WAVE: A Tutorial

Roberto A. Uzcátegui, Universidad Nacional Experimental Politécnica "Antonio José de Sucre"
Guillermo Acosta-Marum, Georgia Institute of Technology

ABSTRACT

Intelligent transportation systems have been under development since at least the early 1990s. The rationale behind the concept is to automate the interactions among vehicles and infrastructure to achieve high levels of security, comfort, and efficiency. Communications, in general, and networking, in particular, have been essential elements in the evolution of these systems. The IEEE has developed a system architecture known as WAVE to provide wireless access in vehicular environments. This article gives an overview of the associated standards. The presentation loosely follows the order of the layers of the open systems interconnection model.

INTRODUCTION

In the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA), the United States Congress mandated the creation of a program called Intelligent Vehicle Highway Systems (IVHS), whose main goals were to increase safety, ameliorate congestion, reduce pollution, and conserve fossil fuels while vehicles use the nation's surface transportation infrastructure. Responsibility for the program was assigned to the U. S. Department of Transportation (DOT), which sought the advice of the Intelligent Transportation Society of America (ITSA) — a nonprofit organization whose members come from industry and academia, as well as federal, state, and municipal government — to perform the assignment. By 1996, the DOT, the ITSA, and several other interested parties had developed a procedural framework wherein IVHS services (or intelligent transportation system [ITS] services, as they are known today) could be systematically planned, defined, and integrated. Known as the National Intelligent Transportation Systems Architecture (NITSA), this framework has served as a master plan for ITS initiatives for the past 13 years.

From the beginning, the NITSA recognized wireless communications as a cornerstone for the implementation of many ITS services. At the time, some applications, such as automated toll collection, were performed using the spectrum between 902 MHz and 928 MHz. Unfortunately, this band was too small and polluted to enable the envisioned evolution of IVHS communications. Consequently, in 1997, the ITSA petitioned the Federal Communications Commission (FCC) for 75 MHz of bandwidth in the 5.9-GHz band with the specific goal of supporting dedicated short-range communications (DSRC) for ITS. The FCC granted the request in October of 1999. The DSRC-based ITS radio services received 75 MHz of spectrum in the 5.85–5.925 GHz range.

By July 2002, the ITSA was actively lobbying the FCC on matters of licensing, service rules, and possible technologies for the ITS-DSRC band. The ITSA recommended the adoption of a single standard for the physical (PHY) and medium access control (MAC) layers of the architecture and proposed one developed by the American Society for Testing and Materials (ASTM) based on IEEE 802.11 [1] (ASTM's E2213-02 [2]). The FCC officially adopted this recommendation in the 2003–2004 timeframe.

In 2004, an IEEE task group (task group p, or TGp of the IEEE 802.11 working group) assumed the role initiated by the ASTM and started developing an amendment to the 802.11 standard to include vehicular environments. The document is known as IEEE 802.11p [3]. Another IEEE team (working group 1609) undertook the task of developing specifications to cover additional layers in the protocol suite. At the time of this writing, the IEEE 1609 standards set consisted of four documents: IEEE 1609.1 [4], IEEE 1609.2 [5], IEEE 1609.3 [6], and IEEE 1609.4 [7].

Collectively, IEEE 802.11p and IEEE 1609.x are called wireless access in vehicular environments (WAVE) standards because their goal, as a whole, is to facilitate the provision of wireless access in vehicular environments. The conceptual design they portray is called WAVE architecture in this article, and the systems that implement it are referred to as WAVE systems.

The objective of this article is to give an overview of the IEEE WAVE standards.

To the extent that the model applies, the presentation of the material loosely follows the order of the layers in the open systems interconnection (OSI) model from the bottom up. In this article, we consider only those OSI layers that are covered by a WAVE standard. This content arrangement does not correspond to a monotonic progression of the numerical designations given by the IEEE to the related documents, but it does convey a general sense of the logical flow of information inside a WAVE system within the confines of a sequentially written composition.

We organized the article as follows. First, we

0163-6804/09/$25.00 © 2009 IEEE

give a general description of the architecture of a WAVE system. Then, we follow it with a brief discussion of the PHY layer and the MAC sublayer (as addressed in IEEE 802.11p), the multichannel coordination mechanism used in WAVE (that sits atop the MAC sublayer, as specified in IEEE 1609.4), and the WAVE services at the network- and transport-layer levels (as described in IEEE 1609.3). In the next two sections, we discuss entities that have no counterpart in the OSI model: the resource manager (IEEE 1609.1) and the security services (IEEE 1609.2). We finalize the article with some comments about the state of the art in research and development in the field.

WAVE System Architecture Overview

Imagine the following three scenarios:

- An emergency-response vehicle, such as a fire department truck, rapidly approaches an intersection with a four-way stop. As it nears the intersection, a radio device on the truck sends an electronic message to similar devices located in all nearby vehicles to preempt the crossroad. The onboard computer of any of the receiving vehicles first alerts the driver about the emergency, and then, if necessary, autonomously slows down the car to avoid a collision.
- As they drive by the welcome center of the town that a family is visiting for the weekend, a wireless transceiver in their minivan receives an announcement from an access point in the building, advertising free global positioning system (GPS) maps updated with information about the tourist attractions for that particular weekend. After receiving confirmation that the passengers are interested in this particular information, the transceiver downloads the maps.
- On the way to work and using the speech user interface of her car, the doctor connects to her Web-based calendar application and listens to the list of appointments she has that day.

The first scenario is an example of a public-safety application that implies vehicle-to-vehicle (V2V) communications. The second and third ones are instances of private applications that entail a vehicle-to-infrastructure (V2I) information exchange. The third one, in particular, involves traditional Internet access. These are but three of the potential uses of the WAVE technology that is the focus of this article (see Table 1 for more uses). We use these three scenarios to provide concrete illustrations of the concepts discussed in the rest of this section.

Components of a WAVE System

A WAVE system consists of entities called units (Fig. 1). Roadside units (RSUs) usually are installed in light poles, traffic lights, road signs, and so on; they might change location (for instance, when transported to a construction site) but cannot work while in transit. Onboard units (OBUs) are mounted in vehicles and can function while moving.

User services bundles	User services
Travel and traffic management	Pre-trip travel information En route driver information Route guidance Ride matching and reservation Traveler's services information Traffic control Incident management Travel demand management Emissions testing and mitigation Highway rail intersection
Public transportation management	Public transportation management En route transit information Personalized public transit Public travel security
Electronic payment	Electronic payment services
Commercial vehicle operations	Commercial vehicle electronic clearance Automated roadside safety inspection Onboard safety and security monitoring Commercial vehicle administrative processes Hazardous materials security and incident response Freight mobility
Emergency management	Emergency notification and personal security Emergency vehicle management Disaster response and evacuation
Advanced vehicle safety systems	Longitudinal collision avoidance Lateral collision avoidance Intersection collision avoidance Vision enhancement for crash avoidance Safety readiness Pre-crash restraint deployment Automated vehicle operation
Information management	Archived data
Maintenance and construction management	Maintenance and construction operations

Table 1. *User services considered in the version 6.1 of the NITSA.*

By default, WAVE units operate independently, exchanging information over a fixed radio channel known as the control channel (CCH). However, they also can organize themselves in small networks called WAVE basic service sets (WBSSs), which are similar in nature to the service sets defined in IEEE 802.11 [1]. WBSSs can consist of OBUs only or a mix of OBUs and RSUs (Fig. 1). All the members of a particular WBSS exchange information through one of several radio channels known as service channels (SCHs). Through the appropriate portals, a WBSS can connect to a wide-area network (Fig. 1).

Communication Protocols

The WAVE architecture supports two protocol stacks, as shown in Fig. 2. In the terminology of the OSI model, both stacks use the same physical and data-link layers, and they differ from each other in the network and transport layers. The WAVE standards do not specify session,

presentation, or application layers. However, they do introduce two elements that do not fit easily within the boundaries of the OSI model: the resource manager and the security services blocks (Fig. 2).

The two stacks supported by WAVE are traditional Internet Protocol version six (IPv6) and a proprietary one known as WAVE Short-Message Protocol (WSMP). The reason for having two protocol stacks is to accommodate high-priority, time-sensitive communications, as well as more traditional and less demanding exchanges, such as Transmission Control Protocol/User Datagram Protocol (TCP/UDP) transactions. An application like the crossroad pre-emption mentioned before has scarce requirements in terms of datagram length or complexity but very strict ones in terms of latency and probability of error. WSMP enables the application to send short messages and directly control certain parameters of the radio resource to maximize the probability that all the implicated parties will receive the messages in time. However, WSMP is not enough to support typical Internet applications, and these are required to attract private investment that would help spread, and ultimately reduce, the cost of implementing the systems; hence the inclusion of IPv6.

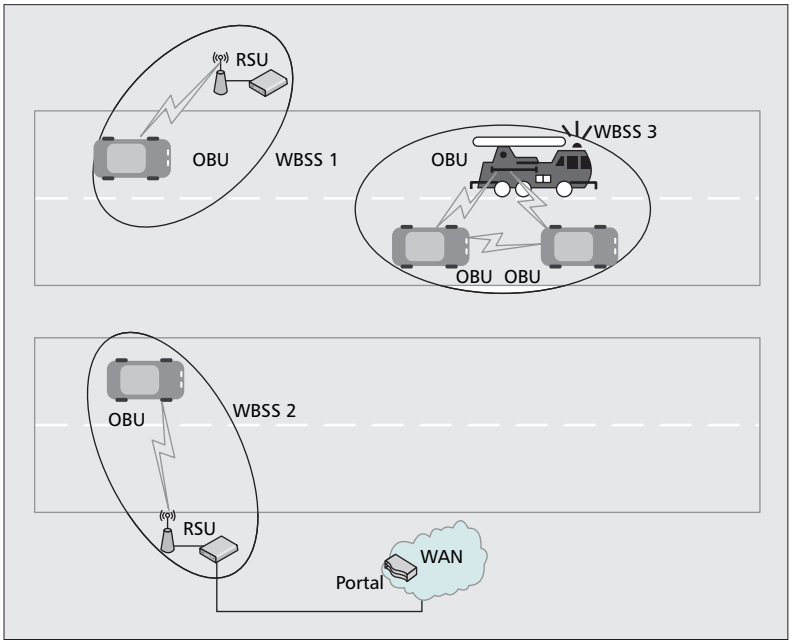

Figure 1. *Illustration of a WAVE system showing the typical locations of the OBUs and RSUs, the general makeup of the WBSSs, and the way a WBSS can connect to a WAN through a portal.*

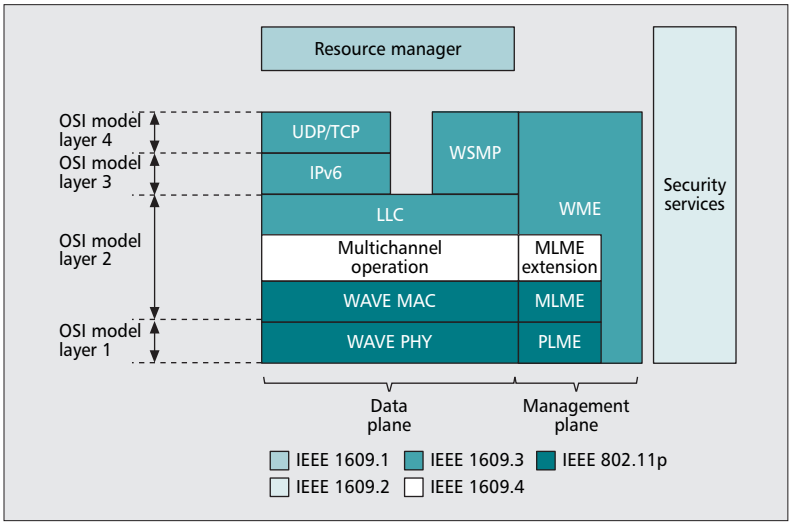

Figure 2. *WAVE communication stack indicating the standard that covers each set of layers. The blocks marked resource manager and security services do not fit easily within the layered structure of the OSI model.*

For reasons that will be explained in the next section, the WAVE architecture is based on the IEEE 802.11 standard [1], which specifies layer one and part of layer two of the protocol stack (Fig. 2). Given the differences between the operating environment of an 802.11 wireless local area network (LAN) and a vehicular environment such as any of the ones described at the beginning of this section, an amendment to the standard was required, which is known as IEEE 802.11p. This norm specifies not only the data transmission portion of the protocols but also the management functions associated with the corresponding layer (the physical layer management entity [PLME] and the MAC layer management entity [MLME] blocks in Fig. 2).

Unlike traditional wireless LAN stations, WAVE units might be required to divide their time between the CCH and the SCHs. Therefore, the WAVE protocol stack includes a sublayer at the level of the OSI layer two, dedicated to controlling this multichannel operation. This sublayer (including the associated management functions) is specified in IEEE 1609.4.

The remaining part of OSI layer two (the logical link control [LLC]) follows the IEEE 802.2 standard, as described in a later section.

At the level of the OSI layers three and four, IEEE 1609.3 specifies the aforementioned WSMP and explains how to incorporate traditional IPv6, UDP, and TCP in the systems. That document also defines a set of management functions (labeled WAVE management entity [WME] in Fig. 2) that must be used to provide networking services.

The remaining two blocks in Fig. 2 (resource manager and security services) do not fit easily in the layered structure of the OSI model. They are covered by IEEE 1609.1 and IEEE 1609.2, respectively.

In subsequent sections of this article, we review the WAVE protocols specified in Table 2, in the order given in the table. Protocols that appear in Fig. 2 but are not specific to WAVE (such as LLC, IPv6, TCP, and UDP) are mentioned without details.

PHY and MAC Layers

The WAVE PHY and MAC layers are based on IEEE 802.11a, and their corresponding standard is IEEE 802.11p [3]. There are several advantages to basing the WAVE on 802.11 because it is a stable standard supported by experts in wireless technology. A stable standard is required to guarantee interoperability between vehicles made by different manufacturers and the roadside infrastructure in different geographic loca-

Protocols	Standard document	Purpose of the standard	OSI model layer numbers
WAVE PHY and MAC	IEEE 802.11p	Specifies the PHY and MAC functions required of an IEEE 802.11 device to work in the rapidly varying vehicular environment	1 and 2
Multichannel operation	IEEE 1601.4	Provides enhancements to the IEEE 802.11p MAC to support multichannel operation	2
WAVE networking services	IEEE 1609.3	Provides addressing and routing services within a WAVE system	2, 3, and 4
WAVE resource manager	IEEE 1609.1	Describes an application that allows the interaction of OBUs with limited computing resources and complex processes running outside the OBUs in order to give the impression that the processes are running in the OBUs	N/A
WAVE security services	IEEE 1609.2	Covers the format of secure messages and their processing	N/A

Table 2. *A list of the protocols that compose the WAVE communications stack, in the order in which they are presented in this article, with the designation of the standard that covers each one of them, a brief description of the purpose of the norm, and the corresponding layers in the OSI model.*

tions. It also guarantees that the standard will be maintained in concert with other ongoing developments in the 802.11 family, which enhances synergies in chipset design to help ensure economies of scale. However, we require a different version of the 802.11 because we must support:

- Longer ranges of operation (up to 1000 m)
- The high speed of vehicles
- Extreme multipath environments
- Multiple overlapping ad hoc networks with extremely high quality of service (QoS)
- The nature of the applications
- A special type of beacon frame

The main requirements, characteristics, changes, and/or improvements for 802.11p are as follows [8]:

- Communications in a highly mobile environment
- 10-MHz channels; one-half the data rates of 802.11
- Control channel and six service channels
- Unique ad hoc mode
- Random MAC address
- High accuracy for the received signal strength indication (RSSI)
- 16 QAM used in the high-speed mobile environment
- Spectral mask modification
- Option for a more severe operating environment
- Priority control
- Power control

We have noted several times that the high mobility and extreme multipath environments present unique challenges in a WAVE system. The main reason for unique challenges is that the wideband V2V or V2I channel is "doubly selective." This means that its frequency response varies significantly over the signal bandwidth, and its time fluctuations happen in the course of a symbol period. Because WAVE uses orthogonal frequency division multiplexing (OFDM), these variations present significant design challenges in the channel-estimation and frequency-offset-detection systems of the receiver. In [9, 10], we can find measurement and modeling studies showing the uniqueness of these high mobility channels. In [11], we find a detailed description of the latest draft of this standard.

Multichannel Operation

A WAVE device must be able to accommodate an architecture that supports a control channel and multiple-service channels. The channel coordination is an enhancement to IEEE 802.11 MAC and interacts with IEEE 802.2 LLC and IEEE 802.11 PHY. In the standard [7], we find the services that are used to manage channel coordination and to support MAC service data unit (MSDU) delivery. There are four services provided in the standard. The channel routing service controls the routing of data packets from the LLC to the designated channel within channel coordination operations in the MAC layer. The user priority service is used to contend for medium access using enhanced distributed channel access (EDCA) functionality derived from IEEE 802.11e [12]. The channel coordination service coordinates the channel intervals according to the channel synchronization operations of the MAC layer so that data packets from the MAC are transmitted on the proper radio frequency (RF) channel. Finally, the MSDU data transfer service consists of three services: control channel data transfer, service channel data transfer, and data transfer services. The design of these three services is concerned mostly with giving a higher priority and direct access to the WSMP, for which the MAC must be able to identify the type of data packet (WSMP or IP) indicated by its EtherType in accordance with the IEEE 802.2 header.

Functional Description

There are two types of information exchanges in the WAVE medium: management frames and data frames. The primary management frame is the WAVE announcement defined in [7]. WAVE announcement frames are permitted to

In the data plane, the WAVE architecture supports two protocol stacks: traditional IPv6 and the unique WSMP. Both of them operate atop a single LLC layer. This dual configuration serves to accommodate high-priority, time-sensitive communications, as well as less demanding, transactional exchanges.

be transmitted only in the CCH. Other IEEE 802.11 management frames may be utilized in the SCH. For data exchanges, data frames containing WAVE short messages (WSMs) can be exchanged among devices on both the CCH and the SCH; however, IP data frames are permitted only in an SCH, and SCH exchanges require the corresponding devices to be members of a WBSS. For control channel priority, the EDCA parameter set is optimized for WSMP data transfer. A predetermined EDCA parameter set must be used for all WAVE devices when operating in the CCH. For service channel priority, the EDCA parameter received within the WAVE announcement frame of the provider must be used. Channel coordination utilizes a synchronized scheme based on coordinated universal time (UTC). This approach assures that all WAVE devices are monitoring the CCH during a common time interval (CCH interval). When a WAVE device joins a WBSS, this channel synchronization approach also assures that the members of that WBSS are utilizing the corresponding SCH during a common time interval (SCH interval). The sum of these two intervals comprises the sync interval.

Networking Services

In the IEEE 1609.3 standard [6], we find the specification of the functions associated with the LLC, network, and transport layers of the OSI model, and the standard calls them WAVE networking services (Fig. 2).

We can functionally divide the WAVE networking services into two sets:

- Data-plane services, whose function is to carry traffic
- Management-plane services, whose functions are system configuration and maintenance

Data-Plane Services

In the data plane, the WAVE architecture supports two protocol stacks: traditional IPv6 and the unique WSMP. Both of them operate atop a single LLC layer. This dual configuration serves to accommodate high-priority, time-sensitive communications (through WSMP), as well as less demanding, transactional exchanges (through UDP/TCP/IP).

At the LLC layer, WAVE devices must implement the type 1 operation specified in [13], the Sub-Network Access Protocol (SNAP) specified in [14], and the standard for transmission of IP datagrams over IEEE 802 networks specified in RFC 1042.

WAVE devices must implement IPv6, as specified in RFC 2460, UDP as defined in RFC 768, and TCP as per RFC 793. Manufacturers are free to implement any other Internet Engineering Task Force (IETF) recommendation they wish, as long as it does not hinder interoperability with other WAVE devices.

Implementations of WSMP must support a short-message-forwarding function consisting of two primitives. Upon receipt of the primitive `WSM-WaveShortMessage.request` from a local (residing on the same device) or a remote (residing outside the WAVE device) application, the WSMP checks that the length of the WSM is valid (or not) and passes it to the LLC layer for delivery over the radio link (or not). Upon receipt of an indication from the LLC of a received WSM, the WSMP passes it to the destination application (local or remote) by way of a second primitive `WSM-WaveShortMessage.indication`.

Management-Plane Services

Management-plane services specified in IEEE 1609.3 are collectively known as the WME and include:

- Application registration
- WBSS management
- Channel usage monitoring
- IPv6 configuration
- Received channel power indicator (RCPI) monitoring
- Management information base (MIB) maintenance

Application Registration — All the applications that expect to use the WAVE networking services first must register with the WME. Each application registers with a unique provider service identifier (PSID). Registration information is recorded in three tables, namely:

- The `ProviderServiceInfo` table, which contains information about the applications that provide a service.
- The `UserServiceInfo` table, which contains information about the services that are of interest to applications residing in the local unit.
- The `ApplicationStatus` table, which contains, among other things, the IP addresses and ports of the applications for notification purposes when they reside outside the local unit.

WBSS Management — The WME is in charge of initiating a WBSS on behalf of any application that provides a service. This may require one or more of the following operations:

- Link establishment
- Addition or removal of applications from dynamic WBSSs
- Inclusion (provider side) and retrieval (user side) of security credentials
- WBSS termination
- Maintenance of the status of each application in the context of a particular WBSS

Channel Usage Monitoring — Although the standard does not specify how to do it, it mandates that the WME tracks the SCHs usage patterns so that it can choose a channel that is less likely to be congested when it must establish a WBSS.

IPv6 Configuration — This service is for managing the link local, global, and multicast IPv6 addresses of the unit as indicated in the corresponding IETF RFCs.

RCPI Monitoring — Any application can query a remote device about the strength of the received signal. The WME sends the corresponding request on behalf of the querying

application. The MLME, not the WME, of the remote unit answers this request.

MIB Maintenance — The WME maintains a MIB that contains system-related and application-related information. The system-related information includes network information (router, gateway, and Domain Name Service [DNS] data, among other types), address information (such as local MAC addresses), and other values, such as registration port, forwarding port, WSM maximum length, and so on. The application-related information includes the `ProviderServiceInfo`, `UserServiceInfo`, and `ApplicationStatus` tables previously mentioned, as well as channel information, like channel number, data rate, and transmit power level.

Resource Manager

In the IEEE 1609.1 standard [4], we find the definition of a WAVE application called the resource manager (RM), whose purpose is to give certain processes access to the system communication resources.

The RM is located in either an RSU or an OBU. It receives requests from applications that run in computers that are located remotely from its host unit. These applications are called resource management applications (RMAs). The goal of the RMAs is to use the resources of one or more OBUs. The RM acts as a broker that relays commands and responses between the RMAs to the appropriate OBUs. A software entity called the resource command processor (RCP) that resides in the OBU executes the commands sent by the RM on behalf of the RMAs.

A summary of the operation of the RM layer is as follows. Each RMA registers with the RM with which it interacts and specifies, among other things, the list of resources that it must use. The RM registers with the WME of its host unit as a provider. When the RMA becomes active, the provider's WME initiates a WBSS and announces, along with other pertinent information, that there is an RMA wishing to use the specified set of resources. The WME of an OBU receiving the announcement notifies the RCP about the RMA and its list of desired resources. If there is a match within the set of resources it administers, the RCP asks the WME of its unit to join the WBSS and registers as a user. Once this is done, the RCP responds directly to the RM. The RM then notifies the RMA that it is in the presence of an RCP that has some or all of the resources that the application requires. An exchange between the RMA and the RCP begins, by way of the RM. This takes place until the RMA decides to terminate the session, issuing the appropriate commands to the RCP, which acknowledges the termination.

The resources that the RMAs may control include, but are not limited to, read/write memory; user interfaces that are included as part of the OBU; specialized interfaces to other onboard equipment; and optional vehicle-security devices connected to the OBU. All these resources are mapped into the memory space of the unit. The commands issued by the RM allow the RMAs to read, write, reserve, and release portions of this memory space.

The RM concept reduces the complexity of the OBUs by freeing them from the requirement of executing applications onboard the vehicle. This was considered a simple way of reducing their production costs, increasing their reliability, and facilitating the interoperability of units produced by different manufacturers.

Security Services

WAVE applications face unique safety constraints because of their wide range of operation. For example, safety applications are time critical; therefore, the processing and bandwidth overhead must be kept to a minimum. For other applications, the potential audience may consist of all vehicles on the road in North America; therefore, the mechanism used to authenticate messages must be as flexible and scalable as possible. In each case, we must protect messages from eavesdropping, spoofing, alterations, and replay. We also must provide owners the right to privacy to avoid leaking of personal, identifying, or linkable information to unauthorized parties. In the IEEE 1609.2 standard [5], we find the security services for the WAVE networking stack and for applications that are intended to run over the stack. Mechanisms are provided to authenticate WAVE management messages, to authenticate messages that do not require anonymity, and to encrypt messages to a known recipient. Services include encryption using another party's public key and non-anonymous authentication. *Confidentiality* (*encrypting* a message for a specific recipient) avoids the interception or altering of a message. *Authenticity* (confirmation of origin of the message) and *integrity* (confirmation that the message has not been altered in transit) avoid tricking a recipient into accepting incorrect message contents. In WAVE, *anonymity* for end users is also a requirement. Cryptographic mechanisms provide most of these security requirements, and their three main families are *secret-key* or *symmetric* algorithms, *public-key* or *asymmetric* algorithms, and *hash functions*.

Symmetric Algorithms

When two entities (traditionally called Alice and Bob) want to communicate, they both use secret data known as a *key*. Alice uses the key to *encrypt* her message; Bob has the same key and can decrypt it. To provide authenticity and integrity, Alice uses the key to generate a cryptographic checksum or message integrity check (MIC), and the MIC only passes the check if Bob uses the correct key. A message can be encrypted-only, authenticated-only, or both. The standard uses the advanced encryption standard — counter with cipher block chaining (CBC) MIC (AES-CCM) mechanism.

Asymmetric Algorithms

We use a *keypair*, known as the *public key* and the *private key*, which are mathematically related so that it is extremely difficult to determine the private key, given only the public key. For an

WAVE applications face unique safety constraints because of their wide range of operation. For example, safety applications are time critical; therefore, the processing and bandwidth overhead must be kept to a minimum.

The goals of safety, comfort, and energy efficiency that motivated legislators to call for the creation of an intelligent ground-transportation system in 1991 are as valid today as they were then, if not more so.

encrypted message to Bob, Alice uses Bob's public encryption key. Bob, who knows the corresponding private decryption key, is the only one who can decrypt it. For an authenticated message to Bob, Alice uses her own private signing key. A cryptographic checksum generated by a private key is known as a digital signature. Bob uses Alice's public verification key to prove that it is her message. Digital signatures are particularly useful for securing communications with parties that have not been encountered previously, such as when broadcasting to a dynamically changing population.

Hash Functions

A cryptographically secure hash function maps an arbitrary-length input into a fixed-length output (the hash value), such that it is computationally infeasible to find an input that maps to a specific hash value and two inputs that map to the same hash value. The standard makes use of the Secure Hash Algorithm (SHA)-1 hash function, defined in Federal Information Processing Standard (FIPS) 180-1.

Anonymity

Broadcast transmissions from a vehicle operated by a private citizen should not leak information that can be used to identify that vehicle to unauthorized recipients. Public safety vehicles do not generally require anonymity. A vehicle can use broadcast or transactional applications. In both cases, the use of these applications should not compromise anonymity. Additionally, the headers in a transmitted packet might reveal information about the sender (e.g., a fixed source MAC address). A truly anonymous system must remove this compromising information. The current standard is focused on protecting message payloads and does not provide techniques for making the message headers anonymous. In addition, mechanisms for providing anonymous authenticated broadcast messages are not given.

Concluding Remarks

This article presented a tutorial overview of the IEEE standards for WAVE, namely, IEEE 802.11p, IEEE 1609.1, IEEE 1609.2, IEEE 1609.3, and IEEE 1609.4. We presented the material from the perspective of the OSI model, highlighting both the common points and the divergences between the two systems.

The WAVE architecture is built on the ubiquitous IEEE 802.11 standard, which gives WAVE the backing of a sizeable community of wireless experts and enough market momentum to make possible the production of complying devices without having to recover considerable sunk costs. Basing WAVE on IEEE 802.11 implies that many design choices already were made when the standardization process started, but the WAVE environment and applications are sometimes so different from those of traditional wireless LANs that changes and adaptations were inevitable. This article highlighted many of them and gave justifications for the less obvious.

All of the standards reviewed in this article are near final approval. This does not mean, however, that the field is closed to new research and development contributions. Submissions on data dissemination, security, applications, testbeds, channel modeling, MAC protocols, and many other subjects are sent in significant numbers to conferences and symposia on WAVE (e.g., the International Conference on Wireless Access in Vehicular Environments [WAVE] or the IEEE International Symposium on Wireless Vehicular Communications [WiVEC]).

At the time of this writing, experimental ITS networks have been implemented in California, Michigan, New York, and Virginia to display and test applications for collision avoidance, traffic management, emergency response systems, real-time traveler information, and e-commerce [15]. The goals of safety, comfort, and energy efficiency that motivated legislators to call for the creation of an intelligent ground-transportation system in 1991 are as valid today as they were then, if not more so; and in the current global economic climate, ITS may be favorably poised to help create jobs while upgrading the transportation infrastructure. Many stakeholders from industry, government, and academia are betting on this [15], and, as this article shows, WAVE technology has an important role to play in the process.

Acknowledgments

The authors thank Dr. Wai Chen for inviting them to write this tutorial for the series "Topics in Automotive Networking" of the *IEEE Communications Magazine*. They also thank Dr. Weidong Xiang for inviting them to WAVE 2008: The First International Conference on Wireless Access in Vehicular Environments to give the tutorial on which this article is based.

References

[1] IEEE Std 802.11, "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," 2007.
[2] ASTM E 2213, "Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems — 5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2002.
[3] IEEE P802.11p/D3.0, "Draft Amendment to 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 7: Wireless Access in Vehicular Environment," 2007.
[4] IEEE P1609.1, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) — Resource Manager," 2006.
[5] IEEE P1609.2, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) — Security Services for Applications and Management Messages," 2006.
[6] IEEE Std P1609.3, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services," 2007.
[7] IEEE P1609.4, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) — Multi-Channel Operation," 2006.
[8] "Conversion of ASTM E 2213-03 to IEEE 802.11x Format," Doc. IEEE 802.11-04-0363-00-wave, Mar. 2004.
[9] G. Acosta-Marum and M. A. Ingram, "A BER-Based Partitioned Model for a 2.4-GHz Vehicle-to-Vehicle Expressway Channel," *Int'l. J. Wireless Personal Commun.*, July 2006.

[10] G. Acosta-Marum and M. A. Ingram, "Six Time- and Frequency-Selective Empirical Channel Models for Vehicular Wireless LANs," *Proc. 1st IEEE Int'l. Symp. Wireless Vehic. Commun. (WiVec 2007)*, Baltimore, MD, Sept. 30–Oct. 1, 2007.
[11] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for WAVE," *Proc. IEEE Vehic. Tech. Conf.*, Singapore, May 11–14, 2008, pp. 2036–40.
[12] IEEE Std 802.11e/D13.0, "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: Medium Access Control (MAC) Enhancements for Quality of Service (QoS)," draft standard.
[13] IEEE Std 802.2, "IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements — Part 2: Logical Link Control," 1998.
[14] IEEE Std 802, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture," 2001.
[15] ITS America, "Letter to the Speaker of the U.S. House of Representatives, Honorable Nancy Pelosi," Mar. 2009; http://www.itsa.org/itsa/files/pdf/ITSAEconStim-Pelosi.pdf

BIOGRAPHIES

ROBERTO A. UZCÁTEGUI (ruzcategui@unexpo.edu.ve) received a B.Sc. degree in electronic engineering, summa cum laude, from the Universidad Nacional Experimental Politécnica "Antonio José de Sucre" (UNEXPO), Barquisimeto, Venezuela. He received a Master of Science in electronic engineering from the Universidad Simón Bolívar, Caracas, Venezuela, and a Master of Science in electrical engineering from the Georgia Institute of Technology, Atlanta. Currently, he is a professor in the Department of Electronic Engineering of the Universidad Nacional Experimental Politécnica "Antonio José de Sucre." His research interests include wired and wireless networks, OFDM, MIMO systems, and channel modeling.

GUILLERMO ACOSTA-MARUM (gacosta@gatech.edu) received Bachelor (with Honors) and Master of Engineering degrees from Stevens Institute of Technology in 1985 and 1987, and an M.B.A. from the ITAM in 1996. He received his Ph.D. from the School of Electrical and Computer Engineering at the Georgia Institute of Technology, Atlanta, in 2007. He has been an adjunct instructor in electrical engineering at the Instituto Tecnológico Estudios Superiores de Monterrey Campus Estado de Mexico (ITESM-CEM), the Universidad Iberoamericana, and Georgia Tech. His research interests include wireless LAN, wireless MAN, OFDM, MIMO, and channel modeling.