[34] D. Jiang and T. Tielert, "PULSAR: A rate adaptation based congestion control protocol for vehicle safety communication," submitted to *8th ACM Int. Workshop on Veh. Inter-NETworking (VANET 2011)*, Las Vegas, Sep. 2011.

[35] A. Weinfield, J. Kenney, and G. Bansal, "An adaptive DSRC message transmission interval control algorithm," accepted for *Proc. ITS World Congr. 2011*, Oct. 2011.

[36] *V2V-Communications Security Project Technical Proposal Statement of Work*, U.S. Dept. Trans., Cooperative Agreement DTFH61-01-x-00014, Dec. 2009.

[37] *Security in VSC-A, Submission to IEEE 1609 WG from Vehicle Safety Communications 2 (VSC2) Consortium*, Jun. 2009. [Online]. Available: http://vii.path.berkeley.edu/1609_wave/jun09/presentations/VSC/VSCA-1609_ecdsa_privacy_final_6_15_2009.ppt

[38] *Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, ITU-T Recommendation X.690, Nov. 2008.

[39] *Connected Vehicle Safety Pilot Frequently Asked Questions*, U.S. DOT Res. Innovative Technol. Admin. [Online]. Available: http://www.its.dot.gov/research/safety_pilot_faq.htm

ABOUT THE AUTHOR

John B. Kenney (Member, IEEE) received the B.S. (high honors) and Ph.D. degrees in electrical engineering from the University of Notre Dame, Notre Dame IN, in 1982 and 1989, respectively, and the M.S. degree (NSF Graduate Fellow) in electrical engineering from Stanford University, Stanford CA, in 1983.

He joined the Tellabs Research Center in 1983, where he was a Senior Research Engineer until 2007. He was Adjunct Assistant Professor of Electrical Engineering at Notre Dame from 1989 to 2010. From 2007 to 2010, he was a Consultant for Toyota Motor Engineering & Manufacturing North America (TEMA) and Toyota InfoTechnology Center, USA. He joined Toyota InfoTechnology Center USA in 2010 (Mountain View, CA), where he is Senior Research Manager in the Network Group. He represents Toyota in cooperative projects between the Vehicle Safety Communication (VSC) consortium and the U.S. Department of Transportation: VSC-Applications (2007–2009), VSC-Interoperability (2010–2012), and VSC-Communications Security (2010-12). He also represents Toyota in DSRC-related standards groups: IEEE 802.11 Working Group (WG), IEEE 1609 DSRC WG, SAE DSRC Technical Committee, and ETSI TC ITS. He is the author of the "Standards and Regulations" chapter in *VANET: Vehicular Applications and Inter-Networking Technologies* (Hartenstein and Laberteaux, Eds., Wiley, 2010). He is Co-General Chair of the Eighth ACM VANET Workshop (part of MobiCom 2011). His current research is in wireless congestion control and performance of vehicular networks. His prior research interests include adaptive systems, high speed packet switch architectures, and packet network quality of service.

Dr. Kenney was recognized by the IEEE Standards Association for his contributions to IEEE Standards 802.11p-2010, 1609.3-2010, and 1609.4-2010.