4

Emerging Technologies for Urban Traffic Management

Antonio Guerrero-Ibáñez, Carlos Flores-Cortés,
Pedro Damián-Reyes, M. Andrade-Aréchiga and J. R. G. Pulido
School of Telematics, University of Colima, Colima, México

1. Introduction

Nowadays, the number of vehicles on the road and the need of transporting people grow fast. Road transportation has become the backbone of industrialized countries. Nevertheless, the road network system in cities is not sufficient to cope with the current demands due to the size of roads available. Building additional or extending existing roads do not solve the traffic congestion problem due to the high costs and the environmental and geographical limitations. As a consequence, the modern society is facing more traffic jams, higher fuel bills and high levels of CO2 emissions.

Vehicular traffic is one of the most critical concerns of modern societies where cities are ever growing. The *United Nations Population Foundation* published in its technical report (UNFPA, 2007) that for the first time, more than half the world's population lives in urban areas and the balance of people continue shifting to the cities. As a consequence, drivers and passengers spend a large percentage of their day stuck in traffic.

Traffic congestion in urban areas is a serious problem that has an important economical, environmental and road safety impact. The technical report of the *Texas Transportation Institute* shown that in 2010 traffic congestion represented an $101 billion annual drain on the U.S. economy, with 4.8 billion hours and 1,9 billion gallons of fuel spent on traffic, the equivalent of one work week and three weeks worth of gas every year (Schrank et al., 2011). According to the *Intelligent Energy Europe* in the European Union (EU), traffic congestion costs $50 billion per year or 0.5% of the community Gross Domestic Product (GDP), and by 2010 this figure could go up to 1% of EU GDP.

Therefore, traffic congestion has an important environmental impact. According to the technical report on traffic congestion and greenhouse gases (Barth & Boriboonsonsim, 2009) a third of America carbon dioxide (CO_2) emissions come from moving people or goods, and 80 percent of these emissions are from cars and trucks. According to the Eurostat data, road transport accounted for 19.5% of the EU total greenhouse gas emissions in 2008 (Bakas, 2008).

On the other hand, regarding road safety impact, 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. Significantly, 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 (Commission for Global Road Safety, 2009).

It is essential to improve the safety and efficiency of transportation. Several research groups focus their attention on the emerging technologies as a feasible alternative to solve the traffic and transportation problems. The primordial objective is that emerging technologies can contribute to the solution of transportation issues by making transport safer, more efficient and competitive, more sustainable and more secure.

In this way, emerging technologies are established as basic elements of transportation systems. The increasing capacity and flexibility of emerging technologies could make it possible to create cooperative automotive systems and reduce investment, operational costs and accidents, making more efficient transport systems. Emerging technologies must guarantee the required demands of transportation systems. Communication technologies should be used to build vehicular networks to reduce traffic congestion and improve safety. Safety and efficiency on roads can be substantially improved with the deployment of intelligent systems such as adaptive traffic control, incident detection and management systems both in cities and highways. To enable these systems, vehicles must be equipped with wireless radios and communication devices must be placed on the roadsides. Roadside units can be utilized to extend the network coverage, enabling communication between distant vehicles (i.e. beyond its radio range), support a high-speed and low-latency network and provide services to both public and private companies. In this sense, recent advances in technology, particularly in the areas of mobile computing, a new generation of wireless ad-hoc networks, which is named *Vehicular Ad-hoc Networks* (VANETs), is emerging. In this kind of network vehicles could communicate with each other on the road and the intention of this network is to solve traffic problems by means of *vehicular to vehicular* communication (V2V) and *vehicular to infrastructure* communication (V2I) as shown in figure 1. For this communication, some devices known as *on-board units* (OBUs) must be placed at each vehicle. These devices can send or receive data to or from *roadside units* (RSUs). Nevertheless, if a vehicle cannot directly send its data to an RSU, it can relay its data to other vehicles until the data reach to the RSU using a multihop transmission strategy (Yang et al., 2007).

In the near future, it is expected that urban and vehicular networks will co-exist and be interconnected for exchanging and sharing of information and services. This mixture of networks represents an important opportunity for optimizing traffic flow in urban areas, improving urban transportation services, and monitoring the environment. However, in order to enable interconnectivity between these networks and support the development and deployment of such type of applications there still exist important challenges in terms of heterogeneity, security, privacy, quality of services and scalability that need to be overcome.

It is being proposed to accelerate and coordinate the deployment and use of vehicular networks applications and services for road transportation and their connections with other modes of transport, to ensure seamless access and continuity of services. Some areas involved in this integration are: optimal use of road and traffic data, traffic and freight management, road safety and security, integrating vehicular networks applications in the vehicle, data protection and liability. The direct benefit will be a faster, better-coordinated

and more harmonious use of intelligent transportation systems and services, which in turn will contribute to more efficient, cleaner and safer transportation.

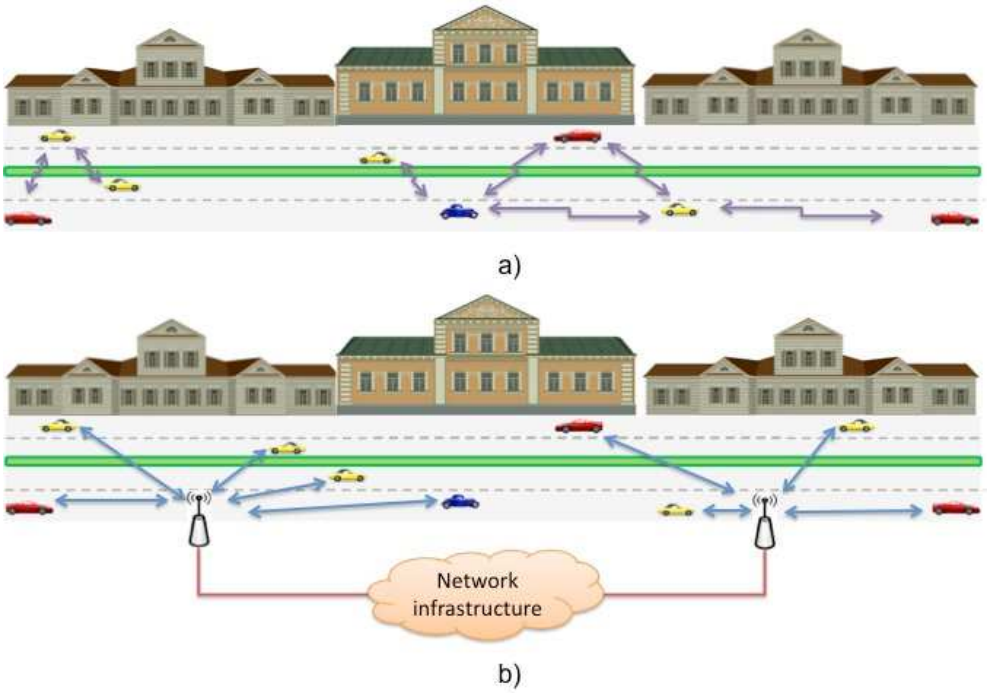

Fig. 1. Communication modes for VANET a) vehicle-to-vehicle mode (V2V) and b) vehicle-to-insfrastructure mode (V2I).

This chapter gives the readers a global vision of traffic and transportation issues and how the application of emerging technologies might contribute to the solution of transportation challenges. The chapter is organized as follow: The first section of the chapter provided a global view of traffic and transportation issues. The second section of the chapter provides an overall view of the fundamental challenges of vehicular networks and their applications. The third section presents a global analysis of the emerging technologies that can be used in the vehicular communications. Finally, the last part of the chapter describes several sensing platforms for collecting information about traffic conditions.

2. Challenges of vehicular networks

In comparison to other communication networks, vehicular communication networks come with some unique attractive features: unlimited transmission power, predictable mobility and plethora of potential applications. However, vehicular networks have to cope with some important challenges that include: 1) extreme heterogeneity, 2) rapidly changing topology subject to frequent fragmentations and congestion, 3) the stringent application requirements on real-time and robust message delivery, 4) security of the information and users. In this section of the chapter we analyse some of these challenges that the vehicular networks face.

2.1 Extreme heterogeneity

VANETs are an important component of any Intelligent Transportation System (ITS) and a promising environment to support a number of safety, driving and entertainment applications. However, to support such applications important heterogeneity challenges need to be overcome:

- *Wireless technologies.* Existing network technologies are different in terms of geographical coverage, data transfer rate, transmission range and supported content types. Thus, a vehicle using one network technology may not be able to communicate with a vehicle using a different technology. Even tough most on-board devices utilize the 802.11p standard; VANET applications would require to interact with nodes or networks utilizing a different technology. For example, a VANET application may require interacting with a wireless sensor network dedicated to manage traffic lights using the Zigbee technology or to gather data from on-board sensors or devices using Bluetooth.
- *Routing protocols.* Recently, many VANET routing protocols have been proposed (Li & Wang, 2007), these protocols have important differences in the mechanims they utilize as many of them target at different VANET environments. For example, some of them consider highly populated environments whereas others are optimized to operate in sparse networks. These differences mean that additional mechanisms are necessary to enable interoperability among heterogeneous routing protocols. The research community has already identified this problem and possible solutions have been investigated (Nundloll et al., 2009).
- *Sensors*. In future VANET scenarios different on-board and roadside sensor will be available. On-board sensors will be utilized to capture different vehicle, driver or surrounding parameters whereas roadside sensors will help gather road conditions affecting driving safety (e.g. big holes, thick ice, malfunctioning cars). All this information is important not only for driver in the vehicle but also for neighbouring drivers. However, sensors accuracy, measurement units, among others may vary from one manufacturer or model to another. Thus it is necessary to further investigate mechanisms that allow to correctly exchanging sensed data.
- *On-Board Units (OBU).* Some manufacturers have started to release to the market different on-Board units. Telargo[1], Kapsch[2] and Efcon[3] are examples of such manufacturers. These units offer different capabilities (e.g. positioning, communication, I/O features, sensors) and use different software platforms. This heterogeneity is a clear concern for developers as developing an application that can be deployed on different on-Board-units may be too difficult or in some cases not possible.

2.1.1 Standards

VANETs standards are important for applications as they guarantee interconnectivity and interoperability. Connectivity is an important characteristic of wireless networks. In the Internet model paths between two nodes are always there. In VANETs is not the case.

[1] http://www.telargo.com/overview/technology/on_boardequipment/obu.aspx
[2] http://www.kapsch.net/cl/en/ktc/portfolio/products_components/Pages/on-board_units.aspx
[3] http://www.efkon.com/en/products-solutions/ITS/gnss-onboard-unit.php

Mobility is to be considered especially as the path becomes sparser. Regarding operability heterogeneous protocols are also to be considered. For instance in pocket switch network the capabilities and behaviour of the sensors vary largely. Two standards are described in turn (Zeadally et al., 2010; Spyropoulos et al., 2010):

- **Dedicated Short Range Communication (DSRC)** short to medium range service for vehicle-to-vehicle and –roadside communications. It provides high data transfers and low communication latency in small communication zones.
- **Wireless Access in Vehicular Environments (WAVE)** a universal standard as the DSRC effort of the ASTM E2213 working group migrated to the IEEE 802.11 standard group. It works at the media access control and physical layers and enables communications even for vehicles coming from opposite directions.

In (Ma et al., 2009) some additional evaluations procedures are presented as alternatives for analyzing vehicular traffic.

2.2 Application requirements for VANET

Covering the whole requirements for vehicular networks and their applications is imperative for carrying out in an efficient and effective way their functions. As new advances in hardware and software communication technology emerge, new applications are enabled in different contexts including vehicular networks.

2.2.1 Classification of applications for VANET

Vehicular software applications may be categorized into four groups (Popescu-Zeletin et al., 2010):

- *Safety* related to the different kinds of collisions that most frequently occur between vehicles and other objects such as animals, trees, and pedestrians. This kind of real-time proactive application usually is vehicle-to-vehicle. They use beacon messages, a single-hop position based or fast-bidirectional communication regime, their latency cannot be higher than 100ms, whereas the packet delivery ratio cannot be lower than 99%.
- *Assistance* provides features such as repair notifications, remote diagnostics, context information, navigation facts, and alerts. This type of time-to-live provider application usually is vehicle-to-backoffice or vehicle-to-roadside. They use normal messages, bidirectional communications; their latency cannot be higher than 400ms, whereas the packet delivery ratio cannot be lower than 95%.
- *Resource* captures domain issues such as traffic bottlenecks and fuel consumption amongst other, including environmental issues. This type of time-to-live traffic application usually is vehicle-to-backoffice or vehicle-to-roadside. They may use beacons or alerts, a multi-hop position based communication regime, and their latency cannot be higher than 400ms, whereas the packet delivery ratio cannot be lower than 95%.
- *Infotainment* also known as in-car comfort entertainment, usually do not use inter-vehicular communications. This kind of time-to-live ad-hoc application usually takes place in-car or vehicle-to-roadside. They use alerts, a multi-hop position based communication regime, and their latency cannot be higher than 400ms, whereas the packet delivery ratio cannot be lower than 95%.

Some other requirements must be considered for all the above applications, for instance whether they need sensors, human-machine interfaces, GPS, or maps in order to provide extra functional capabilities. Table 1 shows the requirements for types of applications for vehicular networks (CAMP Vehicle Safety Communications Consortium, 2005).

Application	Communication Type	Rate	Maximum latency	Data transmitted	Range
Traffic signal violation	V2I	10 Hz	100 ms	Signal phase, timing, position, direction, road geometry.	250 m
Curve speed warning	V2I	1 Hz	1000 ms	Curve location, curvature, slope, speed limit, surface.	200 m
Emergency brake lights	V2V	10 Hz	100 ms	Position, heading, velocity, acceleration.	200 m
Pre-crash sensing	V2V	50 Hz	20 ms	Vehicle type, position, heading, velocity, acceleration, yaw rate.	50 m
Forward collision	V2V	10 Hz	100 ms	Vehicle type, position, heading, velocity, acceleration, yaw rate.	150 m
Left turn assist	V2I or V2V	10 Hz	100 ms	Signal phase, timing, position, direction	300 m
Lane-change warning	V2V	10 Hz	100 ms	Position, heading, velocity, acceleration, turn signal status.	150 m
Stop sign assist	V2I or V2V	10 Hz	100 ms	Position, velocity, heading.	300 m
Electronic Toll Collection	V2I	10 Hz	50 ms.		15 m
Internet Access	V2I	10 Hz	500 ms		300 m
Automatic parking	V2I	10 Hz	500 ms	Position, distance	300 m
Roadside service finder	V2I or V2V	10 Hz	500 ms	Position, velocity	300 m

Table 1. Requirements for different types of vehicular networks applications

2.3 Data dissemination schemes

Given the complexities of VANET in terms of their dynamic topology, mobility models, hard delay constrains, and the different system architectures utilized, transporting information from one vehicle to another or to all vehicles within a given region or area is a highly challenging 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. Next, a classification of the different protocols for transporting information that have been proposed is presented and briefly analyzed (Li & Wang, 2007; Maihofer, 2004; Nundloll et al., 2009; Zeadally et al., 2010; Mauve, 2010):

- *Broadcast*. This routing method is generally utilized for disseminating information such as traffic, weather, emergency, road conditions, among others, to other vehicles. This communication scheme sends packets to all nodes in the network using flooding. When messages need to be disseminated beyond the radio transmission range, a multi-hop mechanism is then 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 messages area of distribution. Using this routing scheme, delivery of messages to all nodes is guaranteed, however, a large amount of bandwidth is consumed, this is 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.

- *Geocast*. It is a multicast routing service that delivers messages to nodes located within a given geographical region. These routing protocols generally define a forwarding zone that limits 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.
- *Forwarding*. The purpose of this routing scheme is to transport messages between two nodes via multiple hops. 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.
- *Clustering*. The cluster-based approach consists on grouping nodes located within a given region (e.g. nodes with direct link with each other). For each cluster, a cluster head node is selected which is responsible for managing inter and intra-cluster communication. The cluster-based structure functions as a virtual network infrastructure whose scalability favors routing and media access protocols although an overhead cost is paid when forming clusters in highly mobile network environments and network delays may occur on large networks.
- *Beaconing*. This routing mechanism is suitable for applications that require sharing information with other vehicles periodically (e.g. exchange of local traffic information). In this routing scheme a node announces information periodically. Receiving nodes, do not re-broadcast the received message immediately, instead, they integrate and store received information on its local information cache. On the next beacon, a message is constructed using both local and the incoming information and broadcasted to neighboring nodes.
- *Position-based*. For this routing scheme to work, information on the location of each node is fundamental. To decide how to route messages, nodes utilize geographical location information obtained from sources such as street maps, traffic models and on-board navigational systems. Routing decisions at each node are done 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.
- *Delay-tolerant*. There exist scenarios where the density of vehicles is really low and consequently establishing end-to-end routes is not possible. For example at 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 vehicles density may be low. In sparse networks like those, 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 carried.

- *Ad-hoc (address-based/topology-based).* This category groups routing protocols 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. However, requirements on these address-based and topology-based mechanisms such as unique address identification among others make these protocols less suitable for VANETs.

2.4 Security on VANETs

As mentioned before vehicular networks could help improve traffic management and roadside safety. Several efforts have been focused on the development of applications for these kinds of networks. However, those applications will have important requirements regarding data security. Vehicular communication security is a major challenge, having a great impact on future development of vehicular networks. According to Weimerskirch, security is defined as "protection against malicious manipulation of IT systems and plays an important role when designing and implementing such applications" (Weimerskirch et al., 2010).

In this sense, VANET's applications face important challenges in the security area, as they are more vulnerable to attacks. In vehicular communication scenarios, due to exhaustive data exchange amongst vehicles and the infrastructure the potential risk of violation of data security is greatly increased. Therefore, applications could be used for illegal objectives such as tracking people on their vehicles or to disseminate false information about traffic conditions.

In vehicular networks is needed an exhaustive risk analysis in order to identify potential attacks. However risk analysis has not yet been studied in an extensive way. Some works as the proposed in (Aijaz et al., 2006) and (Schneier, 1999) are cited by different authors on attacker capabilities in vehicular communications. In (Huanqun et al., 2008) authors presented some possible security threats and attacks scenarios which are described as follow:

- *Eavesdropping.* This consists on diffusing wrong information in the networks to affect the behaviour of the drivers.
- *Denial of service.* This is related to restrict the accessibility of services.
- *Bogus information.* This consists on faking a warning message.
- *Spoofing.* This is related to taking-over the identity of an authorized device.
- *ID disclosure of other vehicle.* This scenario is related to put under surveillance vehicles by means of vehicular networks.
- *Cheating with sensory information.* This problem consists on altering information (such as perceived position, speed, direction, among others) in order to avoid liability especially in the case of an accident.
- *Theft.* Breaking in someone else's vehicle, i.e. impersonation.

There are several research efforts in the area of security in vehicular networks. A majority of works converge towards a design with vehicles frequently beaconing their position along with warnings on their condition or the environment. Typical beaconing periods considered are in the order of one beacon per 100 milliseconds per vehicle. Other efforts have been focused on the definition of security architectures as the developed by the *Vehicle Safety Communications consortium* (VSCC), which defines a PKI-based approach for messages, sent

in vehicle-to-vehicle and vehicle-to-infrastructure communication environments (Papadimitratos et al., 2008). However, VANET applications will bring a series of challenges on the security area that help to solve several issues such as integrity, privacy and the non-repudiation of messages and authentication.

2.4.1 Integrity

Integrity is related to honesty and verification of the information. For applications trustworthiness of data is more useful that trustworthiness of nodes communicating data. Data trust and verification ensures that, on the one hand, the exchanged information can be trusted, and on the other hand, the receiver nodes can verify the integrity of the received information in order to protect the vehicular network from attacks and impersonation security. In (Leinmuller et al., 2007) authors classify the trust and verification concepts into proactive security and reactive security. According to Leinmuller the former has been researched extensively and consists of digitally signed messages, a proprietary system design, and Tamper resistant hardware (Caladriello et al., 2007; Hu & Labertearx, 2006; Garfinkel et al., 2003). The latter consists of signature-based, anomaly-based and context-based approaches. Their main characteristic is that they correlate the received information with information that is either already available into the system from observations on normal system operations or that is introduced additionally (Brutch & Ko, 2003; Zhang et al., 2003).

2.4.2 Privacy and non-repudiation

As mentioned before, security in vehicular networks must be designed to prevent potential attacks caused by drivers reacting dangerously as a result of receiving erroneous messages. Non-repudiation is related to define mechanisms, to prevent an entity from denying previous commitments or actions. Vehicular applications require a strong mutual authentication with non-repudiation because all safety-related messages may contain life-saying information. For instance, the diffusion of fake safety messages by an attacker could produce potentially dangerous situations on the road.

Privacy is related to protect user information, while at the same time authorities have to be able to reveal the identity of message senders in case of an eventuality (Raya et al., 2006). Therefore it is critical to develop mechanisms to preserve privacy in vehicular networks. Some of the proposed techniques to provide privacy are: anonymous certificates, group signatures and pseudonym certificates. The anonymous certificates technique is based on the usage of a list of anonymous certificates for message authentication, which is stored in a central repository (such as a transportation regulation center). The second technique is in charge of providing anonymity to a group of members. Any node of the group has the capacity of verifying whether a group member sent a certain message, however it is not necessary to know the real identify of the sender node. Finally, pseudonymous authentication is a technique widely accepted in vehicular networks. Its main use is anonymous authentication.

In (Rivas et al., 2011) authors analyse other important issue in the security area for vehicular networks, the detection and eviction of misbehaving and faulty nodes. Due to the attacker's ability or just to the devices aging process at some point in the time there will be

misbehaving or faulty nodes in the vehicular networks. Several works in the literature study this issue. For instance, in (Golle et al., 2004) authors proposed a heuristic approach, which consists in finding the best explanation for corrupted data. In reference (Xiao et al., 2006) authors proposed an approach to detect attacks based on radio signal strength analysis and use the idea that a vehicle cannot be on different places at the same time. In (Raya et al., 2007) authors proposed an approach that uses the Tamper Proof Devices (TPD) and assumed the existence of a honest majority on the attacker's neighborhood. TPD are used to execute their protocol and revoke themselves if they detect that have been tampered.

2.4.3 Message authentication

Vehicular networks require a mechanism to help authenticate messages, identify valid vehicles, and remove malevolent vehicles. Reference (Kargl et al., *2006)* explains that authentication ensures that a message is trustable by correctly identifying the sender of the message. With an ID authentication, the receiver is able to verify a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. In other cases receivers are not interested in the actual identity of nodes. They are satisfied if they are able to verify that the sender has a certain property. Property authentication is a security requirement that allows verifying properties of the sender, e.g. the sender is a car, a traffic sign. For applications using location information, location authentication allows verifying that the sender is actually at the claimed position, or that the message location statement is valid. Some protocols have been proposed for safety messages in vehicular networks. On the one hand, some of these protocols rely on the concept of pseudonymous authentication, also known as *Baseline Pseudonym* (BP). In this kind of protocols each vehicle generates its own pseudonyms, in order to eliminate the need of pre-loading, storing and refilling pseudonyms and the corresponding private keys. In this way, the burden of key and pseudonym management is greatly reduced. Other protocols are based on *Group Signatures* (GS) for V2V communication (Lin et al., 2007). GS is more robust than pseudonymous authentication, as any two group signatures generated by a node cannot be linked (Calandriello et al., 2007).

3. Wireless technologies for vehicular networks

To support vehicle to vehicle (V2V) or vehicle to infrastructure (V2I) communication in ad-hoc and dynamic environments wireless technologies such as WiFi, WiMAX, 3G, ZigBee and Bluetooth among others, are available (Jain et al., 2009). All these technologies feature important differences in terms of transmission range, transfer data rate, geographical area of coverage, supported content types, etc. In a VANET environment different subsets of this type of technologies can be present at a same time and place; therefore, support for heterogeneous wireless technologies is important. For example, a tracking application may require GPRS connectivity, intersection collision avoidance may require of DSRC communication and text message application may require Bluetooth. The main features of these technologies are described as follows.

3.1 WiFi (802.11p)

The IEEE 802.11p protocol is also known as Wireless Access in Vehicular Environment (WAVE). This protocol was specifically designed operate in V2V and V2I settings, and

makes use of spectrum band and channels allocated to the *Dedicated Short Range Communications* (DSRC) by the U.S. *Federal Communication Commission* (FCC) in 1999. The DSRC radio uses a 75 MHz spectrum at 5.9 GHz (Figure 2). The main aim of this standard is to provide support public safety applications that can save lives and improve traffic flow. The DSRC band is a free spectrum and is licensed by the FCC. The license regulates its usage and the technologies that make us of it, this is, all radio manufacturers, must fulfil FCC regulations (Jiang & Delgrossi, 2008). The DSRC band offers 7 licensed channels with a transmission range of up to 1000 meters and a transmission data rate between 6 to 27 Mbps, supporting speeds of up to 200 Km/h. The Department of Transportation of the United States and the automotive industry are strongly supporting the development of DSRC devices (i.e. on board units and road side units) and applications (Jiang et al., 2006).

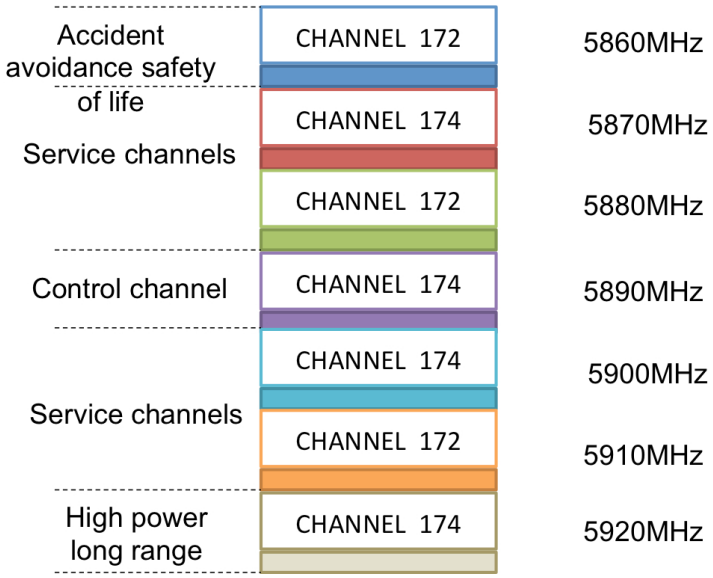

Fig. 2. Available channels for DSRC.

3.2 WiMAX (IEEE 802.16)

WiMAX is a high bandwidth technology designed to provide broadband wireless access over large areas to home and business and to a large number of users. WiMAX is an implementation of the IEEE 802.16 standard and was created by the WiMAX Forum[4] in 2001 (Ghosh & Wolter, 2005). To date more than 500 companies are members of the WiMAX Forum. Some of the potential usages of WiMAX include: mobile broadband connectivity across cities, last mile broadband access, VOIP, Internet connectivity, in-building coverage, temporary coverage and coverage on a mobile vehicle, among others (Peters & Heath, 2009). WiMAX maximum operating range of coverage is 100 Km and supports speeds of up to 1 Gbps (on fixed stations). WiMAX speed depends on the distance covered, the closer the

[4] http://www.wimaxforum.org

WiMAX station the higher the speed and the farther the station the lower the speed. Table 2 summarizes the mobility performance of WiMAX (Cudak, 2010).

Mobility	Performance
Stationary, Pedestrian 0-10 km/h	Optimized
Vehicular 10-120 km/h	Graceful degradation as function of vehicular speed
High Speed Vehicular 120 – 350 km/h	System should be able to maintain connection

Table 2. WiMAX mobility support.

3.3 Cellular technology (3G)

The third-generation (3G) system comprehends a set of standards that aim to support global communication for mobile telecommunication services such as mobile Internet, video calls and mobile TV. These standards are defined in the IMT-2000 vision of the International Telecommunications Union. The most popular implementations of 3G are: UTMS or 3GPP which is widely utilized in Europe, Japan and some parts of Asia and CDMA2000 also referred as 3GPP2 which has been deployed in the United States, South Korea, Belarus, Romania, and some parts of Russia, Japan and China (Etoh, 2005). The IMT-2000 standard aims to provide minimum transmission rates of 2 Mbps for stationary or walking users, and 348 kbps in a moving vehicle (ITU, 2011).

3.4 Zigbee

This technology is built upon the IEEE 802.15.4 standard which defines the physical and MAC layers for low cost and low rate personal area networks. Zigbee has a coverage range of up to 400 meters and a maximum data rate of 250 kbps with network latency between 15 and 30 ms (Backer, 2005). It operates in three different radio bands: 868 Mhz in Europe, 915 Mhz in the USA and Australia, and 2.4 Ghz worldwide. The Zigbee Alliance defines 7 application profiles including building automation, remote control, smart energy, health care, home automation among others. Besides, the research community is also investigating the usage of Zigbee in vehicular applications such as intra-car wireless sensor networks (Tsai et al., 2007), wireless vehicular identification and authentication system (Dissanayake et al., 2008), wireless sensor networks for CO_2 monitoring (Hu et al., 2009).

3.5 Bluetooth

Bluetooth is a low power consumption and short-range communication system (power-class-dependent: 1 meter, 10 meters, 100 meters) originally designed to replace cables connecting electronic devices. Bluetooth devices can communicate with up to 7 slave devices forming a piconet network (1 master + 7 slaves), where a piconet is an ad-hoc computer network of interconnected Bluetooth devices. Piconets can communicate with each other forming a scatternet, in which some devices act as bridges to provide communication between piconets. The Bluetooth core system utilizes a protocol stack consisting of a radio protocol, a link control protocol, a link manager protocol and a logical link control and adaptation protocol. It operates in an unlicensed band at 2.4 to 2.485 Ghz. The list of Bluetooth applications includes wireless headsets, printers, keyboards, game controllers (e.g. Nintendo's Wii and Sony's PlayStation), medical equipment, bar code scanners. -

Examples of vehicular applications includes wireless control and communication with mobile phones, multimedia and entertainment devices.

4. Sensing platforms

Successful of vehicular networks will depend upon the definition of sensing platforms that allow providing a means of collecting/processing/accessing sensor data. Comprehensive and accurate data are the primary requirement of vehicular networks. Various technologies have been enhanced/developed in recent years to improve this data collection quantity and quality though two main categories can be identified:urban sensing technologies, where field infrastructure is needed and intra vehicular sensors technologies in which a vehicle needs to be equipped. This section describes the most relevant sensing platforms for collecting information about traffic conditions.

4.1 Intra vehicular sensors

Advances in vehicular communications make it possible to implement vehicular sensor networks, i.e., collaborative environments where mobile vehicles that are equipped with sensors of different nature (from toxic detectors to video cameras) interworking to implement monitoring applications. Vehicles continuously collect sensor data from urban streets (e.g., images, accelerometer data, among others), which are then processed to search for information of interest (e.g., recognizing license plates, or inferring traffic patterns). This challenging environment requires novel solutions with respect to those of more-traditional wireless sensor nodes. Additionally, vehicles can be used by the VSN to improve its performance, for example, vehicles have much higher power reserves than a typical mobile computer, power can be drawn from on-board batteries, and recharged as needed from a gasoline or alternative fuel engine, vehicles are orders of magnitude larger in size and weight compared to traditional wireless clients, and can therefore support significantly heavier computing (and sensorial) components.

Some intra vehicular sensors are:

- *MobEyes*. A middleware that supports VSN-based proactive urban monitoring applications. This middleware exploits wireless enabled vehicles that are equipped with video cameras and a variety of sensors to perform event sensing, processing and classifying of sensed data, and inter-vehicle ad hoc message routing (Lee et al., 2009).
- *On-Board Diagnostic systems (OBD).* These are commonly used in most vehicles. The OBD-II interface is a standard that provides almost complete engine control and also monitors parts of the chassis, body and accessory devices, as well as the diagnostic control network of the vehicle. OBD-II systems provide real-time data streams, including data from a host of sensors, e.g. oxygen, coolant, pressure, temperature, airflow, vehicle speed, steering angle. This information can be used for fine-tuning the vehicle performance (Birnbam, & Truglia, 2000).
- *Vehicle tracking systems.* Also found in most vehicles. Automatic vehicle location (AVL) systems allow for easy localization of the vehicle (Lim et al., 2009).
- *Collision warning (CW).* This sensor is combined with a laser ranger finder and vehicle speed sensor in order to predict dangerous happens in the forward direction. The

speech suggestion of CW will be activated and the evaluation degree is also sent to the far-end monitoring center (U. Lee & Gerla, 2010).

- *Vehicle navigation System.* This sensor can display the current position of the vehicle or local area in which the vehicle navigates. To locate the vehicle and the driver at the required location, a *Global Position System* (GPS), map matching, and dead-reckoning (DR) are used with integration of an *Inertia Measurement Unit* (IMU) for enhanced positioning performance and availability (Chen et al., 2009).
- *Comfort-meter.* This sensor uses the algorithm refered to as ISO 2631-1 in which the ride comfort standard for the drivers in the vehicle vibration environment is specified. Here the input signals are the accelerations of three axes. These signals will be transformed into the decision index, which specifies the ride quality (T. Lee et al., 2009).

4.2 Urban sensing

Urban sensing is a paradigm on collecting information about systems and the environment, which are closely related to and affected by human activities. Most prior work on sensor networks is based on collecting and processing environmental data using a static topology and an application-aware infrastructure. Urban sensing, on the other hand, involves collecting, storing, processing and fusing large amounts of data related to everyday environmental changes resulting from human activities, vehicles and other agents. This form of sensing is performed in highly dynamic and mobile environments.

Urban sensing applications are emerging in several areas. A good example of human centric urban sensing is Active Mapping. It is built on top of a geographical map, and collects and exchange information about human activities such as location and other details. Therefore it provides a platform for people interaction and also serves as an interface for registering context-aware events. An important application area within urban sensing is urban information systems. A common design approach is to build a publish-and-subscribe mechanism and provide differentiated services to meet individual user's interests. Therefore, real-time, context-aware and online information management systems of urban sensing applications are highly encouraged.

Urban sensing can be primarily divided into two kinds: static infrastructure and human-centric urban sensing.

The former includes urban multifunction traffic lights control system, equipped with sensing infrastructure that has often been an effective measure applied to regulate vehicle flow inside cities. This static infrastructure uses real-time measurements such as inductive loops or pattern-recognition digital cameras to decide the suitable traffic signal. Infrared remote control apparatus recognizes the signal light control of each intersection. Moreover, these infrastructures are equipped with communication networks that enable adaptive coordination between different intersections in order to improve the traffic flow globally.

The latter has typically been used in the context of human-in-the-loop sampling scenarios where human involvement is mainly in the sampling or the sensing process (through handheld mobile devices etc.). In (Lim et al., 2009) authors propose to redefine or extend the definition of human-centric urban sensing. In the proposed framework, human-centric urban sensing refers to human involvement in the data assimilation, processing, inference as well as decision, control and feedback processes.

According to research of Lee and Gerla (U. Lee & Gerla, 2010), some technologies for communications in vehicular environments are DSRC/WAVE, cellular networks, WiMAX/802.16e, WiFi/802.11p. These technologies will enable operations related to the improvement of traffic flow, highway safety, and other ITS applications in a variety of application environments.

Given the above sensors and communications technologies, it is possible summarizes vehicular networking scenarios as shown in figure 2.

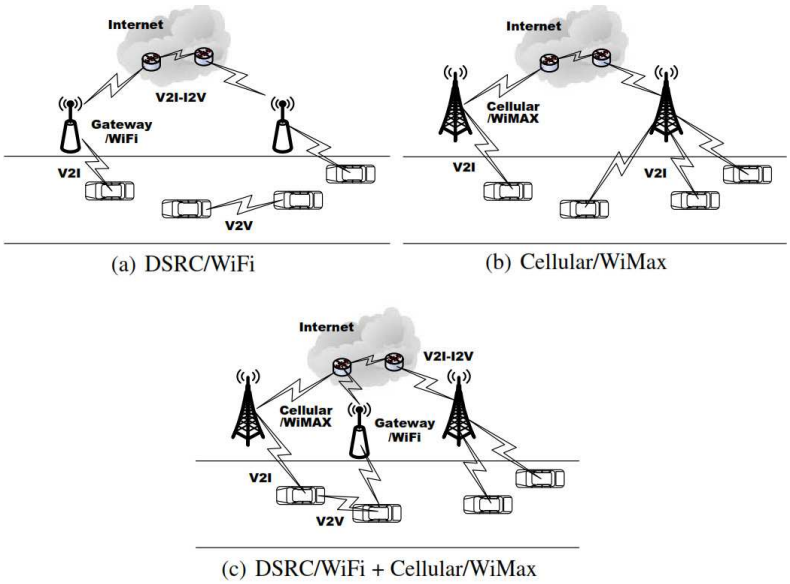

Fig. 2. Wireless vehicular networking scenarios.

Vehicles only equipped with DSRC can operate on infrastructure-free mode (V2V only), infrastructure mode (V2I), and mixed mode (V2V and V2I) as shown in Fig. 2a. Vehicles equipped with other broadband wireless access (i.e., cellular, WiMAX), can operate on scenarios where vehicles can talk to each other via Internet as in Fig. 2b. For instance, people with smartphones and Internet access can conform a P2P overlay network via the Internet. Finally, when vehicles have both DSRC and other broadband wireless access methods, we can have a mixed access scenario (Fig. 2c). Researchers have mostly focused on the first scenario, yet the second scenario has recently received a lot of attention due to the widespread usage of smartphones and WiBro (Lee & Gerla, 2010).

In (Hounsell et al., 2009) authors describe other models and technologies that can be used for traffic data collection. For example, inductive loops embedded are used to detect the movement of vehicles over a road surface and is extensively used in traffic responsive traffic signal systems to provide relevant information about traffic conditions such as traffic density, flows and speeds, among others, that can be used to optimize traffic flows. Beacon-based technology detects a vehicle by a 'beacon' positioned at a known location employing various technologies such as microwave, infra-red and dedicated short-range

communication (DSRC) beacons. Closed-circuit television (CCTV) provides a mechanism to monitor traffic operations at key locations in urban networks, such as major junctions, road bottlenecks, tunnels and so on. Information of this kind of systems is used as a basis for managing traffic control strategies, for confirmation of incidents, and to record conditions or events over a period of time.

5. Conclusions

One of the major priorities for governments is to define mechanisms and schemes that could help solve traffic problems that modern society faces. Governments are addressing their efforts in the use of emerging technologies as base elements for transportation system. 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, and making more efficient the driver tasks and comfortable the time passengers expend inside the vehicle. With technologies like these, it is possible to develop transport systems that are capable of optimizing fuel consumption, minimizing traffic congestion, reducing CO_2 emissions and more importantly reducing human casualties.

In addition, there exist an important number of private and public initiatives that have been created and are dedicated to the development and research of vehicular systems. Still, because of the characteristics of VANETs in terms of, for example, its dynamic network topology, mobility patterns, low latency, among others, development and deployment of vehicular applications is still very challenging. What is more, to correctly operate, most VANET applications require support of special infrastructure (i.e. RSU) to extend vehicles short range communication coverage enabling and extending data dissemination. Unfortunately, the number of available RSUs and OBUs in today's scenarios is still very limited and this condition limits and makes difficult to deploy and evaluate existing applications. In this chapter we have analyzed some of the main challenges that the development of vehicular networks face. We presented a general study about some of the emerging technologies that can be used for vehicular networks. We have also showed some platforms that can be used as data collectors about traffic conditions, warning or emergency situations. Successful development of VANETs and the related applications are conditioned to the definition of standards that facilitate the integration of heterogeneous systems. Similarly, the creation of strategies for increasing users acceptability and accessibility to vehicular applications and technologies is necessary. Finally, to guaranty privacy and security of users, data and applications novel mechanisms need still to be developed.

6. References

Aijaz, A.; Bochow, B.; Dotzer, F.; Festag, A.; Gerlach, M.; Kroh, R. & Leinmuller, T. (2006). Attacks on inter vehicle communication systems – an analysis. *Proceeding of the 3rd International Workshop on Intelligent Transportation,* pp. 189-194, Hamburg, Germany, March 14-15, 2006.

Backer, N. (2005). Zigbee and Bluetooth strengths and weaknesses for industrial applications. *Computing & Control Engineering Journal*, Vol. 16, No. 2, pp. 20-25, ISSN 0956-3385.

Bakas, L. (2008). *Transport and greenhouse gas emissions*. CORPUS, The SCP Knowledge Hub, available from http://www.scp-knowledge.eu/sites/default/files/Poster%20GHG.pdf.

Barth, M. & Boriboonsomsin, K. (2009). *Traffic congestion and greenhouse gases*. Technical report, available from : http://www.uctc.net/access/35/access35_Traffic_Congestion_and_Grenhouse_Gases.pdf

Birnbam, R. & Truglia, J. (2000). *Getting to know OBD-II*, A S T Training, ISBN 0970671105, New York, 2000.

Brutch, P. & Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks. *Proceeding of IEEE Workshop on security and assurance in ad hoc networks*, ISBN 0-7695-1873-7, pp. 368-373Washington, USA, January 27-31, 2003.

Calandriello, G. ; Papadimitratos, P. ; Lloy, A. & Hubaux, J-P. (2007). Efficient and robust pseudonymous authentication in VANET. *Proceedings of 4th ACM International Workshop on Vehicular Ad Hoc Networks*, ISBN 978-1-59593-739-1, pp. 19-28, Montreal, Canada, September 9-14, 2007.

CAMP Vehicle Safety Communications Consortium. (2005). DOT HS 809 859 [online] Vehicle Safety Communications project task 3 final report: identify intelligent vehicle safety applications enabled by DSRC. In *Washington DC: U.S. Department of Transportation official website*, Available from http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2005/CAMP3scr.pdf

Chen, Y.; Xiang, Z.; Jiang, W. & Jiang, W. (2009). Design and Implementation of Multi-Source Vehicular Information Monitoring System in Real Time. *Proceedings of the IEEE International Conference on Automation and Logistics*, ISBN 978-1-4244-4794-7, pp. 1771-1775, Shenyang, China, Auust 5-7, 2009.

Commission for Global Road Safety (2009). Make roads safe, a decade of action for road safety. ISBN-13: 978-0-9561403-2-6. In : *Make the road safe*, 29.07.2011, Available from http://www.makeroadssafe.org/publications/Documents/decade_of_action_report_lr.pdf.

Cudak, M. (2010). IEEE 802.16M System Requirements. In : *IEEE 802.16 Broadband Wireless Access Working Group*, 15.09.2011, Available from http://www.ieee802.org/16/tgm/.

Dissanayake, S., Karunasekara, P., Lakmanaarachchi, D., Rathnayaka, A., & Samarasinghe, A. (2008). Zigbee Wireless Vehicular Identification and Authentication System. *4th International Conference on Information and automation for Sustainability*, ISBN 9781424428991, pp. 257-260, Colombo, Sri Lanka, December 12-14, 2008.

Etoh, M. (2005). *Next Generation Mobile Systems 3G and Beyond*. John Willey & Sons, ISBN 0470091517.

Garfinkel, T. ; Pfaff, B. ; Chow, J.; Rosenblum, M. & Boneh, D. (2003). Terra : a virtual machine-based platform for trusted computing. *Proceeding of the 19th Symposium on Operating systems principles*, vol. 37, no.5, October 19-22, 2003.

Golle, P. ; Greene, D. & Staddon, J (2004). Detecting and correcting malicious data in vanets. *Proceedings of the 1st. ACM international workshop on vehicular ad hoc networks*. Phildelphia, Phennsylvania, USA, September 26 - October 1, 2004.

Ghosh, A., & Wolter, D. (2005). *Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential*. IEEE Communications Magazine, Vol. 43, No. 2, pp. 129-136. ISSN 0163-6804.

Hounsell, B. ; Shrestha, B. ; Piao, J. & McDonald, M. (2009) *Review of urban traffic management and the impacts of new vehicle technologies*. IET Intelligent Transportation Systems, vol 3, No. 4, pp. 419-428, ISSN 1951-956X.

Hu, Y. & Labertearx, K. (2006). Strong security on a budget. *Proceeding of the Workshop embedded security for cars*, Berlin, Germany, November 2006.

Hu, S.-C., Wang, Y.-C., Huang, C.-Y., & Tseng, Y.-C. (2009). A Vehicular Wireless Sensor Network for CO2 Monitoring. *Proceeding of IEEE Sensors*, ISBN 978-1-4244-4558-6, pp. 1498-1501, October 25-28, 2009.

Huanqun G. ; Lek Heng N. ; Yongdong W. ; Lian Hwa L. ; Choon Hwee K. ; Feng T. & Jun Jie A. (2008). Embedded info-security solutions for vehicular networks. *Proceedings of Conference on Communication and Networking*, ISBN 978-1-4244-2373-6, pp 29-33, Hangzhou, Chine, August 25-27, 2008.

ITU. (4 de April de 2011). About mobile technology and IMT-2000. In : *About mobile technology and IMT-2000*, 20.09.2011, Available from http://www.itu.int/osg/spu/imt-2000/technology.html#Cellular%20Standards%20for%20the%20Third%20Generation.

Jain, S. ; Taneja, S. ; & Jain, D. (2009). Fuzzy Logic Based Routing Strategies in VANETs. *Proceeding of 3rd Nationall Conference INDIACom-2009*, New Delhi, India, February 26-27, 2009.

Jiang, D., & Delgrossi, L. (2008). IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. *Proceeding of Vehicular Technology Conference*, ISBN 978-1-4244-1644-8, pp. 2036-2040, Singapore, May 11-14, 2008.

Jiang, D., Taliwal, V., Mier, A., & Holfelder, W. (2006). Design of 5.9 GHz DSRC-based Vehicular Safety Communication. *IEEE Wireless Communications*, Vol. 13, No. 5, pp. 36-43, ISSN 1536-1284.

Kargl, F.; Ma, Z. & Schoch, E (2006). Security Engineering for VANETs. *Proceeding of 4th Workshop on Embedded Security in Cars*, Berlin, Germany, November 14-15, 2006.

Lee, T.; Chiang, H.; Perng, J.; Jiang, J. & Wu, B. (2009). Multi-sensor Information Integration on DSP Platform for Vehicle Navigation Safety and Driving Aid. *Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control*, ISBN 978-1-44244-3491-6, pp. 653-658, Okayama, Japan, March 26-29, 2009.

Lee, U. & Gerla, M. (2010). A survey of urban vehicular sensing platforms. *Computer Networks : Elsevier*, Vol. 54, No. 4, pp. 527-544, ISSN 1389-1286.

Lee, U.; Magistretti, E.; Gerla, M. & Bellavista, P. (2009). *Dissemination and Harvesting of Urban Data Using Vehicular Sensing Platforms.* IEEE Transactions on Vehicular Technology. Vol. 58, No. 2, pp. 882-901, ISSN 0018-9545.

Leinmuller, T.; Schoch, E. & Maihofer, C. (2007). Security requirements and solution concepts in vehicular ad hoc networks. *Proceedings of 4th annual conference on wireless on demand network systems and services*, ISBN 1-4244-0860-1, pp. 84-91, January 24-26, 2007.

Li, F., & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, Vol. 2, No. 2, pp. 12-22, ISSN 1556-6072.

Lim, H.B., Fu, Ch., Nasir, A., Srirangarajan, S., Wang, B., Wong, K.J. & Soong, B.H., (2009). An Integrated Framework for Vehicular and Urban Sensing. *Proceeding of GLOBECOM Workshops, 2009 IEEE*, ISBN 978-1-4244-5626-0, pp. 1-6, Honolulu, Hawaii, USA, November 30 – December 04, 2009.

Lin, X. ; Sun, X. ; Ho, P.-H. & Shen, X. (2007). GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications. *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, ISSN 0018-9545.

Ma, Y. ; Zhou, Y. ; Chowdhury, M. ; Wang, K. & Fries, R. (2009). A framework for performance evaluation of communication alternatives for Intelligent Transportation Systems. *Journal of Intelligent Transportation Systems*, Vol. 13, No. 3, pp. 111–126, ISSN 1547-2450.

Maihofer, C. (2004). A Survey of Geocast Routing Protocols. *IEEE Communications Surveys and Tutorials*, Vol. 6, No. 2, pp. 32-42, ISSN 1553-877X.

Mauve, M. (2010). Information Dissemination in VANETs. In *VANET Vehicular Applications and Inter-Networking Technologies*, H. Hartenstein, & K. Laberteaux, pp. 49-80. Wiley&Sons Ltd, ISBN 0470740566.

Nundloll, V., Blair, G., & Grace, P. (2009). A Component-based Approach For (Re)-Configurable Routing in VANETS. *Proceeding of 8th International Workshop on Adaptive and Reflective Middleware*, ISBN 978-1-60558-850-6, Urbana Champaing, Illinois, USA, November 30 – December 4, 2009.

Papadimitratos, P.; Calandriello, G.; Hubaux, J-P and Lioy, A. (2008). Impact of Vehicular Communications Security on Transportation Safety. In IEEE INFOCOM Workshop 08, ISBN 978-1-4244-2219-7, pp.1-6, Phoenix, Arizona, USA, April 13-18, 2008.

Peters, S., & Heath, R. (2009). The Future of WiMAX: Multihop Relaying with IEEE 802.16j. *IEEE Communications Magazine*, Vol.47, No. 1, pp. 104-111, ISSN 0163-6804.

Popescu-Zeletin, R.; Radush, I. & Rigani, M. (2010). *Vehicular-2-X Communications: State-of-the-art and research in Mobile vehicular ad-hoc networks. Springer, ISBN: 3540771425.*

Raya, M. ; Papadimitratos, P. ; Aad. I. ; Jungels, D. & Hubaux, J-P. (2007). Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, Vol. 25, No. 8, pp. 1557-1568, ISSN 0733-8716.

Raya, M.; Papadimitratos, P. & Hubaux, J-P. (2006). Securing vehicular communications. *IEEE Transaction on Wireless Communications*, Vol. 13, No.5, pp. 8-15, ISSN 1536-1276.

Rivas, D. ; Barceló-Ordinas, J. ; Guerrero, M. & Morillo-Pozo, J. (2011). Security on VANETs : Privacy, misbehaving nodes, false information and secure data aggregation. *Journal of Network and Computer Applications*, vol 34, No. 6, pp. 1942-1955, ISSN 1084-8045.

Schneier, B. (1999). Attack trees: modeling security threats. *Dr. Dobb's Journal*, ISSN 1044-789X.

Schrank, D. ; Lomax T. & Turner S. (2010). TTI's Urban Mobility Report. In : *Texas Transportation Institute,* 29.07.2011, Available from http://mobility.tamu.edu/ums/report/.

Spyropoulos, T.; Naveed, R.; Obraczka, K. % Vasilakos, A. (2010). Routing for disruption tolerant networks: taxonomy and design. *Journal of Wireless Networking*, Vol. 16, No. 8, pp. 2349–2370, ISSN 1022-0038.

Tsai , H.-M., Saraydar, C., Talty, T., Ames, M., Macdonald, A., & Tonguz, O. (2007). Zigbee-based Intra-car Wireless Sensor Network. *Proceeding of IEEE International Conference on Communications*, ISBN 1-4244-0353-7, pp. 3965-3971, Glasgow, Ireland, June 24-28, 2007.

UNFPA (2007). Technical Report: State of World Population 2007: Unleashing the potential of urban growth. In *United Nations Population Foundation official website*, 25.09.2011, Available from http://www.unfpa.org/swp/2007/presskit/pdf/sowp2007_eng.pdf.

Weimerskirch, A ; Haas, J. ; Hu, Y. & Laberteaux, K. (2010). Data security in Vehicular Communication Networks, In : *VANET Vehicular applications and Inter-networking technologies,* Hartensteing, H. & Labeteaux, K., pp 299-363, Wiley, ISBN 9780470740569, UK.

Xiao, B. ; Yu, B. & Gao, C. (2006). Detection and localization of sybil nodes in vanets. *Proceeding of the 2006 workshop on dependability issues in wireless ad hoc networks and sensor networks*, ISBN 1-59593-471-5, New York, NY, USA, 2006.

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*, Vol. 56, No. 6, pp. 3358–3370, ISSN .

Zhang, Y. ; Lee. W. & Huang, Y. (2003). *Intrusion detection techniques for mobile wireless networks*. Journal of wireless netorks, vol. 9, no. 5, pp. 545-556, Springer.

Zeadally, S. ; Ray, H. ; Yuh-Shyan, C. ; Angela, I. & Aamir, H. (2010). *Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges*. Telecommunication Systems. Springer Science+Business Media. doi: 10.1007/s11235-010-9400-5

Urban Development

Edited by Dr. Serafeim Polyzos

ISBN 978-953-51-0442-1
Hard cover, 296 pages
Publisher InTech
Published online 30, March, 2012
Published in print edition March, 2012

Cities are growing as never before and nowadays, it is estimated that at least 50% of the world's population lives in urban areas. This trend is expected to continue and simultaneously the problems in urban areas are anticipated to have an increase. Urbanization constitutes a complex process involving problems with social, economic, environmental and spatial dimensions that need appropriate solutions. This book highlights some of these problems and discusses possible solutions in terms of organisation, planning and management. The purpose of the book is to present selected chapters, of great importance for understanding the urban development issues, written by renowned authors in this scientific field. All the chapters have been thoroughly reviewed and they cover some basic aspects concerning urban sustainability, urban sprawl, urban planning, urban environment, housing and land uses. The editor gratefully acknowledges the assistance of Dr Marius Minea in reviewing two chapters.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821