1

Vehicular Networks

1.1. Introduction

Vehicular networks are at the core of the intelligent transport system (ITS). Interest in these networks is constantly growing due to the need to reduce road fatalities, which result in immense yearly losses in terms of human lives, physical and mental health repercussions, property damage and financial losses. They were initially developed to ensure the safety of road users by providing them with accurate prior knowledge about the traffic, road conditions and shortcuts. They were also intended to provide users with safe, comfortable trips in their autonomous vehicles. Moreover, vehicle networks help to lower fuel consumption by reducing traffic jams and streamlining the driving experience.

In this type of network, the vehicles are the main nodes. They are also referred to as computers on wheels in the literature. The vehicles are equipped with various types of sensors for external and internal roles such as sensing proximity or engine heat. They also contain a global positioning system (GPS) to localize the vehicle, cameras, radar and lidar to sense the surroundings and detect obstacles and road conditions. The on-board unit (OBU) is the brain of the vehicle and computer controlling it; it ensures the vehicle's correct functioning and processes the sensed data. The OBU gives the vehicle the trait of smartness, which is the same reason they are known as "smart vehicles". They also have network interfaces that are used to communicate, alongside a storage space to save sensed data, security programs and received messages.

The vehicular networks encompass several types of networks in which the main type of node is a vehicle. It comprises the autonomous vehicles, Vehicular Ad hoc Networks (VANETs), vehicular data named networks, vehicular cloud computing, Internet of vehicles, etc. The appearance of these types is due to the evolution of the on-road users' service demands and corresponding answering applications. The earliest applications of VNs were safety-related, oriented towards assisting the driver. Then, the infotainment applications became a necessity later on. Lastly, the Internet and cloud computing were extended to road-edge in order to provide road users with their services.

This chapter reviews vehicular networks, their evolution and their applications. It depicts the yearly fatalities caused by vehicle causalities and the assessments of the benefits of using the vehicular networks to ensure safety, alongside the evaluation of their market value. It describes the vehicular networks' evolution as part of the intelligent transportation systems and road automation projects. It also explains the components of intelligent vehicles and the architectures of vehicular networks. It describes the main distinguishable characteristics of the vehicular networks. It enumerates the issues and technical challenges halting the vehicular networks' real implementations. Furthermore, it lists the wireless technologies that could potentially be used in vehicular networks. It outlines the vehicular networks regulating standards and explains the vehicular network's different existing types along with its test beds. Lastly, it reviews the public opinion and acceptance of the technology.

1.2. Motivation by numbers

The following statistics emphasize the importance of vehicular networks (Contreras-Castillo et al. 2018):

– approximately 1.3 million people die every year;

– more than 7 million people are injured;

– nearly 8 million traffic accidents are recorded;

– estimated wasted time because of traffic jams and accidents is over 90 billion hours;

– vehicles produce 220 million tons of carbon;

– the expected global market of the Internet of Everything may reach 14.4 trillion dollars by 2022 (Bonomi 2013) and the value of the Internet of vehicles (IoV) alone was estimated to be 115.26 billion Euros by 2020 (Contreras-Castillo et al. 2018);

– more importantly, autonomous vehicles usage would eliminate 80–90% of vehicles' accidents and crashes (Maglaras et al. 2016);

– a rough estimation (Bai and Krishnamachari 2010) states that 100% market penetration by vehicular networks would take 14–15 years from its initial deployment date.

With these statistics, it is abundantly clear that vehicular networks are most likely serving the purposes they were developed for in reducing car accidents, injuries, mortalities, pollution, etc. Academics and industry are doing their best to concretize and market this technology. What is left is to convince the public and draw attention to its benefits.

1.3. Evolution

Automated roads and the creation of self-driving vehicles have been the dream of various researchers and industry sectors. General Motors was the leader in exhibiting the basic concepts of road automation, known as "Futurama", at the 1939 World Fair. In 1970, a follow-up proposition came from the United States, which is the Electronic Route Guidance System (ERGS). It pilots the drivers to their destination by decoding and transmitting routing instructions to and from roadsides at intersections. In Japan, between 1973 and 1979, the Comprehensive Automobile Traffic Control System was launched. The project aimed to reduce air pollution and traffic congestion and prevent accidents. It also aimed to provide the driver with appropriate route directions thanks to the accurate information and warnings received (Gerla et al. 2014). In Europe, the PROMETHEUS (Program for European Traffic with Highest Efficiency and Unprecedented Safety) framework was introduced in 1986 and launched in 1988.

The term vehicular ad hoc networks was first coined by Ken Laberteaux in the first International Workshop on Vehicular Ad hoc Networks (VANET) held in Philadelphia in 2004 (Hartenstein and Laberteaux 2010). VANET is considered to be the first commercialized version of Mobile Ad-hoc Networks and one of its most promising applications, aiming to automate the roads and ensure user comfort and safety. It draws the community nearer to realizing the self-driving vehicles' vision (Gerla et al. 2014).

Ever since the VANET became a hot topic, various related consortiums and projects were launched yearly. We mention a few of them as an example: FleeNET, CarTalk2000, Car2Car consortium, PReVENT, Network on Wheel (NoW), MobiVip, etc. (Meraihi et al. 2008).

Starting from 2010, a new vehicular networks type appeared, the vehicular cloud (VC) concept, which combines cloud computing with vehicular networks. The VC takes advantage of the vehicles' sensing, calculation and storage capacities to extend the clouds that offer various kinds of stable services (Gu et al. 2013). As of 2014, researchers focused on the Internet of vehicles (Gerla et al. 2014; Yang et al. 2014), which is the evolution of VANETs and an instantiation of the Internet of Things.

In 2009, Google's first autonomous vehicle project started. It continued its tests and trials until 2015, when it first hit the public road. In 2016, the project became independent and was named Waymo under Alphabet, a self-driving technology company. Meanwhile, major car companies such as Renault, Mercedes, Tesla and Audi have been competing to launch their own self-driving vehicles (top companies for self-driving vehicles).

1.4. Architecture

Autonomous vehicles, also known as self-driving vehicles, are smart. They have two types, illustrated in Figure 1.1. The first type is the self-dependent (self-contained) vehicle, relying only on its smarts and computational capacities to process sensed data, execute instructions and make decisions. The second type is the interdependent vehicle, where a vehicle either exchanges data and instructions with a control server via Vehicle-to-Infrastructure (V2I), or, it is connected to other network nodes (vehicles) via Vehicle-to-Everything (V2X) to interchange sensed data. The second type is denoted as vehicular networks. Although the types differ, the design and components of the smart vehicles are similar (Glancy 2012).

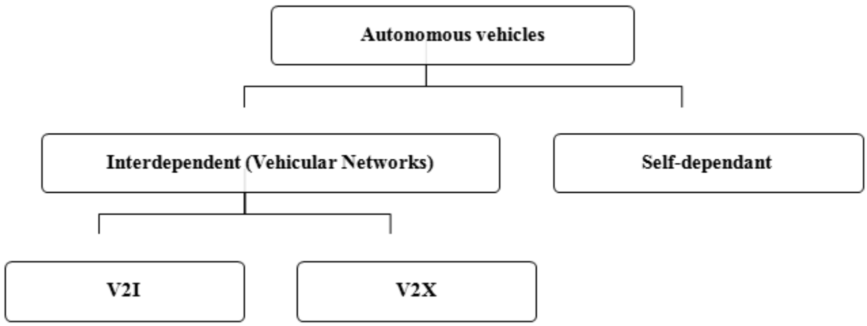

Figure 1.1. *Autonomous vehicles*

Vehicular networks in general are built upon the VANETs basic architecture. They are composed of vehicles as mobile nodes known as on-board units (OBU) and road side units (RSU) as static infrastructures. The OBU stores, locates, calculates and sends messages over a network interface (Gerla et al. 2014). It is composed of a read/write memory used to store/fetch information, a Resource Command Processor (RCP), a user interface and a network device using IEEE 802.11p radio technology for short-range wireless communication (Al-Sultan et al. 2014).

The RSUs broadcast advertisement and road information; they also spread data sent by OBUs (Gerla et al. 2014). They are equipped with network interfaces using IEEE 802.11p radio technology for a dedicated short-range communication, and wired interfaces for communication with the other infrastructures in the network (Al-Sultan et al. 2014). The basic components of a smart vehicle were initially summed up into the use of GPS, radar, sensors, an on-board computer (for processing and storage), network interfaces and a human-friendly interface.

However, the technology is constantly developing, with numerous carmakers competing on intelligent vehicles' implementations and testing. Therefore, the components are more sophisticated, refined and advanced. For illustration purposes, we study the components of a Google smart car as an example of the current design and technology in use.

A Google vehicle uses a distinguishable set of hardware and software technologies, and we mention a few of them (national):

– laser range finder (lidar, 360° camera), which can create 3D images of objects within a 200 m range and calculate the distances;

– front camera for near vision, which can detect front objects, pedestrians, obstacles, traffic lights, road signs, etc.;

– bumper-mounted radar, which are mounted on the front and rear of the vehicle to avoid bumps and crashes with vehicles, pedestrians and obstacles;

– an aerial on the rear of the vehicle that reads precise geo-location; this is done by matching the GPS location received from the satellite with the sensed location and internal map to render the location more accurately;

– ultrasonic sensors on rear wheels, which are used to keep track of the wheel's movement and detect the obstacle on the rear of the vehicles;

– the altimeters, gyroscopes and tachymeters inside the vehicle give precise information about its position;

– synergistic combining of sensors. The vehicle has a set of sensors for various purposes, all of the sensed data is combined and processed by the on-board unit to help achieve safe self-driving;

– in-built programmed maps, human behavior, data processing and decisional algorithms.

1.5. Characteristics

Vehicular networks have a particular nature and characteristics that differentiate them from other networks:

– their topology is highly dynamic due to the vehicles' high speed;

– predictable patterned movements defined by the roads and paths the vehicles run through;

– frequently disconnected networks causing a delay and potential loss of messages;

– the use of different types of external and internal sensors for various purposes;

– unlimited battery power and large storage capacity (Kumar et al. 2013);

– variable network density in roads (in rural areas, in the city, during daytime, during nighttime, etc.) (Al-Sultan et al. 2014);

– the various obstacles on road and surrounding it, such as trees and tall buildings;

– security and privacy threats (Guo and Balon 2006);

– availability of the vehicles' accurate real-time geographic positions (Sivasakthi and Suresh 2013);

– geographical communications using location information (Da Cunha et al. 2014).

1.6. Technical challenges and issues

Few technical issues and obstacles that need to be resolved confront the real-world implementation of vehicular networks. We mention some of them in this section:

– signal fading due to large distance between vehicles in case of a sparse network and/or the existence of the multiple obstacles in the case of urban areas;

– limitation of bandwidth, which engenders congestion when excessive simultaneous applications are being used in dense urban areas. Therefore, even the fair use of bandwidth increases latency in a dense environment;

– connectivity fluctuation and frequent fragmentation due to the high mobility of vehicles and the small effective diameter of the network;

– balancing and satisfying security and privacy requirements in VANETs;

– the rapidly changing topology hardens the task of researchers aiming to design a reliable routing protocol for VANETs. These protocols are responsible for delivering packets in the shortest possible time, even in a dense network (Al-Sultan et al. 2014);

– VANETs inherit the problems of exposed and hidden terminals from MANETs;

– the high cost of the deploying roadside units and infrastructures, IT-management issues and connectivity are among the leading reasons holding the real-world implementation of VANET back (Hartenstein and Laberteaux 2010).

1.7. Wireless technology

Various wireless technologies may be used to ensure the connectivity between the VANET components, among which are:

– **Cellular systems**: can be used as a communication solution for VANETS to exchange messages and data. Among the reused systems are: the Global System for Mobile (GSM), also known as 2G, the General Packet Radio Service (GPRS), also known as 2.5 G, Enhanced Data rates for GSM Evolution (EDGE), also known as 2.75 G, the Universal Mobile Telecommunication System (UMTS), also known as 3G, High-Speed Downlink Packet Access (HSDPA), CMDA2000, LTE 4G and 5G.

– **WLAN/Wi-Fi**: may also possibly be used to provide wireless access enabling V2I or V2V communications.

– **WiMAX**: Worldwide Interoperability for Microwave Access, also known as IEEE 802.16e. It covers a wide transmission range, achieves high data rate and has a high quality of service.

– **DSRC/WAVE**: licensed spectrums of 75 MHz at 5.9 GHz in the United States and at 5.8 GHz in Japan and Europe. It can be used solely for vehicle-to-vehicle and vehicle-to-infrastructures communications.

– **Combined wireless access technology**: combines various wireless technologies, such as GPRS, GSM and 3G (Al-Sultan et al. 2014).

1.8. Standards

To specify the operation of vehicular networks from the physical to the application layer, a group of protocols were standardized. The standards are primarily developed in Japan, Europe and North America. There are two major standardization groups: the ETSI ITS-G5 and IEEE WAVE stack protocols in Europe and North America respectively (Boualouache 2016).

The vehicles communicate with each other and with road side units (RSU) through dedicated short-range communications (DSRC). The DSRC provides low communication latency and high data transfer rate in small communication zones. In

1999, the United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band to be used for a service called DSRC. The DSRC is a licensed free spectrum divided into seven channels that are 10 MHz each, among which only one channel is for safety communications, while four are service channels and the remaining two channels are reserved for special purposes (Boualouache 2016). The data rate varies between 6, 9, 12, 18, 24 and 27 Mbps for the 10 Mhz channel. It may increase to 54 Mbps for 20 MHz channels.

1.8.1. *IEEE WAVE stack*

The WAVE IEEE standards define the standards set for each layer. It has a stack for safety and for non-safety applications. Figure 1.2 illustrates the IEEE WAVE standards (Sjöberg 2011), and Figure 1.3 shows a simplified view of it.

<table>
<tr><td></td><td>Safety applications</td><td>Non-safety applications</td></tr>
<tr><td></td><td>Safety application sublayer</td><td>Application</td></tr>
<tr><td rowspan="2">Security
IEEE1609.2</td><td>Message sublayer
SEA J2735</td><td>Transport (TCP/UDP)
IETF RFC 793/768</td></tr>
<tr><td>WSMP
(IEEE 1609.3)</td><td>Network (IP V6)
IETF RFC 2460</td></tr>
<tr><td></td><td colspan="2">LLC sublayer
IEEE 802.2</td></tr>
<tr><td></td><td colspan="2">MAC sublayer extension
IEEE1609.4</td></tr>
<tr><td rowspan="2">802.11P</td><td>MAC sublayer</td><td>MAC layer</td></tr>
<tr><td>PHY sublayer</td><td>PHYSIC layer</td></tr>
</table>

Figure 1.2. *IEEE WAVE standards (Sjöberg 2011)*

– **IEEE 802.11p**: IEEE 802.11p mac protocol for VANET extending the 802.11e.

– **IEEE1609.1**: defines the formats of messages and their responses.

– **IEEE 1609.2**: defines the secure messages' formatting, processing and exchange.

– **IEEE 1609.3**: defines the transport and routing layer services.

– **IEEE 1609.4**: describes the multichannel operations (Rawashdeh and Mahmud 2011).

Security IEEE1609.2	Resource manager	IEEE 1609.1
	Networking services	IEEE 1609.3
	Multi-channel operations	IEEE 1609.4
	Phys./MAC IEEE 802.11P	

Figure 1.3. *A simplified WAVE standard view (Rawashdeh and Mahmud 2011)*

1.8.2. *ETSI standards*

The ETSI standards is the European equivalent of the US IEEE WAVE standards for vehicular networks and ITS. The access technologies layer adapts IEEE 802.11p standards on the European version, defining its physical and MAC layer protocols. The network and transport layer defines the IP-based and geo-networking protocols, in addition to the transport layer protocols. The facilities layer manages the services and messages supporting information, applications and communications. The application layer basically defines the applications related to traffic efficiency and road safety. The management layer is a cross-layer that plays a pivotal role in controlling all of the layers. The security layer defines the protocols, ensuring the integrity, privacy, authentication and non-repudiation (Sjöberg 2011). Figure 1.5 illustrates the ETSI ITS layers.

Management	Applications	Security
	Facilities	
	Network and transport	
	Access technologies	

Figure 1.4. *ETSI TC ITS protocol stack (Sjöberg 2011)*

1.8.3. *The 3GPP standard*

The 3GPP V2X leverages traditional cellular networks to enhance the DSRC to double range for V2V communications. It also functions both in and out of cellular networks coverage via V2V communications. Moreover, it offers robust V2I and vehicle-to-network (V2N) communications (Lucero 2016). Compared with IEEE 802.11p, cellular-based V2X provides better quality of service (QoS), higher data rate and larger coverage for moving vehicles. Additionally, V2X is synchronous, while IEEE 802.11p is asynchronous. Although V2X services may coexist with IEEE 802.11p-based radio access in adjacent channels, V2X is additionally advantageous for being scalable and evolvable (Wang et al. 2017). The 3GPP V2X standard supports a frequency of up to 10 messages per second and variable payloads of 50–300 bytes; event-triggered messages have payloads up to 1,200 (3GPP (2017-03)).

1.9. Types

Vehicular networks characterize various types of networks in which the vehicles on the roads are the main type of nodes. Usually, people's familiarity with the VANET confuses them to think that all vehicular network types are VANETs. Although it is true that the VANET is the first type introduced, as time has passed, the concept has continuously evolved with the introduction of new purposes, needs and applications. VANET may now be considered as the building block of more global, sophisticated and advanced vehicular technologies and networks. Figure 1.6 depicts, in an encapsulated illustration, the vehicular networks, which are explained in the following sections.

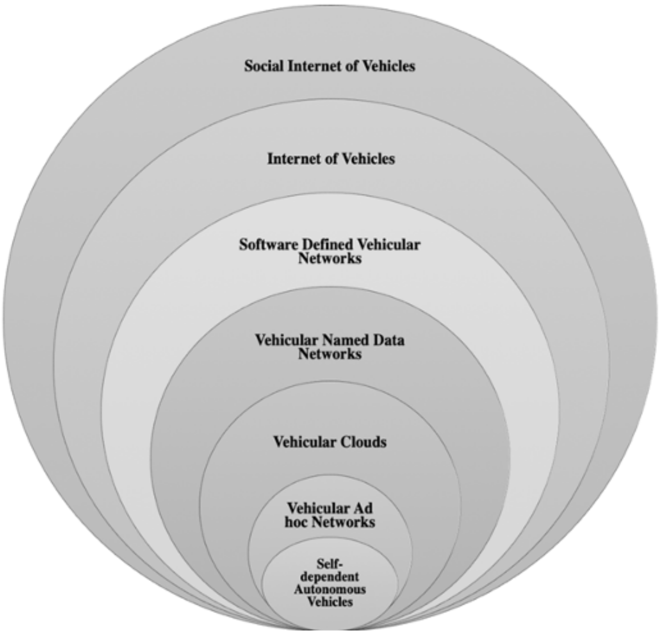

Figure 1.5. *Vehicular networks. For a color version of this figure, see www.iste.co.uk/benarous/vehicular.zip*

1.9.1. *The autonomous vehicle (self-dependent)*

The self-contained (self-dependent) autonomous vehicles rely solely on their processing abilities, artificial intelligence and sensing powers. Vehicles that are equipped with GPS, maps, cameras and radars make decisions locally. No instructions or commands are sent from distant servers or control units. Also, no network is used in the process (Glancy 2012).

1.9.2. *VANET*

The VANET or Vehicular Ad hoc Network refers to the vehicular networks composed of vehicles (OBU) and RSU as their main nodes. The communication between the vehicles is wireless through DSRC, and is known as the vehicle-to-vehicle (V2V). The DSRC is also used between the vehicle and the infrastructure (RSU), and is known as vehicle-to-roadside (V2R). The VANETs were developed primarily for safety applications to decrease road causalities, in addition to offering infotainment applications. Hence, the vehicles engender three classes of messages, which are: safety messages, also known as periodic state beacons, event-based alert messages and non-safety messages or service messages, related to information, entertainment and comfort applications (Hartenstein and Laberteaux 2010; Al-Sultan et al. 2014).

1.9.3. *Vehicular clouds*

The vehicular cloud is the road edge extension to conventional clouds. Due to this fact, each vehicle has an on-board unit that senses its surrounding environment, stores the sensed data and processes it. The sensing, processing and storing capacities may be made use of to form clouds known as VANET clouds or vehicular clouds.

Gerla (2012) suggested benefiting from vehicle storage and sensing capacities to improve traffic management. They proposed a vehicular cloud-based urban surveillance system and navigation system that saves sensed data from the road. It uses the vehicles' cameras to film roads and read the number plates of other cars. These videos and data are locally saved in the vehicle, while their descriptive meta-data saved on the Internet enables police forensic investigators to harvest them. The videos may record proofs against criminals, especially in assaults, hit-and-run accidents or bombings.

Whaiduzzaman et al. (2014) cited different applications that the vehicular clouds could offer, such as:

– **The network-as-a-service (NaaS)**: vehicles with Internet access offer it as a service to other road nodes that require it.

– **The storage-as-a-service (StaaS)**: vehicles may lease their storage capacity as a service to other road users to provide them with storage for large files.

– **The cooperation-as-a-service (CaaS)**: vehicles cooperate to gather and broadcast the data based on the interest. In other words, the data is routed based on its content to interested parties faster. Consequently, the vehicular cloud is formed of content-based clusters.

– **Computing as a service**: vehicles have sophisticated processing units that handle calculations and data treating. Unfortunately, these capacities are not exploited when vehicles are idly parked for hours each day. Hence, computing as a service was thought of to resolve this issue and benefits from the vehicles on-board units.

– **Photography-as-a-service**: vehicles with high-resolution cameras may offer better and wider road-vision than static infrastructures due to their mobility. They could deliver recorded proof on road crimes to the police and may send real-time updates on road conditions.

– **Information-as-a-service (InaaS)**: vehicles generate and process a variety of road information related to the driver's safety or entertainment. They can exchange this data on the road as a service.

The same authors classified vehicular clouds (VCs) into three types: static, dynamic and infrastructure-based. In static VCs, vehicles unify their resources and capacities while static, such as in parking lots, to offer services to users like in conventional clouds. Dynamic VCs are formed on-road by moving adjacent vehicles that combine their resources. Infrastructure-based VCs are suitable for urban areas with infrastructures distributed over roads that can form clouds with the passing vehicles. The infrastructure or RSU becomes the cloud coordinator, bridging the VC and conventional clouds.

Hussain et al. (2015) stated that vehicular clouds are more appropriate to provide infrastructure and software as services rather than offering platform-related service, noting that in clouds offering the platform as service, the user is provided with a development platform enabling them to develop remote applications. Likewise, they considered that the VANET clouds have three types, which they denoted as: vehicular clouds (VCs), the vehicle using the cloud (VuC) and hybrid vehicular clouds (HVCs). In VCs, the vehicles that are either static or dynamic combine their resources, forming a cloud offering paid services. In the VuC, the on-road vehicles use conventional cloud services, and, in HVCs, VC vehicles use conventional cloud services, i.e. HVCs combine both VCs and the VuC.

1.9.4. *Internet of vehicles*

The Internet of vehicles (IoV) is a vital part of the Internet of Things (IoT) and one of its promising instantiations (Gerla et al. 2014; Yang et al. 2014). It is the extension and evolution of VANETs. It incorporates vehicles, things, humans and the environment. The humans are people in vehicles (passenger, driver) and people in the surrounding environment, such as pedestrians and cyclists. The things refer to other entities and devices that are neither human nor vehicles, such as access points or traffic signs. The environment englobes humans, vehicles and things (Yang et al. 2014).

The IoV uses vehicular clouds as its basic technology (Gerla et al. 2014) and may rely on diverse kinds of wireless communication technologies, such as the DSRC, WIMAX, cellular networks (3G, 4G, 5G) and satellite networks. Therefore, it is able to offer more stable and global real-time and asynchronous services (Yang et al. 2014).

Mainly, the IoV has two technology directions. The first is the vehicle's networking consisting of the vehicle telematics (exchange of data), VANET and mobile Internet. The second is the vehicle's intelligence, reflecting the combination of the vehicle and the user's, as well as the use of artificial intelligence, cognitive computing and deep learning (Yang et al. 2014). Note that the IoV's vehicle is regarded as a swarm of sensors collecting road-related data, the vehicle's inner condition and its surrounding environment. The IoV's vehicle also has large storage capacities and sophisticated processing units (Bonomi 2013).

Contreras-Castillo et al. (2018) illustrated the IoV's seven-layer model, and each of these layers is briefly explained below:

– ***the user interface layer***: facilitates the interaction between the vehicle and the user. They may query the on-board system, receive notifications and use the IoV services through this layer;

– ***the data acquisition layer***: collects the data that are either sensed by the vehicles sensors or received from other vehicles and infrastructures;

– ***the filtering and pre-processing layer***: pre-processes and filters the data based on their validity, utility and used service;

– ***the communication layer***: enables the broadcast of communication and messages using different types of technologies, such as DSRC, WiMax, WiFi, 3G, 4G and 5G;

– ***the control and management layer***: uses various packet inspections and traffic management policies methods to process the received information;

– ***the processing layer***: uses the conventional clouds along with vehicular clouds capacities to store and process the received and collected data;

– ***the security management layer***: is a transversal layer that handles and ensures security properties for all other layers.

Owing to the intelligence of the autonomous vehicle and the deep learning algorithms it uses, a new paradigm has appeared, which is the cognitive IoV (CIoV), the evolution of the IoV (Chen et al. 2018). It amalgamates the intelligence of autonomous vehicles with the vehicular networks, cellular networking and cloud computing. It is more precise in terms of perceptive ability concerning the vehicle's interactions and surrounding environment. It makes more reliable decisions, and uses its resources more efficiently.

The architecture of C-IoV has five layers:

– ***sensing layer***: responsible for collecting data;

– ***the communication layer***: includes interactions related to the cloud along with communications required for the functioning of conventional vehicular networks;

– ***cognition layer***: uses data mining, machine learning, deep learning and pattern recognition to process sensed and collected data;

– ***control layer***: makes decisions in a distributed manner to ensure the vehicular networks expected QoS and faster responses;

– ***application layer***: provides a variety of applications and stable global services.

1.9.5. *Social Internet of vehicles*

After the social media networks emanation usage and knowing that the vehicle is most likely the third place people spend the majority of their time after their home and office, combining the social network with the vehicular network is now a necessity, in which passenger and drivers share road-related real-time events such as accidents, road works, café and restaurants offers, new gyms and shops or beautiful sceneries (Lequerica et al. 2010). This procreated a social vehicular network, more precisely, the social Internet of vehicles (IoV), which is a special case of Social IoT.

The social IoV is described as the social interactions between drivers and vehicles. It is also stated as a network created by the drivers within the same area with similar interests. Likewise, it is defined as the interactions between autonomous vehicles and interchange services and data (Maglaras et al. 2016). Alam et al. (2015) defined the social IoV as "a cyber-physical application over the physical vehicle networks of WAVE", in which the home, RSU and OBUs exchange data over cyber-physical formed social networks. The data interactions form a social graph where the graph nodes represent the entities and the graph links represent the exchanged data (Alam et al. 2015).

Nevertheless, Maglaras et al. (2016) asserted that in the future the social IoV will be defined as the social interactions of passengers, drivers and vehicles. It will allow the ranking of vehicles based on a set of characteristics. The ranking will help in making interaction decisions, and may be used to build trust and reputation, which are essential security properties in vehicular networks.

1.9.6. *Data named vehicular networks*

An information-centric network on wheels, or IC-NoW, is a vehicular network in which the data routing is based on information content rather than the usual IP addressing methods. The scope of information is defined by its time, space and user's interest relevance. It is referred to as a vehicular NDN, or named data vehicular network (Bai and Krishnamachari 2010).

The exchanged packets between roadside units and vehicles are information-centric, which means that they are shared among users with similar spatiotemporal and interest scope. However, these networks are still not completely independent of the IP-based networks. The IC-NoW encapsulates the packets exchanged via V2V, V2I within IP packets before sending them over the Internet (Bai and Krishnamachari 2010).

Note that each NDN node possesses three types of data structures: content store (CS), pending interest table (PIT) and forwarding information base (FIB). A vehicle interested in a packet sends an interest packet (IntPk). If the CS has the requested content, the requester receives a DataPk. Otherwise, the IntPk is added to the PIT to be forwarded to a potential CS from the FIB (Chen et al. 2014; Bouk et al. 2017).

1.9.7. *Software-defined vehicular networks*

In software-defined vehicular networks (SDVN), the centralized control plane logically controls the data communication. The difference between the SDVN and vehicular NDN is that the latter focuses on content-based routing of data, while SDVNs separate the control and data plane to make various services manageable without physical interference with switches and routers. Note that the vehicles in SDVN have multiple interfaces (Ahmed et al. 2017).

The SDVN consists of:

– an SDN controller, which has an overall view of the networks. It coordinates its elements to perform the NDN operations, which are intelligent interest, cashing, data forwarding and so on;

– cashing, which is an ultimate task performed by forwarding nodes. The forwarding nodes selection and the format of the cashed content are essential to ensure instant query/response. The content formats are compressed, non-compressed and chunked, saved entirely in a single or multiple node(s);

– content naming, which is another fundamental component that labels the contents and their chunks. This labeling smoothes the data search upon the vehicle’s reception of an interest request, noting that each content has a specific spatiotemporal frame validity;

– intelligent forwarding: the FIB maintains the content communication. With this in mind, a face is ranked every time some content is satisfied through it. The face rank is dropped each time it does not satisfy an interest. If no interest is satisfied through this face, it gets purged from the FIB. If the FIB is empty, the requests are forwarded to the controller to be satiated;

– push-based forwarding, which delivers warnings constantly to potentially interested nodes;

– intrinsic data security: data messages are digitally signed. The SDN controller spreads the content security policies to interested vehicles;

– congestion control: congestion occurs because of certain contents’ popularity. Thus, to alleviate congestion, each node has to send the traffic status at every face to evenly distribute the traffic over diverse cashing points;

– a topology indicator: each vehicle postulates its position, direction and speed to the control manager so that it can settle on the forwarding rules and disseminate them;

– a content prefix manager: every node sends its content store (cashed data) with its validity and expiry to the controller to help in forwarding the interest requests;

– the vehicle calculates state information at each interface. It sends a report about the requests and satisfied queries so that the controller can improve the cashing/forwarding policy (Lutterotti et al. 2008).

1.10. Test beds and real implementations

Middlesex University in the United Kingdom built the Middlesex VANET Research Testbed located at Hendon Campus in London. It has four RSUs fixed on different buildings. The test bed evaluates studies done by the developing team on VANET[1].

The Porto Living Lab in Portugal built a couple of independent test beds for VANET: harbor and urban, sited in the harbor and city of Porto respectively. In both

1 See: https://mdxminds.com/2016/01/11/the-future-of-driving-is-here/.

urban and harbor test beds, vehicles are equipped with OBUs, GPS receivers, DSRC, cellular and Wi-Fi communication interfaces. Vehicles connect to the Internet using cellular communications or through RSUs. The DSRC is used in V2V and V2I communications. In the urban test bed, most of the deployed RSUs were mounted on traffic light poles, control camera poles and buildings managed by the University of Porto[2].

The C-VeT vehicular test bed has been developed by UCLA-USA to evaluate MAC and network layer protocols and models. The CarTel and Cabernet test beds were developed by MIT-USA. Massachusetts Amherst-USA also developed two projects named Dome and DieselNet (Lutterotti et al. 2008). In 2008, Microsoft established its VANET Test bed called VanLan[3]. ITS corridor is another in-progress project from Amsterdam, passing by Germany to Vienna[4].

Among the European accomplished projects are SimTD (2013)[5], DRIVE C2X (2014)[6] and Compass4D (2016)[7]. Similarly, over 200 ITS-related projects are ongoing in Canada, two of which are at the Universities of Alberta and British Columbia (Lawson et al. 2015).

1.11. Services and applications

The vehicular networks aim to safeguard users' safety, ensure comfortable driving, maintain sleek traffic, reduce consumption of fuels and pollution of air, etc. They offer varied services and applications such as (Meraihi et al. 2008; Kumar et al. 2013; Al-Sultan et al. 2014; Seuwou et al. 2014):

– **Safety application**: has the top priority due to its role in preventing accidents and saving human lives. Among its examples are:

- accident alerts: prevent road causalities engendered from accidents that have already occurred. It speeds up the response by rescue services (Ambulance, Police). It facilitates the evacuation of the road and assists secondary roads and detour planning,

- cooperative driving: improves traffic management and reduces fuel consumption. It is known as vehicle platooning,

2 See: http://cordis.europa.eu/result/rcn/188104_en.html.

3 See: https://www.microsoft.com/enus/research/project/vanlan-investigating-connectivity-from-moving-vehicles/.

4 See: http://c-its-korridor.de/?menuId=1&sp=en.

5 See: http://www.simtd.de/index.dhtml/enEN/news/Presse.html.

6 See: http://www.drive-c2x.eu/project.

7 See: http://www.compass4d.eu/.

- collision avoidance: to avoid crashes and bumps, vehicles detect road obstacles by using their in-built sensors, lidars and radar and swiftly respond. Furthermore, vehicles disseminate accurate real-time information about current position, headings and speed, in order to avoid the collision, especially when doing U-turns, changing lanes, suddenly braking, etc.,

- security distance warning: the vehicles maintain a safety distance that is either preliminarily set as a few meters or dynamically adequate to vehicles' sudden brake response time. This distance also depends on the speed of the vehicle. The warning is sent when the vehicles do not keep to the defined security distance,

- lane changing: the vehicle alerts other vehicles when it is changing its lane to avoid collisions and accidents. This alert emulates the turn sign in manual driving,

- navigation and map location: the majority of recent vehicles come with a navigation system that corrects the users' location obtained from GPS with their in-built map so that they can plan their trajectories,

- traffic jam and road work alerts: these event-based messages propagate in the network to assist users in planning secondary routes,

- public safety (SOS, post-crash warning, nearing emergency vehicle, etc.),

- vehicle diagnostic and maintenance: vehicles can have on-road diagnosis. If an issue is detected, early reports are sent to the closest car care center for more efficient and prompt service provision.

– **Comfort application**: ensures the users' entertainment and comfort, such as:

- Internet access, chat between car users, video streaming, network games and other advanced stable services,

- weather forecasts and alerts,

- advertisement messages regarding close, affordable or ranked hotels, gyms, restaurants, gas stations or tourist spots, etc.

– **Driver assistance**: assists the driver through the provision of crucial warnings and aid information. A few examples of its applications are:

- parking spot reservation and parking management,

- automatic parking,

- self-driving vehicle (driverless cars): a vehicle is totally autonomous when it is driven solely by its system; it is semi-autonomous if the driver's intervention is still needed in driving. Figure 1.7 depicts the automated driving levels that are explained below (Maglaras et al. 2016; Wang et al. 2017):

– *level 0*: a human driver is needed to drive and monitor the vehicle's surrounding environment,

– *level 1*: the driving system assistance is either in steering ***or*** acceleration/deceleration based on the actual driving environment,

– *level 2*: the driving system assists both acceleration/deceleration ***and*** steering based on the actual driving environment,

– *level 3*: the driving system interferes in the dynamic driving tasks based on the surrounding environment, while drivers sort and respond to the requests of intervention they receive from the system,

– *level 4*: the driving system interferences in the dynamic driving tasks are with or without the driver's approval, based on the driving environment,

– *level 5*: the driving system executes the entire dynamic driving tasks, emulating the human driver.

<table>
<tr><td rowspan="3">Human Driver Monitors the driving environment</td><td>0</td><td>No Automation</td></tr>
<tr><td>1</td><td>Driver Assistance</td></tr>
<tr><td>2</td><td>Partial Automation</td></tr>
<tr><td rowspan="3">Automated driving System Monitors driving environment</td><td>3</td><td>Conditional Automation</td></tr>
<tr><td>4</td><td>High Automation</td></tr>
<tr><td>5</td><td>Full Automation</td></tr>
</table>

Figure 1.6. *Automated driving levels (Litman 2018)*

1.12. Public opinion

In the report presented by Schoettle and Sivak (2014), the public's opinion about autonomous and self-driving vehicles was surveyed in the United States, the United Kingdom and Australia. The plurality of respondents were acquainted with the technology or at least acknowledged its existence. While most of them showed their high expectations about it, they also voiced their concerns about it in terms of security, privacy and reliability, in addition to their concerns about the vehicle's self-dependency and absence of human intervention, questioning whether it can emulate human driving skills. Unlike the men, the women expressed more concerns about this technology and were more cautious about it. Lastly, at the time of the survey, the majority of respondents were reluctant about paying extra fees to obtain it, despite being interested in it.

The Office of the Privacy Commissioner of Canada conducted a similar survey where over one-third of Canadians expressed their concerns about their privacy if they were to use these connected cars. Similarly, over half of the respondents preferred their privacy over the advantages of connected car services. In a more recent poll conducted in the United States, Spain, Germany and the United Kingdom (Lawson et al. 2015), the respondents also voiced their concerns about their privacy and personal data, insisting that the vehicle is their private space, emphasizing the importance to protect them.

1.13. Conclusion

This chapter explains vehicular networks, their purpose, underlying technologies and offered applications. Moreover, it stated the vehicular networks evolutions and types. It concluded with a survey of public opinion illustrating the users' hesitation about VN technology and concerns about their confidentiality, as well as the VN reliability from a technical perspective.

Indeed, it is an undeniable fact that both privacy and security are equally important in vehicular networks. Likewise, they are also among the key issues hindering vehicular network market penetration and they top the end-users' concerns. The following chapter explains these issues and surveys the existing solutions to preserve them.