Internet of Vehicles: Architecture, Protocols, and Security

Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez

***Abstract*—Today, vehicles are increasingly being connected to the Internet of Things which enable them to provide ubiquitous access to information to drivers and passengers while on the move. However, as the number of connected vehicles keeps increasing, new requirements (such as seamless, secure, robust, scalable information exchange among vehicles, humans, and roadside infrastructures) of vehicular networks are emerging. In this context, the original concept of vehicular ad-hoc networks is being transformed into a new concept called the Internet of Vehicles (IoV). We discuss the benefits of IoV along with recent industry standards developed to promote its implementation. We further present recently proposed communication protocols to enable the seamless integration and operation of the IoV. Finally, we present future research directions of IoV that require further consideration from the vehicular research community.**

***Index Terms*—Internet of Vehicles (IoV), protocol, security, standards, vehicular ad-hoc networks (VANETs).**

I. Introduction

TODAY, the transportation systems in many countries are increasingly being stretched to their limits as the number of people using them keeps increasing. In many cases, these transportation systems have become inefficient and costly to maintain or upgrade. A recent report noted that the number of vehicles (passenger and commercial) used worldwide is slightly higher than one billion [1] and is expected to reach two billion by 2035 [2]. The rapid growth in the number of vehicles causes an increase in traffic congestion and number of fatalities that occur due to accidents on the roads [3]. In the future, we anticipate substantial changes in the transportation system to cope with emerging requirements of new vehicles, passengers, and drivers along with new paradigms such as the Internet of Things (IoT), cloud computing, among others. Recent advances in computing and networking technologies have led to the development of a wide range of intelligent devices often equipped with embedded processors and wireless communication technologies. These intelligent devices are being deployed to provide a safer and more convenient environment through their interconnection and interoperability, creating the new concept of IoT. In addition, as high speed mobile Internet access becomes more affordable and ubiquitous, opportunities for new products and services for society are emerging.

Raymond James' industry reported that in 2011 the number of Internet-connected devices surpassed the number of people on the planet, and it is expected to reach between 26 billion and 50 billion by 2020 [4]. This exponential increase in the number of connected devices opens the door for different types of machine-to-machine (M2M) communications which enable ubiquitous connectivity among devices thereby enabling the IoT paradigm. Vodafone stated that the automotive industry is one of the fastest growing sectors (with an increase of approximately 32% and 19% for automotive and logistic and transportation sectors, respectively [5]) where M2M communication is being heavily deployed.

The concept of vehicular ad-hoc networks (VANETs) was conceived over a decade ago and has since then been a very active area of research both in academia and industry [6]–[9]. However, as the number of vehicles connected to the IoT increases, new requirements of VANETs (such as intervehicular, vehicular-infrastructure and vehicular-Internet, vehicular-personal devices, and intravehicular communications) are emerging. One of the main problems of VANETs is its limited capacity for processing all the information that is collected by themselves and other actors (such as sensors and mobile devices) around the environment. In this context, vehicles must evolve into "smart" objects equipped with a multisensor platform, with a set of communication technologies, robust computational units, IP-based connectivity to the Internet, and a direct or indirect connection to other vehicles and with all devices around the environment. In this context, the concept of VANETs is evolving into the Internet of Vehicle (IoV).

The basic principle of a VANET is that a vehicle is a mobile node that enables it to connect to other vehicles thereby creating a network. Vehicles are connected or disconnected as they fall inside or outside of the coverage range. However, we consider a VANET to be a conditioned network with mobility constraints, affected by the number of connected vehicles, and several factors such as traffic jams, tall buildings, and bad driver behaviors which affect its performance and use.

VANETs lack the processing capacity for handling global information. VANETs does not have the capacity to analyze, process, and evaluate the global information that is collected

Manuscript received October 1, 2016; revised December 23, 2016; accepted December 30, 2016. Date of publication April 4, 2017; date of current version November 14, 2018. The work of S. Zeadally was supported by the University Research Professorship Award from the University of Kentucky in 2016. *(Corresponding author: Sherali Zeadally.)*

J. Contreras-Castillo and J. A. Guerrero-Ibañez are with the School of Telematics, University of Colima, Colima 28040, Mexico (e-mail: juancont@ucol.mx; antonio_guerrero@ucol.mx).

S. Zeadally is with the College of Communication and Information, University of Kentucky. Lexington, KY 40506 USA (e-mail: szeadally@uky.edu).

Digital Object Identifier 10.1109/JIOT.2017.2690902

from the different vehicles that are part of the network. However, VANETs are well suited for short term applications or for small scale services such as collision prevention or road hazard control notifications services. In contrast, IoV integrates two technological visions: 1) vehicle's networking and 2) vehicle's intelligence [10] and focuses on the integration of objects such as humans, vehicles, things, networks, and environments to create an intelligent network based on computing and communication capabilities that supports services (such as global traffic efficiency and management service based on pollution levels, road conditions, congestion traffic level, or vehicular safety services) for large cities or even a whole country.

By using intelligent systems on vehicles and different cyber-physical systems (such as sensors, vehicles, and mobile devices) in cities we can develop a global network that provides different services to vehicles and the humans associated with them. IoV also refers to vehicles, humans, components of the transportation infrastructure, and a set of devices allocated in the environment, connected through an all IP-based infrastructure, that exchange information directly or indirectly to contribute toward a more efficient, safer, and greener world of transportation [11].

The main contributions of this paper include: first, we describe and discuss how IoV can help to achieve a sustainable intelligent transportation system and bring considerable benefits to drivers and passengers, society, service providers and auto manufacturers; second, we propose a new seven-layered IoV model that addresses some of the deficiencies and drawbacks of previously proposed IoV models; and finally, we identify future challenges that must be addressed in order to achieve a scalable, robust, secure, and fully operational IoV environment.

The remainder of this paper is organized as follows. Section II describes the concept of the IoV. We present the current architecture or architectures being proposed for IoV in Section III. Section IV focuses on message exchange protocols for IoV. Section V discusses how security solutions can be deployed to address some of the security and privacy challenges in IoV. Section VI presents some of the future research challenges for IoV. We make some concluding remarks in Section VII.

II. Benefits of IoVs

Recent technological advances and ease of access to mobile Internet have transformed the car into "the new mobile device" enabling people in these vehicles to become "connected occupants." When vehicles and occupants are connected, they access, consume, create, enrich, and share a lot of digital information among businesses, people, organizations, infrastructure, and other cars leading to the emerging concept of IoVs.

The IoVs might be defined as a platform that enables the exchange of information between the car and its surroundings through different communication media. As a result of the integration of the IoT technology with intelligent transportation systems (ITSs), IoV will create an integrated network for supporting different functions (such as intelligent traffic management, dynamic information services, intelligent vehicle control, among others) [12]. IoV is composed of three fundamental components: 1) the intervehicular network; 2) intravehicular network; and 3) vehicular mobile Internet. IoV allows vehicles to be permanently connected to the Internet, forming an interconnected set of vehicles that can provide information for different services such as traffic management, road safety, and infotainment [13]. IoV enables the exchange of information among vehicles, road infrastructures, passengers, drivers, sensors and electric actuators, and the Internet using communication protocols and standards such as IEEE 802.11p, directional medium access control (DMAC), vehicular cooperative media access control (VC-MAC), ad hoc on demand distance vector, dynamic source routing, general packet radio services, and others [14]. IoV differs from ITS because it puts more emphasis on information interaction among vehicles, human, and the surrounding road infrastructures.

Every year, approximately 1.3 million people die and more than 7 million people are injured in around 8 million traffic accidents. People waste more than 90 billion hours because of traffic problems (accidents and traffic jams), causing a loss of 2% of the global gross domestic product and vehicular travel generates 220 million metric tons of carbon equivalent [15]. The cost of personal transportation in cars (not including public or commercial vehicles) is about $3 trillion per year in the United States and 40% of this cost is related to crashes, parking, roads, traffic services, and pollution [16].

The IoV concept opens up many new opportunities and applications and offers various benefits to drivers, society, and businesses. Cisco IBSG Automotive and Economics practices indicate that IoV will help provide $1400 U.S. in benefits per vehicle, per year [17]. These include the following.

1) Vehicle User: It is estimated that the saving will be around $550 U.S. based on lower insurance rates, lower operation costs and less time spent in traffic which increases productivity due to reduced traffic congestion by recognizing and anticipating risk and dynamically calculating optimal routes.

2) Society: Societal benefits could be around $420 U.S. that could be obtained through lower traffic road operational costs, a decrease in the number of crashes and better control of congestion through traffic management and optimization of road networks and reduced CO_2 emissions.

3) IoV Service Providers: They could save around $160 U.S. through traffic guidance, navigation, emergency services, and location-based services.

4) Auto (Original Equipment Manufacturers/Original Equipment Suppliers): They could save around $300 U.S. through lower service/warranty costs and new profit pools amortized over eight years [18].

In 2015, the National Highway Traffic Safety released the results of a study which showed that the United States spend more than $836 billion on crashes, insurance premiums, and traffic law enforcement accounts [19]. Another report released in 2014 by Seattle-based INRIX and the Centre for Economics and Business Research revealed that traffic congestions cost Americans $124 billion in direct and indirect losses, and this

number is expected to increase to $186 billion in 2030 [20]. Increasing road safety and reducing traffic congestion can yield major benefits for public health expenditure because if the number of road accidents reduces then related public health costs will also be reduced. If drivers spend less time in traffic jams and vehicles are connected all time, real-time traffic solutions will contribute to increased productivity. Mai market research shows that IoV might create a total of 400 000 new jobs in the U.S. [21].

Finally, IoV will create a whole new set of service providers which will develop new services such as parking spot locator services, real-time traffic information, and location-based services that create immediate value not only for drivers but also for businesses in terms of future services they can sell to their customers. The European Union estimates that the global market size for IoV components will be 115.26 billion Euros by 2020 [22].

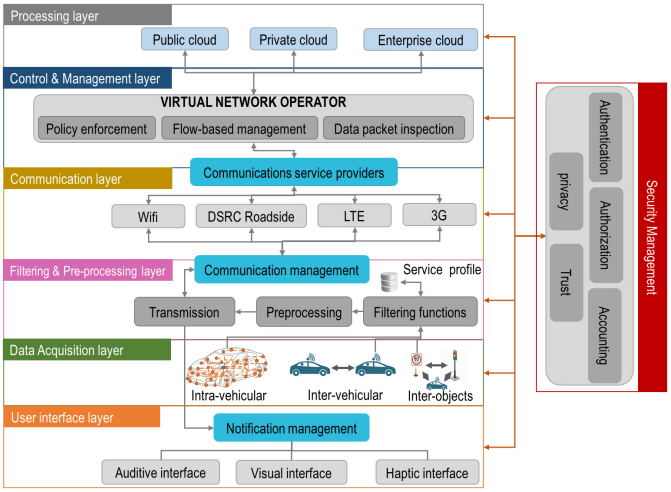

Fig. 1. Proposed seven-layer IoV architecture based on [24]–[26].

III. Architecture of IoV

Based on the interaction of different technologies in the IoV environment, researchers have identified a three-level architecture [23], [24]. The first level contains all the sensors within the vehicle that gather environmental data and detect specific events of interest such as driving patterns and vehicle situations, environmental conditions, among others.

The second level is the communication layer which supports different wireless communication modes such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian, and vehicle-to-sensor. The communication layer ensures seamless connectivity to existing and emerging networks (such as GSM, Wi-Fi, LTE, Bluetooth, 802.15.4, among others).

The third layer includes statistics tools, support for storage, and processing infrastructure which constitutes IoV intelligence and provides mobile cars with big data-based processing (i.e., accessing computing resources, content searching, spectrum sharing, etc.) and is responsible for storage, analysis, processing, and decision making about different risk situations (such as traffic congestion, dangerous road conditions, among others). The goal is to be able to make unified decision based on the fusion of information obtained from different systems and technologies (big data, wireless sensor network, cloud computing, etc.).

CISCO has proposed an IoV architecture based on four layers [25]. The *end points layer* covers the vehicles, software, and the V2V communication through 802.11p. The *infrastructure layer* defines all technologies that allow connections between all actors of IoV. The *operation layer* monitors the policy enforcement and the flow-based management. Finally, the *service layer* specifies the services that the different types of cloud (public cloud, private cloud, and enterprise cloud) offer to drivers based on subscription, data center, or on-demand. IoV allows vehicles and drivers to be connected to the Internet, and therefore, enables them to have access to a broad range of service providers. This access will facilitate commercial business services' integration with vehicles hence creating the vehicle-to-business (V2B) communication. SAP research proposed a service-based architecture based on the service oriented architecture and the event-driven architecture. V2B integration architecture specifies two dedicated components: 1) the vehicle integration platform as a back-end system that enables efficient information exchange between vehicles and enterprise applications and 2) the back-end integration manager that connects in-vehicle components [26].

After we analyzed the proposed IoV layered architectures in [24]–[26], we identified the following weaknesses: 1) the previous IoV models proposed do not consider security (authentication, authorization, accounting, and trust relations); 2) they do not provide a layer to integrate the communication intelligence (selection of the best network for information transmission/dissemination or accessing a service); 3) in these models the interaction with drivers and passengers is limited to providing notifications through the different car devices; 4) additionally, all the collected information is transmitted without preprocessing, which could lead to network congestions he number of vehicles increases. To address these weaknesses, we propose a new seven-layered model architecture for IoV that allows a transparent interconnection of all the network components and dissemination of data into an IoV environment. In this seven-layer architecture, we provide a security layer to manage authentication, authorization, and accounting of all the transactions among the different IoV entities. The IoV model supports a user-vehicle interface to manage the interactions between the vehicle and the driver. We also have a communication interface which selects the optimal network to transmit. For example, if we are going to use a Wi-Fi network, it selects the best service provider based on several factors, such as the requirements of the communication, the vehicle profile and quality of the network, and transaction cost, among others to maintain the quality of the communication. Fig. 1 shows the proposed architecture.

User Vehicle Interface Layer: This layer provides direct interaction with the driver through a management interface to coordinate all driver notifications and select the best display element for the current situation or event to help reduce driver's distractions. For example, if there is a collision risk

with a vehicle ahead, a set of lights on the car's dashboard can activate while a sound is emitted to alert the driver.

Data Acquisition Layer: This layer collects data from various sources (vehicle internal sensors and the navigation system, data collected from intervehicle communication, data from sensors, traffic lights, and signals among others) located on the roads.

Data Filtering and Preprocessing Layer: This layer analyzes the collected information to avoid the transmission of irrelevant information and reduce the network traffic. Transmission decisions are based on a service profile created for the vehicle which has subscribed or active services.

Communication Layer: This layer selects the best network to send the information by using several selection parameters such as congestion and QoS level in the different available networks, information relevance, privacy and security, among others.

Control and Management Layer: This layer is responsible for managing different network service providers that are within the IoV environment. In this layer, different policies (such as traffic management, traffic engineering, and packet inspection) and functions are applied to better manage the information received.

Processing Layer: This layer processes large amounts of information using various types of cloud computing infrastructures locally and remotely. The results of the processed information can be used by massive data services providers to further improve the service or to develop new applications. The results obtained after processing can also be used by various government agencies in the development of future infrastructures, V2B services [27], and policies to help improve or better manage road traffic.

Security Layer: This is a transversal layer that has direct communication with the rest of layers. It is responsible of all security functions (such as data authentication, integrity, nonrepudiation and confidentiality, access control, availability, among others) within the proposed architecture. The layer is designed to support mitigating solutions for address various types security attacks (such as cyberattacks and others) in IoV.

As shown in Fig. 2, when a vehicle starts its engine, it triggers the initialization process to authenticate itself with the IoV network and begins the environmental data acquisition process. This acquisition step collects all the information generated by vehicles, humans, and roadside infrastructures (car sensors, location, pollution level sensors, traffic lights, signs, cell phones, mobile devices, body area networks, among others) within the mobility area of the vehicular network. The collected information is filtered and preprocessed to obtain the most relevant information to be transmitted to: 1) the driver, using one of the interaction mechanisms such as visual, acoustic or haptic; 2) to the network depending on the coverage, type and sensitivity of the information; or 3) discarded to reduce the load on the IoV network.

For example, if a vehicle receives an accident notification, it is displayed to the driver and the notification is then broadcasted. But if another vehicle receives the same information, without changes, then it will not rebroadcast it a second time.

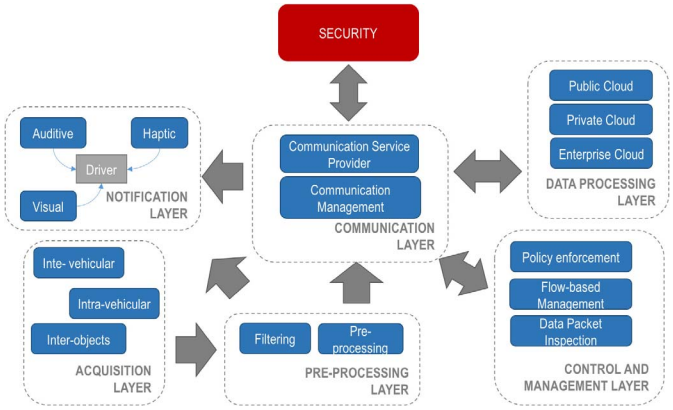

Fig. 2. Communication example of the proposed seven-layered architecture.

Based on the vehicle's profile (service requirements) and the available information in the environment (such as available network access technologies, available network service providers, QoS of each network, costs, and others) the best network is selected using some intelligent algorithm (implemented in the communication layer). All the information transmitted through the network is managed through a set of mechanisms (such as policies and rules, network flow processing and classification, packet inspection, among others) to maintain high efficiency for all services delivered within the IoV environment. The preprocessed information is classified (e.g., as private and business), and then sent to the most suitable cloud for analyzing, processing, storing, and availability based on the information type.

A. Standards for Internet of Vehicles

IoV involves many participants and the connectivity must be assured between all participants. One of the main challenging issues for the interconnection of vehicles is interoperability. To ensure this, we need to develop standards for the IoV framework.

International organizations and consortia such as the Internet Engineering Task Force, EPCglobal, Institute of Electrical and Electronics Engineers, the European Committee for Standardization (CEN), and the European Telecommunications Standards Institute (ETSI), led by the World Wide Web Consortium (W3C) are investing a lot of efforts to define standards and protocols for IoV.

The W3C is focusing on standards for application developers which will provide more accurate access to vehicle data (such as vehicle identification, acceleration and speed, tire pressure, battery status, and personalization information) [28].

ETSI and CEN published the basic set of standards requested by the European Commission to ensure interoperable communication between vehicles made by different manufacturers.

Fig. 3 provides some of the most prominent protocols defined by the various international standardization organizations [29]. Although almost all application layer protocols have been developed for IoT, however, they can be implemented in IoV.

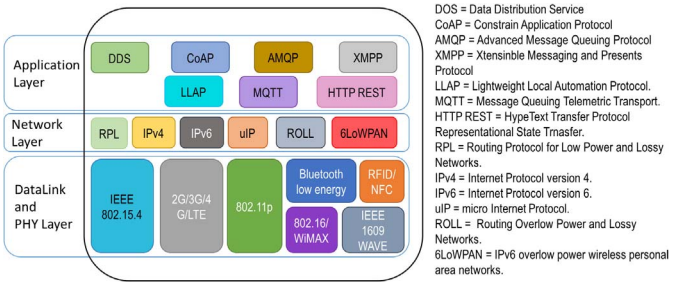

Fig. 3. Standards for IoV [29].

B. Recent Projects and Solutions on the Market for IoV

To address several of the challenges related to IoV, various projects (as shown in Table I) are undertaken by academia, industry, and government recently.

Finally, there are also some recent market developments regarding the IoV. The IoV market is classified in two service categories. The first category is on-board diagnostic which is a service based on the information that is collected inside the car. Companies such as Metromile (http://www.metromile.com), Automile (http://www.automile.com), and Zubie (http://www.zubie.com) deliver vehicle's data such as trip information, fuel consumption, car diagnostics, tracking, among other information.

The second category is a service based on environmental sensors that collect data from the environment of the car and provides information to the driver about traffic conditions, parking services, and so on. In this context, INRIX (http://www.inrix.com) offers dynamic data services to assist drivers. These services provide up-to-date, accurate real-time traffic, parking information, road hazards, fuel and weather conditions, and a range of cloud-based services for the demanding automotive industry. One of the cruise companies (http://www.getcruise.com) sells a device (mounted on top of a car) that monitors the road. The device uses a computer, and switch to auto-pilot mode thereby turning modern Chevrolet bolt EVs into autonomous vehicle with sensors, radars, and actuators collecting and processing data to make real-time decisions based on current traffic conditions.

TABLE I
IoV PROJECTS: GOALS AND ACHIEVEMENTS

Project	Goals and Project Results
Connected car project Local Motors (2015-current) https://localmotors.com/awest/connected-car-project-internet-of-things/activity/	The project is sponsored by IBM & Intel to create an open source connected Rally Fighter to demonstrate Internet of Things capability. Additionally, they will use the Rally Fighter's development platform to integrate technology into all their vehicle innovations. The result is a prototype car that can report oncoming rain, the need to turn on lights and accidents to other connected cars automatically. The car has been showcased at the IBM compact conference held in April 2014.
Sixth Sense Transport Project UK Research Council (2014-current) http://www.sixthsensetransport.com/	The project investigates how travel decisions could be enhanced using social networking principles and smartphone technology to create a snapshot view of transport options in time and space. Thus, a series of innovative applications (such as 6ST CAMPSITE, 6ST OXFAM, goWSB) for tourism, transport and logistic sectors have been developed.
Connected vehicle safety pilot United States Department of Transportation http://safetypilot.umtri.umich.edu	This is a research program focused on testing connected vehicles safety applications in real-world driving scenarios based on the developed platform. They evaluated their platform to determine its effectiveness in detecting risk situations and ensuring that the platform does not distract drivers. The study revealed some prominent characteristics (such as geographic relationship between vehicles) related to motor bus crashes, and how these characteristics are amenable to connected vehicle solutions.

IV. PROTOCOLS IN IoV

Intervehicular communication protocols in VANETs play an essential role in IoV as they enable different levels of interaction among vehicles, humans, and roadside units. They can provide alternate routes efficiently and quickly if a problem arises with the current route. However, IoV extends beyond VANETs (as we mentioned earlier) and places more emphasis on information exchange among vehicles, human, and the surrounding road infrastructures. Next, we briefly present basic VANET communication protocols that can be applied to IoV.

A. Physical Layer Protocols

When a protocol for physical layer is designed some factors such as multipath fading and Doppler frequency shifts that are caused by the movements of vehicles must be considered. Some recent efforts have focused on the use of infrared and radio waves for vehicle-vehicle communications because they offer line-of-sight and broadcast communications. Dedicated short range communication, also known as IEEE 802.11p wireless access in vehicular environments (WAVE), is based on IEEE 1609 standards and describes techniques and interface processes controlled by the MAC layer for public safety and private applications [30]. The frequency band is divided into six service channels that are used for different application types (frequency range 5.855–5.875 MHz for ITS nonsafety applications and frequency range 5.875–5.905 MHz for safety and traffic efficiency applications) and one control channel. The main idea of IEEE 802.11p WAVE protocol is to integrate PHY and MAC layers of the IEEE 802.11 wireless standards

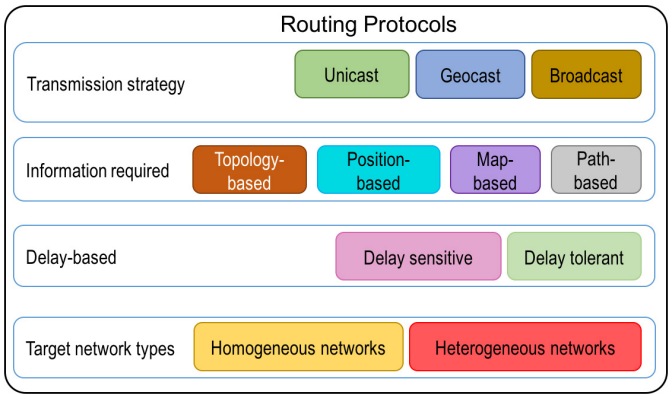

Fig. 4. VANETs Routing protocols taxonomy adapted from [35].

to allow data exchange among vehicles and roadside devices in the 5.9 GHz band [31].

B. MAC Layer Protocols

MAC protocols for IoV should support different types of applications with different requirements for QoS (such as low delay or failure rates). MAC protocols need to solve several problems such as hidden station problem or the shared bandwidth among the communicating vehicles. Some protocols such as IEEE 802.11p or DMAC [32] use OFDM technology and a CSMA mechanism to control the medium access and to avoid collisions. IEEE 802.11p provides reliability and low latency requirements present in intervehicular communications. DMAC increases the re-use of the transmission channel to improve the performance and reduce collisions using directional antennas. Other type of MAC protocols use the ALOHA approach in their transmission scheduler. In this category, some protocols such as ADHOC MAC [33] or VC-MAC [34] have recently been proposed in the literature as alternative protocols for cooperative communication protocols in VANETs environments to: use spatial reusability to maximize the network throughput, guarantee QoS, address terminal problems, reduce transmission collisions and [15].

C. Routing Protocols in IoV

Cheng *et al.* [35] presented a taxonomy on routing protocols ranging from protocols with a transmission strategy to those for network types (as shown in Fig. 4).

Transmission strategy-based routing protocols focus on transmitting data from a single node to a destination node, either through all nodes within a specified geographical region or all nodes of the network through multihop transmissions as discussed in [36]–[39]. However, this type of protocols can incur high delays when finding routes. Consequently, their performance is very poor in large networks and could cause excessive network flooding, which in turn, could cause a disruption in nodes' communications.

Information-based routing protocols distribute routing information among nodes by sending entire dumps infrequently and smaller incremental updates based on beacon messages. Several examples of such routing protocols are described in [40]–[44]. However, in IoV, vehicles could have dynamic behavior where the routing tables may contain inconsistent information which makes it difficult to find and maintain routes which in turn require an accurate vehicle's position to determine the type of services that can be offered.

Delay-based routing protocols are classified into two categories: 1) delay sensitive protocols which need to exchange data as soon as possible and 2) delay-tolerant protocols which manage connection failures occurrences using a carry and forward mechanism [45]–[47]. However, some challenges need to be solved: 1) delay-tolerant protocols to need to maintain substantial network coverage while limiting network transmissions and 2) delay-sensitive protocols need to reduce the probability of congestion of routing paths and maintain a high delivery ratio with low latency.

Target networks routing protocols refer to the type access technology that vehicles can use. In this context, traditional routing protocols in VANETs focus on scenarios in which all packets are transmitted over short distances using the same wireless technology [48]–[54]. However, given that the heterogeneous nature of IoV will include different radio access technologies, one of the main challenges is handoff which involves real-time switching of access technologies based on: network performance, connection availability, packet delay, or pricing, while maintaining active connections.

Even though many routing protocols have been published, they focus on homogeneous network models instead of heterogeneous models (such as those required in IoV) which open up several challenges that must be addressed. These challenges include the handoff timing, the gateway node in a network, the most suitable wireless technology to transmit packets, IP addressing, and vehicles' mobility demeanor.

Routing protocols in IoV must have an efficient model to manage dynamic topology variations which is an issue that has not yet been fully solved by current VANETs routing protocols. The heterogeneous model of IoV requires the handling of different network parameters from applications due to the large scale of IoV. It is worthwhile pointing out that there is a need for hybrid routing protocols that can handle efficient methods to reduce delay due to rapid topology changes and traffic density, efficient privacy preserving location services that protect the privacy of a vehicle's navigation information. In addition, routing protocols should also control the flooding of the network to avoid disruption of nodes' communications.

V. Security in IoV

In IoV, we need to integrate many different technologies, services, and standards [35]. However, heterogeneity and the large number of vehicles will increase the need for data security. Zhang [55] stated that IoVs, as with other technologies, have many security vulnerabilities. Vehicles operate in vulnerable and unprotected environments with serious problems of security in vehicle-to-infrastructure and cloud communications. IoVs can become very vulnerable to cyberattacks. Malicious people can exploit vulnerable connection points and manipulate vehicular data streams with devastating effects such as: MP3 files infecting a whole network of cars very

TABLE II
SECURITY REQUIREMENTS FOR IOV

Security requirement	Description
Data authentication	When data is transferred, the identities of vehicles must be verified
Data integrity	Transmitted and received data must be checked to ensure that data is delivered correctly
Data confidentiality	Data must be protected to ensure secret data transmission occurs between different vehicles participating in IoV.
Access control	In IoV, vehicles should only access available services that they are entitled to
Data non-repudiation	We need to ensure that a vehicle cannot deny the authenticity of another vehicle
Availability	To ensure the communication between vehicles in different conditions
Anti-jamming	To define mechanisms that can prevent malicious vehicles from sending interfering messages that interrupt the communication between vehicles

quickly [56]. Once the cybercriminal gets control of the car's data system, he/she could manipulate different components of the car such as brakes, unlock doors, or even turn the car off. At a recent Black Hat cybersecurity conference, a demonstration showed how some software allows attackers to control a Jeep Cherokee while on the move.

This example demonstrates the potential dangers on the road ahead for the IoV [57]. Hickey [58] mentioned that one way to analyze the security problem from an effort-and-impact perspective is to identify mitigation techniques that are used in comparable critical infrastructure systems of national importance. He argued that disrupting a vehicle's communication or sensors, for example, would require a more complex and sophisticated attack than one designed to simply gather information, and disrupting the vehicle's control commands would be even harder. Regardless, the threat is real and a security breach could have severe consequences on drivers, passengers, other vehicles, and infrastructures. For these reasons is necessary to make security a high priority for the IoV.

Some efforts have been made to address security issues in the IoV. The National Institute of Standards and Technology proposed a framework to improve critical infrastructure cybersecurity that may be incorporated into IoV technologies [59]. Other authors also developed V2V and V2I secure communication schemes for VANET applications [60]–[62].

A. Security Requirements

IoV has several security requirements that must be addressed before it captures a large end-user market. The solutions that meet the security requirements must be developed to maintain privacy and security of end-users. Table II presents a summary of some of the security requirements that IoV must meet [63].

VI. FUTURE RESEARCH DIRECTIONS ON IOV

IoV will improve automotive and information technologies thereby contributing to economic and social development through a more robust, efficient, and intelligent transportation system that will have a direct impact on users' lifestyle [64].

As with other markets, the IoV market is driven by various trends. In this context, Lengton *et al.* [65] identified four major trends that will fuel the growth of IoV in the future.

1) *Energy Efficiency:* This trend is expected to continue because IoV provides several benefits through its potential to maximize fuel economy. A reduction of fuel consumption through better driving and more advanced traffic control systems will reduce traffic jams and subsequently fuel consumption.
2) *Connected Devices:* The trends of integration between devices and applications will promote the IoV market by allowing companies to take advantage of new application opportunities and have access to a much larger end-user base.
3) *Security:* The strong demand for security features in IoV solutions continues to grow. Robust, cost-effective, and scalable security are needed to ensure that the IoV platform conforms with legal requirements for data and identity security protection.
4) *Safety:* This trend is related to various types of safety features. In this context IoV will be able to provide drivers with unprecedented safety features on the road. Furthermore, IoV applications may be able to provide personalized safety features, such as the identification of personal health conditions while on the road and anti-fatigue systems.

Another major trend is the improvement of data processing performance and capability. This trend focuses on the migration from a traditional operating support system to a new platform that can handle the rapid increase of the amount of data collected for the IoV system and the creation of new solutions for data analytics [27].

The application of IoV technology collects and disseminates information and implements supervision and control to improve traffic efficiency, enhance traffic safety, to make the lives of millions of people more enjoyable and convenient, coupled with a wide range of traffic safety services. Complementary efforts should also focus on the design of new middleware platforms to enable analysis and processing of vehicular information to allow informed decision making.

Finally, the main IoV challenges include: 1) efficient and scalable coordination and communication among devices and 2) the lack of standards to enable robust V2V communication. Open standards are needed to achieve a uniform communication and information sharing environment which allows for the transparent and seamless integration with current closed standards in order to improve services and user experiences in the IoV ecosystem.

VII. CONCLUSION

In this paper, we presented some of the most relevant technologies that support IoV. IoV provides numerous benefits including dynamic information services, intelligent vehicle control, and applications to reduce insurance rates and increased productivity due to reduced traffic congestions. We also proposed a seven-layer architecture for IoV as well as the standards used for interoperability of all participants.

Finally, we discussed the protocols used for wireless access communications and routing protocols as well as intervehicular communication protocols. We further discussed some security requirements in IoV followed by future IoV research challenges that must be addressed. We argue that IoV will promote the integration of automotive and information technology which will contribute to the development of applications related to energy efficiency, connected devices, security, and safety all of which will ultimately help reduce the lack of coordination and communication among vehicles and improve products, services, and experiences.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments, which helped them to improve the presentation of this paper.

REFERENCES

[1] Org. Int. Constructeurs d'Automobiles. (2014). *Number of Passenger Cars and Commercial Vehicles in Use Worldwide From 2006 to 2014 in (1,000 Units)*. Accessed on Sep. 16, 2016. [Online]. Available: http://www.statista.com/statistics/281134/number-of-vehicles-in-use-worldwide/

[2] J. Voelcker. (Aug. 2011). *It's Official: We Now Have One Billion Vehicles on the Planet*. Accessed on Sep. 16, 2016. [Online]. Available: http://www.greencarreports.com/news/1065070_its-official-we-now-have-one-billion-vehicles-on-the-planet

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

[4] J. Raymond, "The Internet of Things: A study in hyper, reality, disruption and growth," U.S. Res. Published Raymond James Assoc., St. Petersburg, FL, USA, Tech. Rep., 2014.

[5] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad hoc networks," *Veh. Commun.*, vol. 1, no. 4, pp. 214–225, Oct. 2014.

[6] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecomun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

[7] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Commun. J.*, vol. 4, no. 7, pp. 894–903, Apr. 2010.

[8] J. Guerrero-Ibanez, C. Flores-Cortes, and S. Zeadally, "Vehicular ad-hoc networks (VANETs): Architecture, protocols, and applications," in *Next Generation Wireless Technologies: 4G and Beyond*, N. Chilamkurti, S. Zeadally, and H. Chaouchi, Eds. London, U.K.: Springer, 2013, ch. 5.

[9] G. Dimitrakopoulos, "Intelligent transportation systems based on Internet-connected vehicles: Fundamental research areas and challenges," in *Proc. 11th Int. Conf. ITS Telecommun.*, St. Petersburg, Russia, Aug. 2011, pp. 145–151.

[10] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, and S. Qibo, "An overview of Internet of Vehicles," *China Commun. Veh. Netw.*, vol. 11, no. 10, pp. 1–15, Oct. 2014.

[11] M. Nitti, R. Girau, A. Floris, and L. Atzori, "On adding the social dimension to the Internet of Vehicles: Friendship and middleware," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw.*, Odessa, Ukraine, May 2014, pp. 134–138.

[12] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.

[13] *IRF World Road Statistics Database, 2008; World Bank Global Road Safety Facility, 2010*, Cisco IBSG, San Jose, CA, USA, 2011.

[14] F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Netw.*, vol. 44, pp. 90–103, Jul. 2016.

[15] "Transportation cost and benefits analysis II—Vehicle costs," Dept. Transp., Amer. Automobile Assoc., Heathrow, FL, USA, and Victoria Transp. Policy Inst., Victoria, BC, Canada, Tech. Rep., 2015.

[16] A. Mai, *The Internet of Cars, Spawning New Business Models. CISCO*, Oct. 2012, pp. 1–9. [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2012/07/12-10-24-SCV-GSMA-Cisco-Perspective-F.pdf

[17] A. Mai and D. Schlesinger, *A Business Case for Connecting Vehicles, Executive Summary*, Cisco Internet Business Solutions Group, San Jose, CA, USA, 2011.

[18] L. J. Blincoe, T. R. Miller, E. Zaloshnja, and B. A. Lawrence, "The economic and societal impact of motor vehicle crashes," U.S. Dept. Transp., Nat. Highway Traffic, Washington, DC, USA, Tech. Rep. DOT HS 812 013, May 2015.

[19] *Traffic Safety Facts Research Note: 2015 Motor Vehicle Crashes Overview*, Nat. Highway Traffic Safety, Washington, DC, USA, Aug. 2016.

[20] "The future economic and environmental costs of gridlock in 2030," INRIX, Kirkland, WA, USA, Tech. Rep., Jul. 2014. [Online]. Available: http://inrix.com/download-the-inrix-cost-of-congestion-report-2/

[21] A. Mai and D. Schlesinger, *Connected Vehicles and Government: A Catalyst to Unlock the Societal Benefits of Transportation*, Cisco Internet Bus. Solutions Group, San Jose, CA, USA, and Safety Admin., Washington, DC, USA, 2011.

[22] R. Viereckl, D. Ahlemann, J. Assmann, and S. Bratzel. (2014). *Racing Ahead the Connected c@r 2014 Study*. pp. 1–11, accessed on Apr. 13, 2017. [Online]. Available: https://www.strategyand.pwc.com/media/file/Racing-ahead.pdf

[23] L. Nanjie, "Internet of Vehicles your next connection," *WinWin Mag.*, vol. 12, no. 11, pp. 23–28, Dec. 2011. Accessed on Apr. 13, 2017. [Online] Available: http://www.huawei.com/en/publications/winwin-magazine/11/HW_110848

[24] K. Golestan, R. Soua, F. Karray, and M. Kamel, "Situation awareness within the context of connected cars: A comprehensive review and recent trends," *Inf. Fusion*, vol. 29, pp. 6–83, May 2016.

[25] F. Bonomi, *The Smart and Connected Vehicle and the Internet of Things*, WSTS, San Jose, CA, USA, 2013.

[26] M. Miche and T. M. Bohnert, "The Internet of Vehicles or the second generation of telematic services," *ERCIM News*, vol. 77, pp. 43–45, 2009. Accessed on Apr. 13, 2017. [Online]. Available: https://ercim-news.ercim.eu/images/stories/EN77/EN77-web.pdf

[27] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Solving vehicular ad hoc network challenges with big data solutions," *IET Netw.*, vol. 5, no. 4, pp. 81–84, Jul. 2016.

[28] *New Connected Car Standards Put Europe Into Top Gear*, Eur. Commission, Brussels, Belgium, Feb. 2014. [Online]. Available: http://europa.eu/rapid/press-release_IP-14-141_en.pdf

[29] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 1st Quart., 2015.

[30] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[31] "Intelligent Transport Systems (ITS); radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band," ETSI, Sophia Antipolis, France, Tech. Rep. ETSI EN 302 571 (V1.1.1), 2013.

[32] Y.-B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," in *Proc. 19th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, Tel Aviv, Israel, 2000, pp. 13–21.

[33] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services," *Wireless Netw.*, vol. 10, no. 4, pp. 359–366, Jul. 2004.

[34] J. Zhang, Q. Zhang, and W. Jia, "Vc-MAC: A cooperative MAC protocol in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1561–1571, Mar. 2009.

[35] J. Cheng *et al.*, "Routing in Internet of Vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[36] A. Bachir and A. Benslimane, "A multicast protocol in ad hoc networks inter-vehicle geocast," in *Proc. 57th IEEE Semiannu. VTC Spring*, vol. 4. 2003, pp. 2456–2460.

[37] C. Maihofer and R. Eberhardt, "Geocast in vehicular environments: Caching and transmission range control for improved efficiency," in *Proc. IEEE Intell. Veh. Symp.*, Parma, Italy, 2004, pp. 951–956.

[38] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, Philadelphia, PA, USA, 2004, pp. 76–85.
[39] M. Durresi, A. Durresi, and L. Barolli, "Emergency broadcast protocol for inter-vehicle communications," in *Proc. 11th Int. Conf. Parallel Distrib. Syst.*, vol. 2. Fukuoka, Japan, 2005, pp. 402–406.
[40] M. Hager, L. Wernecke, C. Schneider, and J. Seitz, "Vehicular ad hoc networks: Multi-hop information dissemination in an urban scenario," in *38th Int. Conf. Telecommun. Signal Process.*, Prague, Czech Republic, 2015. pp. 65–70, doi: 10.1109/TSP.2015.7296225.
[41] R. S. Yokoyama, B. Y. L. Kimura, L. M. S. Jaimes, and E. D. S. Moreira, "A beaconing-based opportunistic service discovery protocol for vehicular networks," in *Proc. 28th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Victoria, BC, Canada, May 2014, pp. 498–503.
[42] S. E. Carpenter, "Obstacle shadowing influences in VANET safety," in *Proc. IEEE 22nd Int. Conf. Netw. Protocols (ICNP)*, Raleigh, NC, USA, 2014, pp. 480–482.
[43] A. Tahmasbi-Sarvestani, Y. P. Fallah, and V. Kulathumani, "Network-aware double-layer distance-dependent broadcast protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5536–5546, Dec. 2015.
[44] J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1910–1922, May 2008.
[45] G. Li and L. Boukhatem, "A delay-sensitive vehicular routing protocol using ant colony optimization," in *Proc. 12th MED-HOC-NET*, Ajaccio, France, 2013, pp. 49–54.
[46] B. Khanna, J. Redi, P. Basu, and R. Ramanathan, "Disrupted adaptive routing: Gossip-based routing in delay-tolerant networks," in *Proc. IEEE MILCOM*, San Diego, CA, USA, 2013, pp. 1099–1104.
[47] U. Lee, S. Y. Oh, K.-W. Lee, and M. Gerla, "RelayCast: Scalable multicast routing in delay tolerant networks," in *Proc. IEEE ICNP*, Orlando, FL, USA, 2008, pp. 218–227.
[48] K.-Y. Ho, P.-C. Kang, C.-H. Hsu, and C.-H. Lin, "Implementation of WAVE/DSRC devices for vehicular communications," in *Proc. 3CA*, vol. 2. Tainan, Taiwan, 2010, pp. 522–525.
[49] P. D. Dorge, S. S. Dorle, M. B. Chakole, and D. K. Thote, "Improvement of QoS in VANET with different mobility patterns," in *Proc. ICRCC*, Tiruvannamalai, India, 2012, pp. 206–209.
[50] K. Shafiee, A. Attar, and V. C. M. Leung, "Optimal distributed vertical handoff strategies in vehicular heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 534–544, Mar. 2011.
[51] Y. Li, K. Ying, P. Cheng, H. Yu, and H. Luo, "Cooperative data dissemination in cellular-VANET heterogeneous wireless networks," in *Proc. 4th HSIC*, Nanjing, China, 2012, pp. 1–4.
[52] Q. Zhao, Y. Zhu, C. Chen, H. Zhu, and B. Li, "When 3G Meets VANET: 3G-assisted data delivery in VANETs," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3575–3584, Oct. 2013.
[53] S. H. Ahmed *et al.*, "CODIE: Controlled data and interest evaluation in vehicular named data networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3954–3963, Jun. 2016.
[54] S. H. Ahmed, M. A. Yaqub, S. H. Bouk, and D. Kim, "SmartCop: Enabling smart traffic violations ticketing in vehicular named data networks," *Mobile Inf. Syst.*, vol. 2016, May 2016, Art. no. 1353290, doi: 10.1155/2016/1353290.
[55] T. Zhang, *Securing Connected Vehicles: Challenges and Opportunities*, CISCO Syst., San Jose, CA, USA, Dec. 2015. [Online]. Available: http://sites.ieee.org/denver-com/files/2016/02/IoV-Security-Challenges-and-Opportunities-zhang.pdf
[56] L. Reger, *Addressing the Security of the Connected Car*, NXP Blog, Eindhoven, The Netherlands, 2014. [Online]. Available: http://blog.nxp.com/addressing-the-security-of-the-connected-car/
[57] D. Yadron, "Hackers demonstrate how to take control of cars," in *Proc. Black Hat Security Conf.*, Las Vegas, NV, USA, 2015. [Online]. Available: http://www.wsj.com/articles/hacking-cars-to-take-focus-at-black-hat-conference-1438723360?mod=videorelated
[58] J. Hickey, *Vice President*, Vínsula. Telephone Interview, Seattle, WA, USA, Oct. 2012.
[59] (Feb. 12, 2014). *National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity*. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[60] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Comput. Commun.*, vol. 71, pp. 50–60, Nov. 2015.
[61] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Comput. Commun.*, vol. 63, pp. 11–23, Jun. 2015.
[62] D. A. Rivas, J. M. Barceló-Ordinas, M. G. Zapata, and J. D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation," *J. Netw. Comput. Appl.*, vol. 34, no. 6, pp. 1942–1955, 2011.
[63] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.
[64] "White paper of Internet of Vehicles," in *Proc. 50th Telecommun. Inf. Working Group Meeting*, Brisbane, QLD, Australia, Sep./Oct. 2014, pp. 1–7.
[65] M. Lengton, D. Verzijl, and K. Dervojeda, *Internet of Things, Connected Cars. Business Innovation Observatory*, Eur. Union, Brussels, Belgium, Feb. 2015.

Juan Contreras-Castillo received the B.S. degree in computer systems from the University of Colima, Colima, Mexico, in 1996, and the M.Sc. degree in computer sciences and Ph.D. degree in telecommunications from the Centro de Investigación Científica y Educaci Superior de Ensenada (CICESE), Ensenada, Mexico, in 1998 and 2003, respectively.

He is a Full Professor of computer sciences with the School of Telematics, University of Colima. His current research interests include ubiquitous computing, distance learning, mobile learning, wireless sensor networks, and vehicular ad hoc networks.

Sherali Zeadally received the bachelor's degree in computer science from the University of Cambridge, Cambridge, U.K., in 1991, and the doctoral degree in computer science from the University of Buckingham, Buckingham, U.K., in 1996.

He is an Associate Professor with the College of Communication and Information, University of Kentucky, Lexington, KY, USA.

Dr. Zeadally is a Fellow of the British Computer Society and the Institution of Engineering Technology, U.K.

Juan Antonio Guerrero-Ibañez received the M.Sc. degree from the University of Colima (UDC), Colima, Mexico, in 1999, and the Ph.D. degree in telematics engineering from the Universitat Politecnica de Catalunya (UPC), Barcelona, Spain, in 2008.

He is a Full Professor and a member of the Telecommunication and Networks Group, School of Telematics, UDC. His current research interests include networking and QoS provision, wireless sensor networks, and vehicular ad hoc networks.