# Chapter 5
# Vehicular Ad-hoc Networks (VANETs): Architecture, Protocols and Applications

**J.A. Guerrero-Ibáñez, C. Flores-Cortés, and Sherali Zeadally**

## 5.1 Introduction

Modern society faces serious problems with transportation systems. Several factors contribute to the increase of the severity of these problems. One factor is the concentration of population in specific areas. The technical report of the *United Nations Population Foundations* showed that for the first time, more than half of the world's population lives in urban areas [31]. As the urban zones become more populated, the needs of mobility and solutions to congestion problems increase. People depend on mobility, which provides personal freedom and access to services for business and pleasure. The amount of time that people spend on traveling from one location to another can vary significantly depending on the traffic conditions. The growing volume of traffic has adverse effects on the environment, economy, and public health and especially in accidents that cause fatalities, injuries, and material damages.

The Texas Transportation Institute published in its technical report that in 2010 traffic congestion represented $101 billion dollars of annual drain on the U.S. economy, with 4.8 billion hours and 1.9 billion gallons of fuel spent on traffic. These numbers are equivalent to one workweek and three weeks worth of gas every year [29]. In Europe, traffic congestion costs $50 billion per year or 0.5 % of the community Gross Domestic Product (GDP). If appropriate measures are not taken in the next few years, this percentage could increase to 1 %.

J.A. Guerrero-Ibáñez (✉) · C. Flores-Cortés
School of Telematics, University of Colima, Av. Universidad 333, Colima, COL 28040, Mexico
e-mail: antonio_guerrero@ucol.mx

C. Flores-Cortés
e-mail: cfcortes@ucol.mx

S. Zeadally
Department of Computer Science and Information Technology, University of the District of Columbia, Washington, DC 20008, USA
e-mail: szeadally@udc.edu

N. Chilamkurti et al. (eds.), *Next-Generation Wireless Technologies*,
Computer Communications and Networks, DOI 10.1007/978-1-4471-5164-7_5,

According to the technical report on traffic congestion and greenhouse gases [3] a third of America's carbon dioxide ($CO_2$) emissions come from moving people or goods, and 80 % of these emissions are from cars and trucks. According to the Eurostat data, road transport accounted for 19.5 % of the European Union (EU) total greenhouse gas emissions in 2008 [2].

In addition, the technical report of the Commission for Global Road Safety indicates that road crashes kill at least 1.3 million people each year and injure 50 million. Notably, 90 % of these road casualties occur in developing countries. Each year 260,000 children die on the road and another million are seriously injured. By 2015 road crashes are predicted to be the leading cause of premature death and disability for children aged five and older [5].

The statistics and data reported above show that our society faces significant challenges in the transportation area that need to be addressed as quickly as possible. To solve several of the aforementioned transportation problems, and improve transportation safety, security, and efficiency and enable the development of novel vehicular applications, the researchers have been focusing on the design, development, and deployment of intelligent mechanisms and technologies. The primary goal of researchers and engineers is to make traffic control and management more efficient and safe. Emerging communication technologies are being used in innovative solutions to reduce traffic congestion and improve safety. Safety and efficiency on roads should be substantially improved with the deployment of intelligent systems such as adaptive traffic control, incident detection and management systems both in cities and highways. Vehicles must be equipped with wireless radios and communication devices must be placed on roadsides. Roadside units can be utilized to extend the network coverage, enable communication between distant vehicles (i.e. beyond the vehicle's radio range), support a high-speed and low-latency network and provide services to both public and private companies. In this sense, recent technological advances, particularly in the areas of mobile computing, electronic and telecommunications have enabled the emergence of new concepts such as *Intelligent Transportation Systems* (ITS) and a new generation of *wireless ad-hoc networks* namely Vehicular Ad-hoc Networks (VANETs).

We present an overview of some of the traffic and transportation issues and how the use of communication and information technologies can address various transportation challenges listed earlier. We focus on how ITS and, specifically, VANETs can contribute to the development of solutions that improve or solve the problems related to transportation systems. The rest of the chapter is organized as follows. Section 5.2 presents an overview of the ITS. In Sect. 5.3, we present VANET applications and communication technologies used in VANETs. Section 5.4 describes various routing protocols that have been recently proposed for VANETs. In Sect. 5.5, we discuss various VANET security issues. Section 5.6 outlines some of the challenges and opportunities for VANETs followed by some concluding remarks in Sect. 5.7.

## 5.2 Intelligent Transportation Systems

To improve safety, security, and efficiency of transportation systems, the development of novel vehicular applications is required. Applications related to transportation systems are commonly referred as *Intelligent Transportation Systems* (ITS) [25]. There is no unique definition of ITS. Each country or region that attempts to implement *ITS* has its own vision and definition. For example, Europe defines ITS as the new application that information and communication technologies are finding in urban transport and it is also referred as *Transport Telematics* [8]. In the United States, the Intelligent Transportation Society of America (ITSA) defines ITS as a broad range of different technologies can address many of the existing transportation problems. ITS consist of various technologies including information processing, communications, control, and electronics. The integration of all these technologies into existing transportation systems is intended to save lives, time and money [13]. Finally, Japan refers to ITS as a fundamental solution to solve the problems related to transportation systems, which in turn covers traffic accidents, traffic congestion and environmental pollution. ITS deals with these issues using the most advanced communication and control technologies [12].

As we mentioned previously, each country has its own vision of ITS but they all share the same common vision: the usage of emerging technologies to solve issues related to transportation systems. Generally, ITS attempt to utilize communication and information technologies in vehicles and vehicular infrastructures to manage all elements (such as vehicles, traffic loads, and routes) that make up the transportation network. The objectives of *ITS* include safety, reduced travel times, optimize the traffic flows and reduce the fuel consumption. ITS aim to solve these aforementioned issues by applying emerging technologies such as wireless, sensing, cellular, and mesh networks.

By carefully integrating relevant emerging technologies into the transportation system's infrastructure, and in vehicles themselves, the congestion can be alleviated and road safety improved along with an increase in productivity. However, the main challenge is to integrate all technologies within a complementary and cooperative environment that can address various transportation problems. This new cooperative environment where all networking, electronic, and computing technologies are well integrated will enable safer roads, and achieve more efficient mobility and minimize the environmental impact.

One of the most important components of ITS is the Vehicular Ad-hoc NETwork (VANET). VANET is a type of wireless ad-hoc network designed to provide support to a wide variety of applications and benefits in areas such as vehicular safety, entertainment, and traffic control among others.

## 5.3 Vehicular Ad-hoc Networks

VANET is considered as a subgroup of *Mobile Ad-hoc Networks* (MANETs) in which all nodes are vehicles that move at various speeds. The main objective of

VANET is to enable communication among vehicles on the road and between vehicles and roadside infrastructures. For this communication to be possible, devices known as *On-Board Units* (OBUs) and *RoadSide Units* (RSUs) must be placed at each vehicle and road, respectively. These devices can send or receive data to or from roadside units. Nevertheless, if a vehicle cannot directly send its data to an RSU, it can relay its data to other vehicles until the data reach a RSU using a multi-hop transmission strategy [35].

### *5.3.1 VANETs and MANETs*

VANETs and MANETs share common features such as the movement, self-organization and self-management of information in a distributed fashion without a centralized authority or server controlling the communication. Although VANETs share common characteristics with MANETs, VANETs have distinctive features that impact the design of communication systems, protocols, and applications. Some of the unique characteristics of VANETs include:

- In VANETs a node movement is restricted by several factors such as road traffic direction and regulations.
- Unlike MANETs, nodes in VANETs are not subject to power and storage limitations.
- In VANETs the topology is considered highly dynamic because it is always changing, as vehicles are moving at various speeds.
- The propagation model is usually not assumed to be free space because of the presence of different obstacles and potential interference of wireless communications from other vehicles or access points.

Dahiya and Chauhan summarized some of the technical aspects that contrast VANETs from MANETs. Their analysis is presented in Table 5.1 [6].

### *5.3.2 Communication Modes in VANET*

VANET communication can be categorized into inter-vehicular communication and vehicle to infrastructure communication. Inter-vehicular communication refers to the kind of communication in which vehicles communicate with each other via wireless technology, also referred to as Vehicle-to-Vehicle communication (V2V) as shown in Fig. 5.1. As Fig. 5.1 illustrates when a vehicle breaks down, immediately, the vehicle begins the information dissemination process using the broadcast communication mode. The vehicles that are near to the vehicle, which has broken down, re-transmit the message. In this way vehicles are notified and can take alternative routes, avoiding a possible problem of traffic congestion.

The second mode of communication refers to communication where vehicles and fixed infrastructure exchange information. This communication mode is referred to

**Table 5.1** A comparison of MANET and VANET

| Parameter | MANET | VANET |
|---|---|---|
| Cost of production | Cheap | Expensive |
| Change in topology | Slow | Very fast |
| Mobility | Low | High |
| Node density | Sparse | Dense and frequently variable |
| Bandwidth | 100 kbps | 1000 kbps |
| Range | Up to 100 m | Up to 500 m |
| Node lifetime | Depends on power resource | Depends on the lifetime of vehicle |
| Multihop routing | Available | Weakly available |
| Moving pattern of nodes | Random | Regular |
| Position acquisition | Using ultrasonic | Using GPS, Radar, etc. |

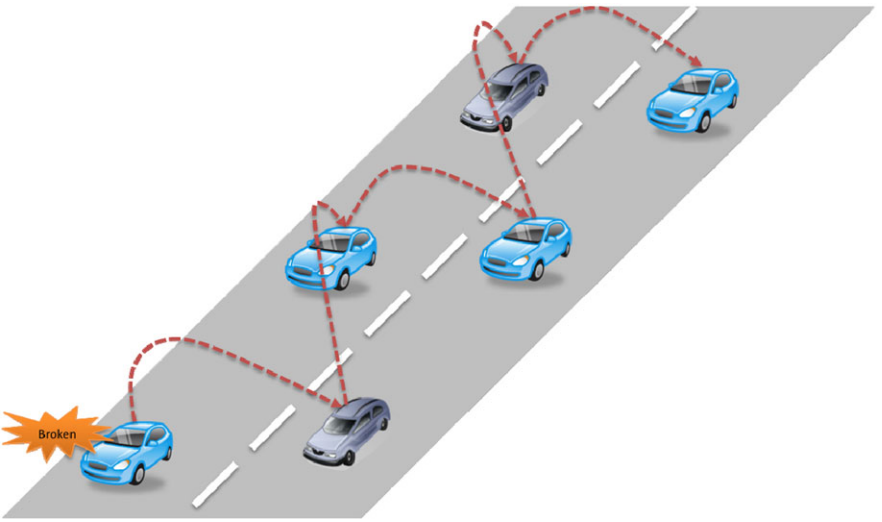


**Fig. 5.1** Vehicle to vehicle communication mode (V2V)

as Vehicle-to-Infrastructure (V2I) or Vehicle to Roadside (V2R) communication. V2I is the direct wireless exchange of relevant information between vehicles and the communication units placed on the side of roads and avenues. Figure 5.2 shows a representation of this kind of communication. In this scenario we observe that when a vehicle is broken down, the vehicle begins the communication with the fixed infrastructure in order to notify the problem. The base station notifies the vehicles that are within its coverage area about the problem identified. At the same time, the base station could begin the inter-roadside communication process to extend the area of coverage. In this way vehicles further away are notified and can take alternative routes, avoiding a potential problem of traffic congestion.

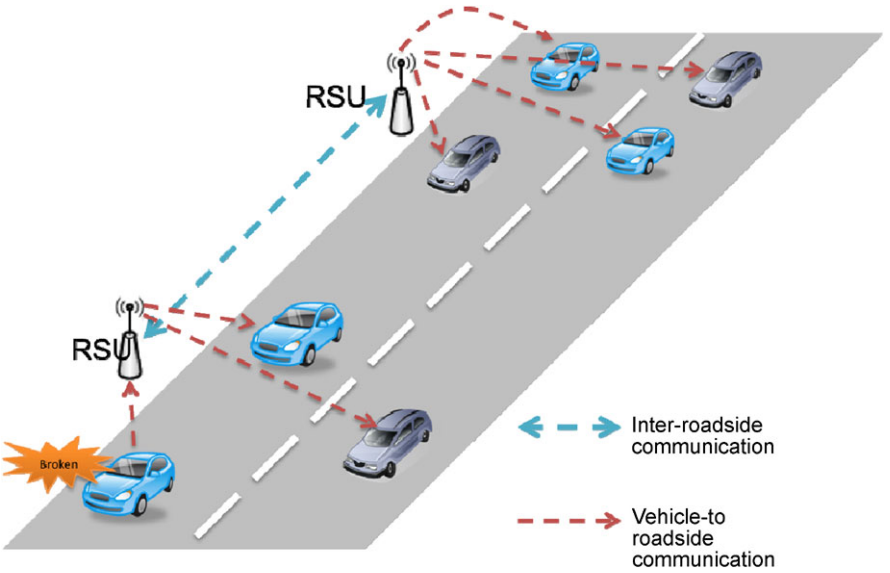


**Fig. 5.2** Vehicle to infrastructure communication mode (V2I)

## 5.4 Vanet Applications and Communication Technologies

### *5.4.1 VANET Applications*

One of the most important challenges that researchers are facing is to satisfy the various requirements associated with VANETs and their applications.

Recent hardware and software advances along with the emergence of VANET have led to the emergence of a wide range of VANET applications. Santa et al. [28] classified vehicular applications depending on the method of communication used [28]. In this case, the authors define three categories: vehicle-to-vehicle, vehicle-to-infrastructure and a combination of both. Another classification method is based on the penetration rate. This method defines two categories: behavior and warning applications [24]. Cooperative behavior applications apply communication technologies for supporting inter-vehicular cooperation schemes for gathering other vehicles information. These applications enhance the perception of the environment through the usage of different on-board sensors. On the other hand, warning applications focus on the dissemination of relevant information, such as traffic conditions and alerts of on-road incidents to improve traffic fluency and safety by preventing and avoiding accidents.

Another classification is based on the application area. According to this classification, applications for vehicular networks are divided into three major groups: safety, infotainment and assistance, and traffic efficiency and management.

- *Safety applications* are those that are employed to minimize the probability of traffic accidents and to avoid collisions situations that most frequently occur be-

tween vehicles and other objects such as animals, trees, and pedestrians. This type of applications relies on real-time information and uses a vehicle-to-vehicle communication scheme. They provide information and assistance to drivers to avoid traffic accidents. Vehicles and roadside units share information, which is then used to predict a dangerous situation. Moreover, this information is used to locate dangerous locations on roads. They use beacon messages, a single-hop position-based or fast-bidirectional communication regime, and their latency cannot exceed 100 milliseconds, whereas the packet delivery ratio cannot be lower than 99 % [24]. Some examples of safety applications include: intersection collision warning, lane change assistance, overtaking vehicle warning, head on collision warning, and emergency vehicle warning.

- *Infotainment and driver assistance applications* provide services such as comfort and driving assistance. This class of applications attempts to support all features needed by drivers and passengers for a convenient travel. Driver assistance applications provide information about repair notifications, remote diagnostics, context information, navigation information, and alerts. These applications usually use vehicle-to-backoffice or vehicle-to-roadside communication. They utilize normal messages and bidirectional communication; their latency cannot be higher than 400 milliseconds, whereas the packet delivery ratio cannot be lower than 95 % [24]. Infotainment applications also are known as in-car comfort entertainment, and they usually do not use inter-vehicular communications. These applications are usually found inside vehicles or at vehicle-to-roadside settings. They use alerts, a multihop position-based communication scheme, and their latency cannot be higher than 400 milliseconds, whereas the packet delivery ratio cannot be lower than 95 % [24]. Applications in this category include cooperative local services and global Internet services.
- *Traffic management applications* capture domain issues such as traffic bottlenecks and fuel consumption amongst others, including environmental issues. These applications focus on improving the vehicle traffic flow, traffic coordination and traffic assistance, and provide updated local information, maps and information of relevance bounded in space and time. This type of time-to-live traffic application is usually used by vehicle-to-backoffice or vehicle-to-roadside scenarios. They may use beacons or alerts, a multihop position-based communication regime, and their latency cannot be higher than 400 milliseconds, whereas the packet delivery ratio cannot be lower than 95 % [24].

### *5.4.2 Communication Technologies in VANET*

VANET applications have different requirements in terms of bandwidth, latency, error rate, and coverage area. These requirements must be satisfied at any time and at any location. It is necessary to evaluate the properties of different existing network access technologies such as Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), cellular networks, and satellite

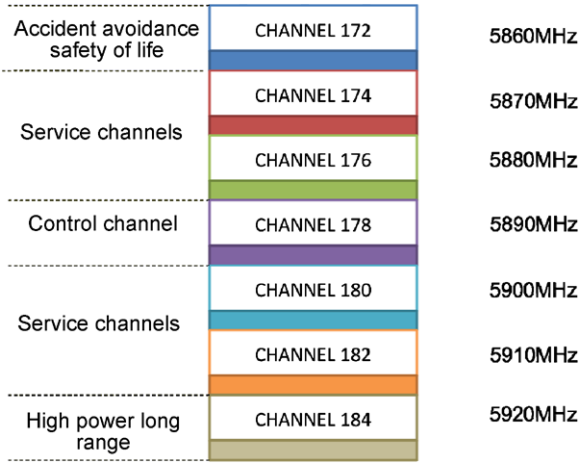


**Fig. 5.3** Channels available in 802.11p

communications. One of the challenges is the selection of the appropriate access technology that can meet the service requirements of the various VANET applications. The 802.11-based WLAN is very popular and it supports fairly high-speed data transmissions but its area of coverage is limited. Even though this technology can reach a data rate of 100 Mbps, its short transmission range leads to frequent interruptions of communications particularly when the speed of vehicles is high making it necessary to deploy an important number of access points along the road.

The 802.11 task force group has been working on the development of a new communication standard known as IEEE 802.11p. This new standard is based on the 802.11a technology and is also referred as the Dedicated Short-Range Communications (DSRC) standard. DSRC uses the 5 GHz frequency spectrum that is divided into seven channels (10 MHz each): one control channel (CCH) and six service channels (SCHs) as shown in Fig. 5.3 [32]. DSRC evolved into Wireless Access in Vehicular Environment (WAVE). WAVE supports high-speed V2V and V2I communications and has major applications in ITS, vehicle safety services, and Internet access. WAVE operates at 5.850–5.925 GHz and adopts Orthogonal Frequency-Division Multiplexing (OFDM) and achieves data rates of 6–27 Mbs/s [34].

Nodes use the control channel to exchange network control messages and the service channels to exchange data packets and WAVE short messages. The link bandwidth of these channels is further divided into transmission cycles. Each cycle comprises a control frame and a service frame. The draft of the IEEE 802.11p standard suggests a frame duration of 50 milliseconds for either a control frame or a service frame. DSRC supports a very high data rate (6–27 Mbps) with a maximum coverage of 1000 m. Some studies have investigated the performance of DSRC for various VANET applications. The results of these investigations have shown that the reliability of DSRC in vehicle-to-vehicle communication is satisfactory for its usage in vehicular safety applications [1, 18].

WiMAX is a technology based on the IEEE 802.16 standard that supports a large geographical coverage (up to 50 km), and offers adequate bandwidth to end-users (up to 72 Mbps theoretically). Even though the IEEE 802.16 standard only supports fixed broadband wireless communication, the versions of the 802.16e and 802.16j standard support speeds of up to 160 km/h and classify the information in several classes of service. In terms of Quality of Service (QoS), WiMAX defines five categories of service. In WiMAX the quality of service is managed by the channel access method. WiMAX makes use of a scheduling algorithm for which the subscriber station needs to compete only once for initial entry into the network. Afterwards, it is allocated an access slot by the base station.

Different performance comparison analyses of 802.11p and 802.16 have been reported demonstrating that the 802.16-based technology offers a wider radio of coverage and higher data rates than IEEE 802.11p. The results also showed that the latency of 802.16 is significantly larger when the communication distance is short (e.g. less than 100 m). However, the results also revealed the strong competitiveness of the 802.16-based technology in the context of vehicle to infrastructure communication [4, 19].

3G cellular wireless technology supports a broad area of coverage and high-mobility. Current third Generation (3G) networks deliver a data rate that ranges from 384 kbps to 2 Mbps for fixed nodes. 3G systems deliver smoother handoffs compared to WLAN and WiMAX systems; however, their main weakness is their latency. The 3G technology usually yields delay values in the order of several hundreds of milliseconds which are too high for critical applications. However, as various studies have shown, cellular networks are able to maintain a regular behavior in latency times [15].

Satellite communication is another technology available for supporting vehicular communications that provides ubiquitous coverage at any location. However, the main problems of networks that utilize this technology are the high costs and large propagation delays. The design of a global platform for vehicular communications is an important challenge. The design of this global platform should be on the basis of intelligent integration of readily available technologies in order to minimize its deployment cost and speed up its deployment. However, the design should also support new emerging technologies. Recent research trends have been focusing on two areas: heterogeneous architectures and multi-interface mobile nodes. Various design of integrated architectures made up of different technologies interconnected using an ad-hoc communication model have been proposed recently [22, 35]. For multi-interface mobile nodes, the usage of several radios in the OBU to enhance the performance of the network has been investigated.

## 5.5 Routing Protocols in VANET

As VANETs become more complex, transporting information from one vehicle to another or to all vehicles within a given region or area becomes a highly challenging

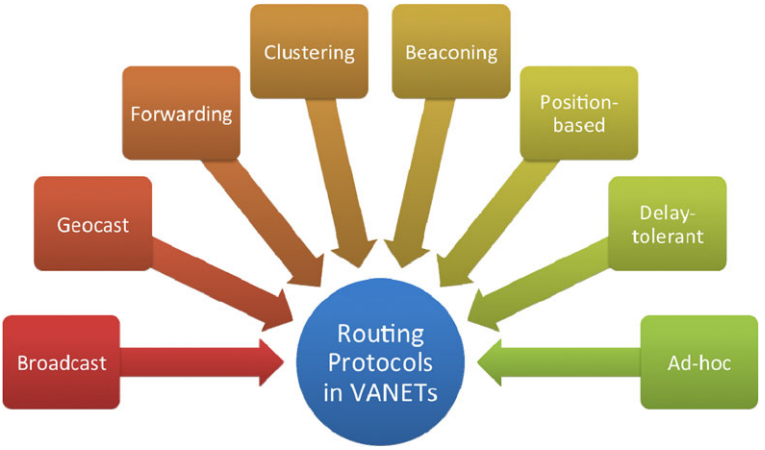


**Fig. 5.4** Classification of VANET routing protocols

task. A lot of research has been carried out to develop protocols and mechanisms that can provide network services (e.g. routing) to applications in a VANET environment. Several classifications of the various routing protocols for transporting information have been proposed in the literature [16, 20, 36]. Figure 5.4 shows a summary of some of the recently proposed routing protocols for VANETs.

### *5.5.1 Broadcast Routing Protocols*

The Broadcast routing approach is generally used for disseminating information on a large scale. This information can be traffic, weather, emergency, and road conditions. This communication scheme sends packets to all nodes in the network using flooding (Fig. 5.5). When messages need to be disseminated beyond the radio transmission range, a multihop mechanism is utilized. Thus, in a native broadcast implementation, all receiving nodes simply rebroadcast the received messages. To limit message duplication, nodes broadcast messages only once, and a time to live parameter can be utilized to limit the area of coverage of messages. Using this routing scheme, the delivery of messages to all nodes is guaranteed. However, a large amount of bandwidth is consumed and is the reason why this routing scheme only performs well when a small number of nodes is participating within the VANET and its performance drops quickly when the size of the network increases.

### *5.5.2 Geocast Routing Protocols*

Geocast is a multicast routing approach that delivers messages to nodes located within a given geographical region (Fig. 5.6). These routing protocols generally

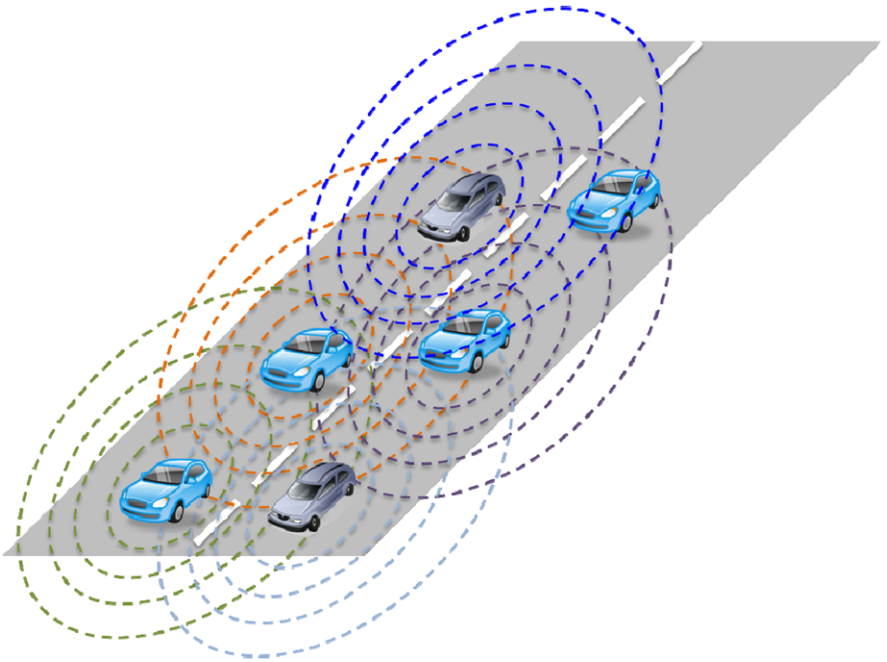

**Fig. 5.5** Broadcast routing protocol

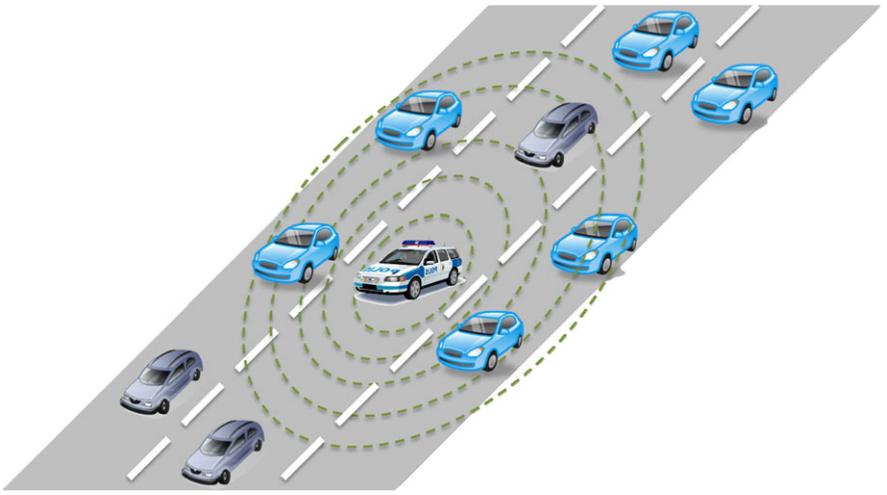

**Fig. 5.6** Geocast routing protocol

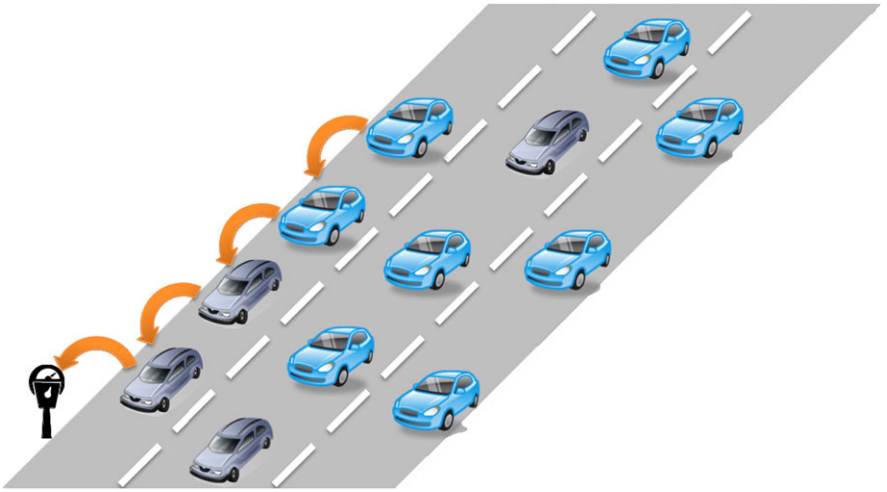

**Fig. 5.7** Forwarding routing protocol

define a forwarding zone that limits the flooding of messages. Using this routing scheme it is possible to, for instance, report an accident to vehicles located within a given region or alert a driver when driving on a motorway in the wrong-way.

### *5.5.3 Forwarding Routing Protocols*

The forwarding routing approach transports messages between two nodes via multiple hops (Fig. 5.7). This mechanism is useful when the requested information is only of interest to a few nodes. For example, a node may request information to a nearby car parking about free car parking spaces and fees. When a node is requesting information, a unicast message is sent. To forward the message to its destination a route is reactively constructed, for example, by looking at local routing tables or by asking nearby nodes whether they know about the destination node.

### *5.5.4 Cluster-Based Routing Protocols*

The cluster-based approach groups nodes located within a given region (e.g. nodes with direct link to each other). For each cluster, a cluster head node is selected which is responsible for managing inter and intra-cluster communication (Fig. 5.8). The cluster-based structure functions as a virtual network infrastructure whose scalability favors routing and media access protocols although an overhead cost is incurred when forming clusters in highly mobile network environments and network delays may occur for large networks.

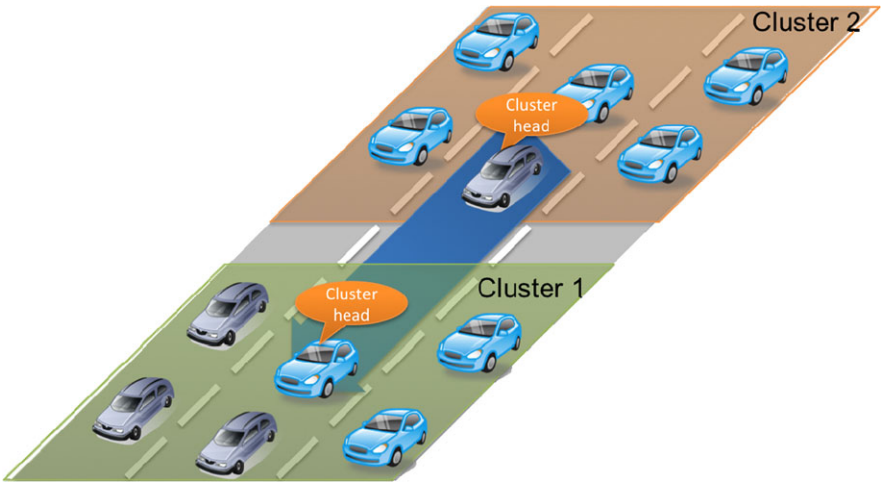


**Fig. 5.8** Cluster-based routing protocol

### *5.5.5 Beaconing Routing Protocols*

The Beaconing routing mechanism is suitable for applications that require sharing information with other vehicles periodically (e.g. the exchange of local traffic information). In this routing scheme a node announces information periodically and the receiving nodes do not rebroadcast the received message immediately. Instead, they store the received information in their local information caches. On the next beacon, a message is constructed using both information from the local cache and the incoming information and is rebroadcast to neighboring nodes.

### *5.5.6 Position-Based Routing Protocols*

For Position-based routing to work, information on the location of each node is fundamental. To decide on how to route messages, nodes utilize geographical location information obtained from sources such as street maps, traffic models and on-board navigational systems (Fig. 5.9). Routing decisions at each node are made by taking into consideration the position of the destination node and each node's location information. As routing tables are not required, no overhead is incurred on maintaining and establishing routes.

### *5.5.7 Delay-Tolerant Routing Protocols*

The Delay-tolerant routing mechanism is used where the density of vehicles is really low and consequently establishing end-to-end routes is not possible. For example at

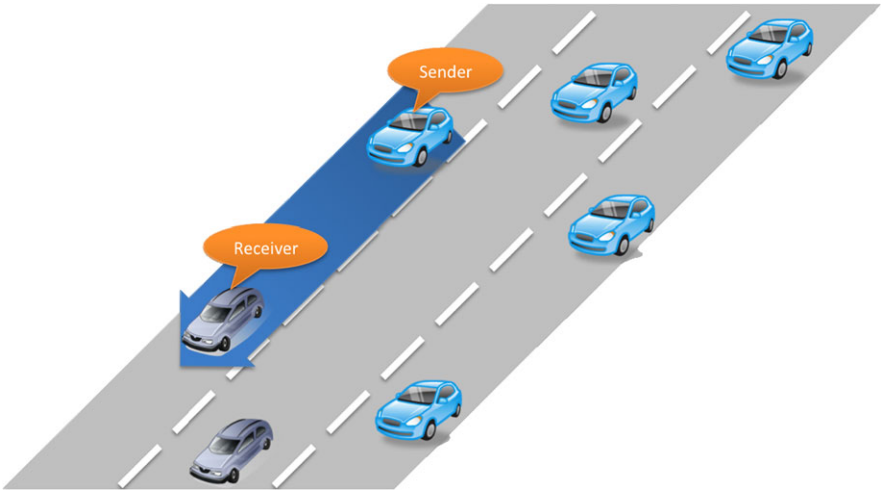


**Fig. 5.9** Position-based routing protocol

nights, traffic in cities can be really low and available vehicles may not be close enough to receive and forward messages. Also, in rural areas vehicle density may be low and, for such sparse networks, a delay-tolerant protocol can be utilized. This routing mechanism is based on the concept of carry and forward, where a node carries messages and these are only forwarded when another node moves into its vicinity, otherwise, they are simply stored.

### *5.5.8 Ad-hoc Routing Protocols*

Ad-hoc routing protocols were initially designed to operate in Mobile Ad-hoc Networks (MANET) environments. VANET attempts to test these routing protocols in such new environments have been carried out [17, 26]. However, requirements (such as unique address identification) of these address-based and topology-based mechanisms make these protocols less suitable for VANETs.

## 5.6 Security in VANET

As VANET becomes more ubiquitous in the near future, a serious challenge in this environment is security. As we mentioned previously, VANET is a special implementation of MANET. Consequently, VANETs inherit all the security issues associated with MANETs. The malicious behavior of users, such as the modification of the disseminated messages, could be fatal to the other vehicular users.

Security and privacy in vehicular networks are important prerequisites for their acceptance. VANETs' architectures and communication schemes will provide developers an environment for the deployment of a wide variety of applications. However, major concerns of such environments are security and privacy. To protect both applications and users from possible attacks, strong security mechanisms are required. Therefore, robust schemes are needed to protect users' private information. For example, user-related privacy information such as driver's name, license plate, speed, position, must be protected and only accessed by authorized users. Such information should be shared by entities that satisfy a set of required privacy and authentication requirements. VANETs' security is of great importance because any vulnerability could lead to disastrous accidents where people's integrity may be put at risk.

Security mechanisms and schemes must guarantee the protection of personal data transmitted through VANET including but not limited to identity, location, and destination, among others. In this context, various authors have recently published in the literature some of the possible security and privacy threats in VANETs [14, 23, 25, 27]. We summarize below some of these threats.

- *Denial of service*: An attacker may intentionally prevent communication of vehicles located within its communication range by jamming their communication (for instance, generating interfering transmissions or selectively erasing messages). This attack may prevent the delivery of important information to the intended destination. In the case of a denial of service attack, vehicles may not be able to receive messages from a vehicle alerting of an accident ahead.
- *Impersonation*: A vehicle within a VANET may pretend to be or act as a special type of vehicle (e.g. ambulance or patrol car) or infrastructure (e.g. roadside unit) spoofing traffic or safety messages. Examples of techniques that can be utilized towards impersonation include message fabrication, alteration and replay. An attacker impersonating a roadside unit, for instance, may contaminate the network fabricating false safety alarms.
- *Privacy violation*: To prevent spoofing attacks (such as a Sybil attack when an entity masquerades as multiple, simultaneous identities) a mechanism to bind each vehicle driver within the VANET to a single identity could be utilized. A strong authentication scheme like this could be used to provide forensic evidence to traditional law enforcement approaches and prevent attacks on vehicular networks. However, such a system may also result in drivers abandoning their anonymity and exposing valuable information to attackers. The frequent exchange of messages containing sensitive personal data such as location, trip details, vehicle identification, and e-payment information among others pose a high risk to privacy violations, as attackers can potentially overhear messages and misuse the information contained in them.
- *On-board and in-transit traffic tampering*: On-board units are susceptible to attacks from outsiders whom may attempt to alter sensed data such as speed or location. Similarly, attackers may manipulate critical in-transit traffic information corrupting or dropping overheard messages.

### 5.6.1 Security and Privacy Challenges

The unique characteristics of VANETs such as fast mobility of nodes, frequent changes in topology, self-organization of nodes and user requirements make it challenging to guarantee security and privacy. As we mentioned earlier, VANET is highly susceptible to different types of attack and adversary (e.g. greedy drivers, snoops and pranksters). To support and protect VANET applications various security and privacy challenges must be addressed. To address these security and privacy challenges the following design principles have been proposed [23, 25].

- *Default network access*: Messages broadcasted should be accessible to all nodes that can receive them, and, all nodes must assist in enabling multihop communication.
- *Authenticated localization of message origin*: Vehicular applications must be able to determine the origin of a message at a given location. With the exception of the originator, nodes should not be able to modify messages and receivers must corroborate the message's sender.
- *Visibility of events*: In the case of distributed protocols, events that trigger joint computations or actions must be visible to or attested by all participating nodes (e.g. neighboring nodes). To attest messages, a node is either responsible for the generated event or has locality and timeliness privileges such as the reception of the message within a given time interval from its generation.
- *Mandated (non-circumventable) mediation*: All actions that impact on the security state of the network (e.g. node identification scheme and authentication mechanism) must be mediated by a network authority and should not be bypassed or avoided by any node.
- *Accountability*: Protocol executions and messages that can have an impact on substantial functions of the network (e.g. an alert message notifying of a vehicle failure) should be subject to auditing.
- *Vehicle autonomy*: With the exception of mediated messages and protocols VANET applications can be autonomous with respect to other nodes. For example, messages from other nodes can be rejected.
- *Separation of privilege*: Security, privacy and fault-tolerance systems must be distributed among multiple authorities. Each authority must be in charge of one activity and should only have the rights necessary to complete the designated task.
- *Liability and faulty behavior*: A node causing deliberate or accidental actions that disrupt the operation of the VANET must be legally responsible for its actions and it should be possible for authorities to identify such a node. As the faulty behavior could be intentional or as a result of network or nodes' failures, authorities could utilize a staged response mechanism where penalties may range from a warning notification at the first stage to an eviction from the system at the last stage.
- *Privacy*: Personal data such as the identity of the driver and the vehicle, location, speed, and traveling routes must be protected. Nevertheless, as mentioned in the liability and faulty behavior principle, authorities must be capable of identifying messages' senders in case of an accident or violation of legal regulations.

- *Availability*: Regardless of faults or malicious conditions, the network and applications must remain operational. This implies that the design of protocols and applications should be secure, fault-tolerant and resilient to attacks.
- *Trust*: Data should not be altered and they should be truthful. False or modified data could lead to potential problems such as crashes, bottlenecks, and other traffic safety problems. For this reason, trusted information must be provided in all VANET communications.

## 5.7 Challenges and Opportunities

Emerging technologies applied to vehicular networks face several challenges. The development of ITS brings new challenges to vehicle driving, controlling and monitoring. In this context, the vehicular network's vision is focused on four fundamental principles: sustainability, integration, safety, and responsiveness as shown in Fig. 5.10 [21].

Vehicular networks will play a major role in promoting and ensuring the sustainability of transport infrastructures. Emerging technologies can facilitate the efficient use of existing transportation infrastructures, regulate and control demand, encourage and facilitate the use of alternative communication modes, and manage congestion and its effects.

Management tools such as electronic tolling, traveler information, and intelligent traffic lights are all based on ITS, and constitute the core of demand management solutions that support transport infrastructure sustainability. Moreover, through a more efficient management of traffic on existing roads, VANET facilities can delay or deny the need of new infrastructures adding to the sustainability of all transportation infrastructures.

However, the current challenge is not the use of VANET and emerging technologies, but developing mechanisms and protocols that allow a complete integration of the different technologies to provide a seamless mechanism to disseminate and access accurate information, facilitating the management of transportation systems and addressing the transportation issues such as traffic congestion and vehicular accidents. In this context, the typical ITS based on discrete and self-contained systems need to evolve towards systems that are based on heterogeneous technologies.

One of the main challenges of VANET and ITS is the compatibility and portability of systems. For example, a collision avoidance system is of limited use if vehicles cannot successfully communicate because of interoperability issues between communication protocols and network devices. Standards are clearly necessary to achieve these objectives.

In the last few years, significant efforts have focused on developing international standards in specific areas such as architectural design; database technology, automatic vehicle and equipment identification, fee and toll collection, general fleet management and commercial-freight, public transport-emergency; integrated transport Information, management and Control, traveler information sys-

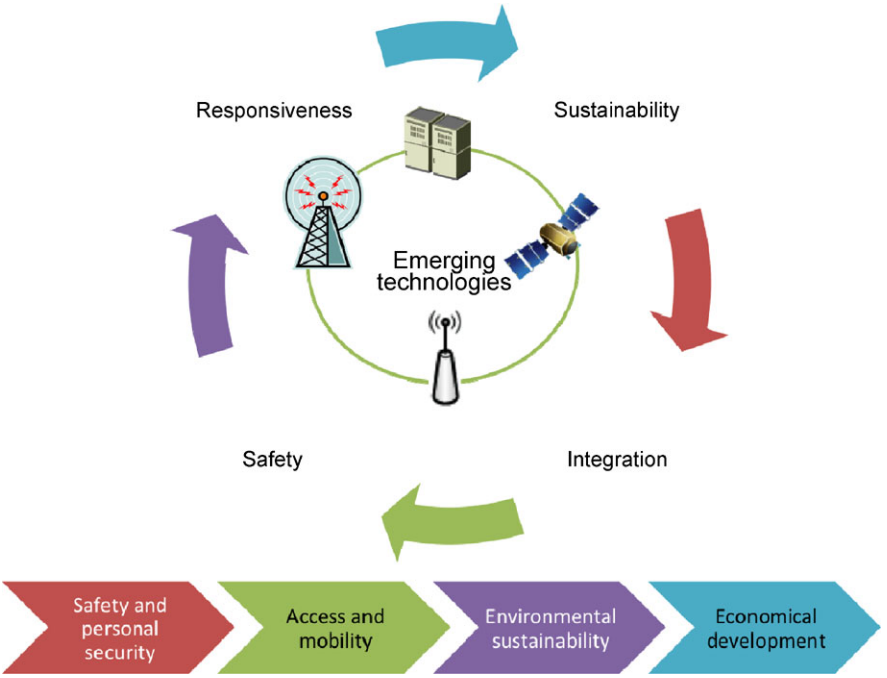


**Fig. 5.10** Principles and objectives of emerging technologies in the transportation

tems; route guidance and navigation systems, vehicle-roadway warning and control systems, DSRC, and wide area communications—protocols and interfaces [33]. The International Organization for Standardization (ISO) has been developing ITS standards since 1994 [30], and the European Committee for Standardization (ECS) since 1991 [7]. The main focus of new developments is the integration of emerging technologies and their generic communications standards such as 2G, 3G, Wi-Fi, Bluetooth and WiMAX in order to create the new generation of standards that allow vehicle-vehicle (V2V)/vehicle-infrastructure (V2I) systems to operate within a heterogeneous communication environment by integrating most of the major vehicle manufacturers, transport management system providers and operators, and highway infrastructure operators.

In this context, ISO has been developing a new communication framework, known as the Communications Access for Land Mobiles (CALM) initiative. CALM is the ISO approved framework for heterogeneous packet-switched communication in mobile environments. CALM focuses on providing a layered solution that enables continuous or quasi-continuous communications between vehicles and the infrastructure, or between vehicles, using wireless communications that are available in any particular location, and has the ability to migrate to different available media when needed [9].

The ISO TC204 Work Group 16 is developing a family of International Standards based on the CALM concept. This family of standards specifies a common

architecture, network protocols and communication interface definitions for wired and wireless communications using various access technologies including cellular 2G, 3G, satellite, infra-red, 5 GHz microwave, 60 GHz millimeter-wave, and mobile wireless broadband. These and other access technologies that can be incorporated are designed to provide broadcast, unicast, and multicast communications between mobile stations, between mobile and fixed stations, and between fixed stations in the ITS sector [11].

ISO 21217 describes the common architectural framework around which CALM-compliant communication entities (called ITS stations) are instantiated, and provide the architectural reference for use by the CALM family of International Standards including the lower layer service access point specifications described in the network protocol specifications (IPv6 networking and non-IP networking), and the ITS station management specifications.

## 5.8 Conclusion

One of the major priorities for many governments around the world is to define mechanisms and schemes that could help solve traffic problems that modern society faces. Recent technological advances have led to the development and usage of integrated intelligent systems. We have presented how the different emerging technologies could be applied to transportation systems in order to solve the traffic problems that modern society is facing. In the last few years a suite of systems and applications for vehicular communications has emerged. This suite includes applications that can be utilized for improving vehicular safety, enhancing traffic control, improving driver efficiency, and making it more comfortable for passengers inside vehicles. In addition, many of the emerging technologies are also enabling the development of transportation systems that are capable of optimizing fuel consumption, minimizing traffic congestion, reducing carbon dioxide emissions, and, more importantly, reducing human casualties.

In addition, there are several private and public initiatives that have been launched that are dedicated to the development and research of vehicular systems. The inherent characteristics of VANETs in terms of, for example, its dynamic network topology, mobility patterns, low latency, among others, development and make the deployment of vehicular applications still a challenge. In this chapter we have identified some of the challenges that vehicular networks face and need to be addressed.

The successful development of VANET technologies and applications depends on VANET standards that enable the integration of heterogeneous systems. We need to continue to promote users' acceptability and accessibility to vehicular applications and technologies. Finally, to guarantee the privacy and security of VANET users, novel secure architectures and protocols still need to be developed in the future.

**Acknowledgements** We thank the anonymous reviewers for their comments, which helped us to improve the quality and presentation of this chapter. Sherali Zeadally was partially supported by a

District of Columbia NASA Space Grant and an NSF TIP grant (Award Number 1036293) during the course of this work.

## Appendix: List of Acronyms

CALM: Communications Access for Land Mobiles
DGP: Gross Domestic Product
DSRC: Dedicated Short-Range Communications
ECS: European Committee for Standardization
IEEE: Institute of Electrical and Electronics Engineers
ISO: International Organization for Standardization
ITS: Intelligent Transportation Systems
ITSA: Intelligent Transportation Society of America
MANET: Mobile Ad-hoc Networks
OBU: On-Board Unit
OFDM: Orthogonal Frequency-Division Multiplexing
QoS: Quality of Service
RSU: RoadSide Unit
VANET: Vehicular ad-hoc Networks
V2I: Vehicle-to-Infrastructure
V2R: Vehicle-to-Roadside
V2V: Vehicle-to-Vehicle
WAVE: Wireless Access in Vehicular Environments
WiMAX: Worldwide Interoperability for Microwave Access
WLAN: Wireless Local Area Network
3G: Third Generation

## References

1. Bai, F., & Krishnan, H. (2006). Reliability analysis of DSRC wireless communication for vehicle safety applications. In *IEEE intelligent transportation systems conference 2006*, Toronto (pp. 355–362).
2. Bakas, L. (2008). Transport and greenhouse gas emissions. Retrieved from CORPUS, The SCP Knowledge Hub: http://www.scp-knowledge.eu/sites/default/files/Poster%20GHG.pdf.
3. Barth, M., & Boriboonsnmsin, K. (2009). *Traffic congestion and greenhouse gases* (Technical report). http://www.uctc.net/access/35/access35_Traffic_Congestion_and_Grenhouse_Gases.pdf
4. Chou, C., Li, C., Chien, W., & Lan, K. (2009). A feasibility study on vehicle-to-infrastructure communication: WiFi vs. WiMAX. In *Tenth international conference on mobile data management: systems, services and middleware*. Washington: IEEE Comput. Soc.
5. Commission for Global Road Safety (2009). Make roads safe, a decade of action for road safety. http://www.makeroadssafe.org/publications/Documents/decade_of_action_report_lr.pdf.
6. Dahiya, A., & Chauhan, R. K. (2010). A comparative study of MANET and VANET environment. *Journal of Computing*, *2*(7), 87–92.

7. ECS (2005). *TS 17261: intelligent transport system—automatic vehicle and equipment identification—intermodal good transport architecture and terminology*. Brussels: Comité Européen de Normalisation.
8. ERTICO (1998). *Intelligent city transport: a guidebook to intelligent transport system*. Brusells: ITS ERTICO. ITS CITY Pionners Consortium.
9. Evensen, K. (2006). In *Proceedings of secure vehicular communications workshop*, EPFL, Lausanne, Switzerland, February 2006.
10. IEEE-SA Standards Board (2009). *IEEE standard for local and metropolitan area networks Part 16: air interface for broadband wireless access systems*. New York: IEEE Comput. Soc./IEEE Microwave Theory Techniq. Soc.
11. ISO TC204 (2008). ISO TC204 WG16 CALM. http://www.calm.hu.
12. ITS Japan (2010). ITS Japan. http://www.its-jp.org/english/.
13. ITSA (2011). ITSA—Intelligent Transportation Society of America. http://www.itsa.org.
14. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys and Tutorials*, *13*(4), 584–616.
15. Landman, J., & Kritzinger, P. (2005). Delay analysis of downlink IP traffic on UMTS mobile networks. *Performance Evaluation*, *62*(1), 68–82.
16. Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: a survey. *IEEE Vehicular Technology Magazine*, *2*(2), 12–22.
17. Lin, Y., Chen, Y., & Lee, S. (2010). Routing protocols in vehicular ad hoc networks: a survey and future perspectives. *Journal of Information Science and Engineering*, 913–932.
18. Ma, X., Chen, X., & Refai, H. (2009). Performance and reliability of DSRC vehicular safety communication: a formal analysis. *EURASIP Journal on Wireless Communications and Networking*, *2009*, 969164.
19. Msadda, I., Cataldi, P., & Filali, F. (2010). A comparative study between 802.11p and mobile WiMAX-based V2I communication networks. In *Fourth international conference on next generation mobile applications, services and technologies* (pp. 186–191). Washington: IEEE Comput. Soc.
20. Nundloll, V., Blair, G., & Grace, P. (2009). A component-based approach for (re)-configurable routing. In *Proceedings of 8th international workshop on adaptive and reflective middleware, VANETS*, Illinois, USA.
21. NZ Transport Agency (2007). Planning policy manual—for integrated planning & development of state highways (versión 1). http://www.nzta.govt.nz/resources/planning-policy-manual/ppm.html.
22. Pack, S., Rutagemwa, H., Shen, X., Mark, J., & Park, K. (2007). Efficient data access algorithms for ITS-based networks with multihop wireless link. In *IEEE international conference on communications* (pp. 4785–4790). Glasgow: IEEE.
23. Parno, B., & Perrig, A. (2005). Challenges in securing vehicular networks. In *Proceedings of the workshop on hot topics in networks*. New York: ACM.
24. Popescu-Zeleti, R., Radusch, I., & Rigani, M. (2010). *Vehicular-2-X communication*. Berlin: Springer.
25. Qian, Y., & Moayeri, N. (2008). Design of secure and application-oriented VANETs. In *IEEE VTC (vehicular technology conference) 2008*. Singapore: IEEE.
26. Rani, P. (2011). Performance comparison of VANET routing protocols. In *7th international conference on wireless communications, networking and mobile computing* (pp. 1–4). Wuhan: IEEE.
27. Raya, M., & Hubaux, J. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.
28. Santa, J., & Gomez-Skarmeta, A. F. (2008). Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. *Computer Communications*, *31*(12), 2850–2861.
29. Schrank, D., Lomax, T., & Turner, S. (2010). TTI's Urban Mobility Report. http://mobility.tamu.edu/ums/report/.

30. TC204 (2006). *Intelligent transport systems—system architecture, taxonomy and terminology—procedures for developing ITS deployment plans utilising ITS system architecture*.
31. UNFPA (2007). *State of World Population 2007: Unleashing the potential of urban growth* (Technical Report). United Nations Population Foundation. http://www.unfpa.org/swp/2007/presskit/pdf/sowp2007_eng.pdf.
32. Wang, S., Chou, C., & Lin, C. (2010). The GUI user manual for the NCTUns 6.0 network simulator and emulator. User manual, National Chiao Tung University, Network and System Laboratory, Department of Computer Science, Taiwan.
33. William, B. (2008). *Intelligent transport systems standards*. Norwood: Artech House.
34. Xiang, W., Gozalvez, J., Niu, Z., Altintas, O., & Ekici, E. (2008). Wireless access in vehicular environments. *EURASIP Journal on Wireless Communications and Networking*, *2009*, 576217.
35. Yang, K., Ou, S., Chen, H., & He, J. (2007). A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks. *IEEE Transactions on Vehicular Technology*, *56*(6), 3358–3370.
36. Zeadally, S., Hunt, R., Chen, Y., Irwin, A., & Hassan, A. (2010). Vehicular ad hoc networks (VANETS): status, results, and challenges. *Telecommunications Systems*, *50*(4), 217–241.