is MANET, or *Mobile Adhoc Networking.*

Mobile Ad Hoc Networks (MANETs) are wireless mobile nodes that cooperatively form a network without infrastructure. Because there is no coordination or configuration prior to setup of a MANET, there are several challenges which include: routing packets in an environment where the topology is changing frequently, wireless communications issues, and resource issues such as limited power and storage. The leading way to research solutions to these difficult MANET challenges is simulation, which is discussed in more detail in chapter 3.

In a MANET, the quality or even availability of a mobile connection strongly relies on the position of the receiver relative to the field of other antennas. We can think of such a network like a honeycomb, where every antenna covers one of the cells. Almost by definition, a network like that has weak spots once it is built, because in the real world it has to coexist with geographical hinderances as forests, roads and rivers. In some areas it is not even realistic to try to build such a network, if only because it is impossible to supply the required amount of energy to the antennas (not to mention the uplink to the telecom infrastructure). Even satellite telephony - though very useful in certain situations - is not the definite answer to this problem, as the capacity is limited and there are situations (for instance underground or up in the air) where the phone cannot 'see' the satellite. Here we come to the point where we can learn a number of things from the internet: when two computers are communicating with each other on the internet, neither one is more important than the other. Well, in a cellular network the phone is subservient to the network: even if two phones are used right next to each other, any connection they make is always via the network and the field antennas and, yet, a mobile phone is as much a broadcast device as it is a receiver (we can talk and listen at the same time). A second useful attribute is the aspect of *flexibility of the connections* for information flows: nodes on the internet (routers) continually learn what connections other nodes are available. With a mobile network perhaps this information exchange should happen at a higher frequency because the individual nodes are free to move, and the availability of connections would therefore vary faster, but the method is still valid.

Now we should get a reasonably good idea of how MANET will eventually be used: mobile devices that form a peer-to-peer network for the exchange of data, or channel through speach or data to the telecom network when there is no other route available.

Furthermore, this technology could generate interesting new business models, because the end users could under certain conditions bypass commercial networks (as when you are standing next to each other). For filesharing and other peer-to-peer services MANET can surely add something to the possibilities of the currently available technologies such as 3G (UMTS and by products). Obviously, MANet itself as a technology is still young and its final impact strongly relies on the way in which both the world of telecommunications and the hardware suppliers will act on its appearance on the scene.

2.2 Vehicular Ad-hoc NETwork (VANET)

The basic concept of VANET is straightforward: take the widely adopted and inexpensive wireless local area network (WLAN) technology that connects notebook computers to each other and the Internet, and, with a few tweaks, install it on vehicles. Of course, if it were truly that straightforward, the active VANET research community would likely have never formed and this thesis would have never been written.
If vehicles can directly communicate with each other and with infrastructure, an entirely new paradigm for vehicle safety applications can be created. Even other non-safety applications can greatly enhance road and vehicle efficiency. Second, new challenges are created by high vehicle speeds and highly dynamic operating environments. Third, new requirements, required by new safety-of-life applications, include new expectations for high packet delivery rates and low packet latency. Further, customer acceptance and governmental oversight bring very high expectations of privacy and security. Even today, vehicles generate and analyze large amounts of data, although typically this data is self-contained within a single vehicle and with a VANET, the horizon of awareness for the vehicle or driver drastically increases. Communication in VANETs can be either done directly between vehicles as one-hop communication, or vehicles can retransmit messages, thereby enabling the so called multihop communication. In order to increase coverage or robustness of communication, relays at the roadside can be deployed. Roadside infrastructure can also be used as a gateway to the Internet and, thus, data and context information can be collected, stored and processed somewhere (e.g. the upcoming *Cloud Computing*[1]). It warrants repeating that the interest in ve-

[1] Cloud computing is a way of computing, via the Internet, that broadly shares computer resources instead of using software or storage on a local PC. A technical definition is *"a computing capability that provides an abstraction between the computing resource and its underlying technical architecture*

hicular inter-networks is strongly motivated by the wealth of applications that could be enabled. First of all, active safety applications, i.e., accident prevention applications, would benefit from this most direct form of communication. Second, by collecting traffic status data from a wider area, traffic flow could be improved, travel times could be reduced as well as emissions from the vehicles. As it was concisely stated as the tenet of the Intelligent Transportation System World Congress in 2008: save time, save lives. The application classes Safety and Efficiency can be used to classify applications based on their primary purpose (Cfr. chapter 4, "Data dissemination survey"). However, the aspects of safety and efficiency cannot be seen as completely disjoint sets of features. Obviously, vehicle crashes can lead to traffic jams.1 A message reporting an accident can be seen as a safety message from the perspective of near-by vehicles. The same message can be seen by further-away vehicles as an input to calculate an alternative route within a transport efficiency application.
While being conceptually straightforward, design and deployment of VANET is a technically and economically challenging endeavour. As described in the following chapters, key technical challenges include the following issues:

- *Inherent characteristics of the radio channel.*
  VANET present scenarios with unfavorable characteristics for developing wireless communications, i.e., multiple reflecting objects able to degrade the strength and quality of the received signal. Additionally, owing to the mobility of the surrounding objects and/or the sender and receiver themselves, fading effects have to be taken into account.

- *Lack of an online centralized management and coordination entity.*
  The fair and efficient use of the available bandwidth of the wireless channel is a hard task in a totally decentralized and self-organizing network. The lack of an entity able to synchronize and manage the transmission events of the different nodesmight result in a less efficient usage of the channel and in a large number of packet collisions.

(e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." - (Cloud Computing Definition, National Insitute of Standards and Technology, Version 15, `http://csrc.nist.gov/groups/SNS/cloud-computing/index.html`)

- *High mobility, scalability requirements, and the wide variety of environmental conditions.*
  The challenges of a decentralized self-organizing network are particularly stressed by the high speeds that nodes in VANET can experience. Their high mobility presents a challenge to most iterative optimization algorithms aimed at making better use of the channel bandwidth or the use of predefined routes to forward information.

- *Security and privacy.*
  There is a challenge in balancing security and privacy needs. On the one hand, the receivers want to make sure that they can trust the source of information. On the other hand, the availability of such trust might contradict the privacy requirements of a sender.

- *Standardization versus flexibility.*
  Without any doubt, there is a need for standardizing communications to allow VANET to work across the various makes and brands of original equipment manufacturers (OEMs). Yet, it is likely that OEMs will want to create some product differentiation with their VANET assets. These goals are somewhat in tension.

From an application and socio-economic perspective, key challenges are as follows:

- Analyzing and quantifying the benefit of VANET for traffic safety and transport efficiency. So far, relatively little work has been done to assess the impact of VANET as a new source of information on driving behavior. Clearly, the associated challenge in addressing the issue of impact assessment is the modelling of the related human factor aspects.

- Analyzing and quantifying the cost/benefit relationship of VANET. Because of the lack of studies on the benefits of VANET, a cost/benefit analysis can hardly be done.

- Designing deployment strategies for this type of VANET that are not based on a single infrastructure and/or service provider. Owing to the network effect, there is the challenge of convincing early adopters to buy VANET equipment when they will rarely find a communication partner.

- Embedding VANET in intelligent transportation systems architectures. VANET will be a part of an intelligent transportation system where other elements are given by traffic-light control or variable message signs. Also public and individual transportation have to be taken into account in a joint fashion. Therefore, truly cooperative systems need to be developed.

As can be seen from the above lists of technical, application, and socio-economic aspects, the field of vehicular application and inter-networking technologies is based on an interdisciplinary effort in the cross section of communication and networking, automotive electronics, road operation and management, and information and service provisioning. VANET can therefore be seen as a vital part of Intelligent Transportation Systems (ITS).

2.3 Network requirements in VANETs applications

This section aims to be a very light introduction to the main technological requirements of vehicular networks which, in most of the cases, need to cover many needs for their efficient operation. In this section we will treat only the most important ones.

2.3.1 Mobility

Wireless network technologies allow devices to move freely. However, this mobility affects the potential permanent access to the network (see the previous point) and causes other problems. In (102), experimental evaluations give real results of these effects. In 802.11 transmissions the distance between the sender and receiver is an important factor; the more the distance, the smaller the probability of reception of packets (24). In infrastructure-based technologies, handoffs between base stations are also relevant, due to the potential decrease of performance in the process. Poor latency and throughput results are obtained if the mobile terminal is moving at locations far away from other nodes without performing a handoff (42). Nevertheless, the distance between two devices during the communication is not the only noticeable effect of mobility. Interference with other radio equipments in the case of VANET should also be taken into account, due to the wide usage of the 2.4 GHz frequency band (102). The presence of the equipment at locations of bad orography could also cause communication problems in vehicular networks. Other external factors, like the existence of other

vehicles or buildings are considered in realistic mobility patterns for VANET solutions (69).

Mobility will be examined in more detail in chapter 2 ("Mobility models in vehicular

Applications\App. Req.	Location awareness	Geocast capability	Penetration rate dependence	Time awareness	Permanent access	Mobility
Safety						
Cooperative Collision Warning	**	**	**	**	*	**
Incident management	**	**	**	**	*	**
Emergency video streaming	**	**	**	**	*	**
Traffic management and monitoring						
Platooning	**	**	**	**	*	**
Vehicles tracking	*		*	*	**	*
Notification Services	*		*	*	*	*
Comfort						
Parking place management	**	**	*	*	*	**
Distributed games and/or talks	*	**	**	*	*	**
Peer-to-peer	*		*	*	**	*

Figure 2.1: Application requirements in VANETs. Please, note that no asterisk means "none or not needed" requirement,"*" means "needed", "**" stands for "suited" requirement.

networks") and chapter 3 ("Vehicular Network Simulators").

2.3.2 Permanent access

Permanent access to the network is *one of the main drawbacks of vehicular communications*. In VANET designs, a physical infrastructure is not necessary, due to the inherent decentralized design. As it concerns infrastructure-based networks, operators do not offer the same service over the entire terrestrial surface. For instance, over urban environments, the coverage is excellent, and the amount of base stations where the mobile terminal could be connected is really high. At rural locations, however, the deployment is poor. A vehicle equipped with a VANET system, however, is always able to emit messages because the vehicle itself is part of the infrastructure. Furthermore, in cellular network connections, it is also important to differentiate between two important concepts regarding the access to the network: *coverage* and *capacity*. The coverage can be understood as the possibility of the mobile terminal to use the network, because at a particular location operators have deployed the necessary infrastructure. However, the user can be rejected to establish a call or a data connection, even in good coverage circumstances, if the capacity of the network has been exceeded. Depending on several

technological issues, such as modulation, frequency allocation, time slot scheduling, etc., this effect has a different impact. According to this, the number of users who are concurrently using the network restricts the potential cellular network usage. At the application level, some services such as file transfer or download, need a permanent communication channel. In this kind of applications, the election of a suited vehicular network is essential.

2.3.3 Location Awareness

Next generation vehicles are expected to exchange information not only beyond their immediate surroundings and line-of-sight with other vehicles, but also with the road infrastructure and Internet databases. This will allow vehicles to anticipate trajectories, coordinate merging manoeuvres, notify a braking action to vehicles behind, warn oncoming traffic of an icy patch, report road traffic conditions, locate parking lots, or simply entertain passengers. In this context, the knowledge of their actual position and trajectory is necessary, and it is only meaningful to vehicles in a particular geographic area. The exchange of information among vehicles in a particular geographic area requires reliable and scalable communication capabilities, which we call geographical routing and addressing. This function mainly rely on the information given by GPS receivers. However, GPS imposes some constraints such as lack of coverage in some environments or its weak robustness for some critical applications. For these reasons, other positioning techniques such as cellular or WiFi localization, dead reckoning (by using last known position and velocity) (94), and image/video localization, have been proposed in the vehicular field (16). Critical safety services such as alert cooperative collision warning and incident management need a high accurate localization, as well as some comfort applications such as parking booking. Note that an accurate positioning system can help us to define the zone of relevance more precisely. Other services, however, require a low accurate localization, like peer to peer applications and vehicle tracking.

2.3.4 Time Awareness

Vehicular applications often require a reliable communication channel that supports time-critical message transmissions (41). One of the most important criterions for

measuring the quality of the network, regardless of the application type, is the communication delay. Although most applications have time constraints, those related with road safety are critical. Due to this, a challenge in vehicular networks is providing a real-time behaviour. In order to enable the driver to react quickly, the information must reach the destination in a very small delay following the event. However, this requirement is not easy to ensure in mobile networks. This difficulty is even greater if we consider vehicular network characteristics, particularly, the high mobility. Thus, real-time communications can only be assured by the presence of an efficient and robust communication system.

2.3.5 Penetration rate dependency

Penetration rate is defined as the percentage of vehicles equipped with the necessary *on board data unit (OBU)* on the road. This parameter may have important consequences in the operation of some applications, especially the critical and safety ones. Although a low penetration rate is obviously a problem in safety applications, such as collision avoidance, an excess of equipped vehicles also arises transmission problems. However, applications such as comfort do not have to be too much aware of this factor. In cellular networks, situations of high penetration are also a problem. The system performance is not affected when the number of equipped vehicles is low, but in high load circumstances, the network connection starts to give a poor performance when the time slot scheduler need to serve too much users (52). Note that penetration rate has a direct bearing on the wireless bandwidth used. The higher the penetration rate, the higher the wireless bandwidth should be used to allow vehicles to communicate.

2.3.6 Geocast capability

Geocast provides the capability to deliver a message to nodes within a geographical region (62). The shape and size of this area depend on the application aims. The complexity of defining this region can be as high as the set of vehicles behind or in front of the subject one. Other times this constraint is relaxed, and defining this region as the vehicles inside a geographic area, or near a designated spot (such as a smog area), is enough. In order to advocate a general communication architecture, where services which require both unicast and geocast capabilities can be deployed, an hybrid networking architecture can be proposed. This way, services such as platooning, which needs

Technology	Range	Link type	Data rate	Frequency band	Standard	Vehicular applicability		
						V2V	V2I	I2V
Bluetooth	100 m	1-to-n	1 Mbps	2.4 Ghz	IEEE 802.15.1	✶		
WLAN	200 m	1-to-1 1-to-n	10-50 Mbps	2.4,5 Ghz	IEEE 802.11a/b/g	✶✶	✶	✶
DSRC	1 Km	1-to-1	50 Mbps	5.9 Ghz	IEEE 802.11p	✶✶	✶✶	✶✶
WiMAX	10 Km	1-to-n	∼20 Mbps	2.4,5 Ghz	IEEE 802.16e		✶✶	✶✶
Cellular	10 Km	1-to-n	∼10 Mbps	700-2600 Mhz	n/a		✶✶	✶✶
RDS/TMC	80 Km	1-to-n	1187.5 bps	87.5-108.0 Mhz	CENELEC EN 50067 CEN ENV 12313			✶✶
Satellite	>10.000 Km	1-to-n	300-500 Kbps	950-1450 Mhz	n/a		✶	✶✶

Figure 2.2: Geocasting forwarding schemes. Typical geocasting forwarding schemes: *unicast* (A), *broadcast* (B) and *topologically scoped broadcast* (C).

unicast communications, do not experience bad performances. Geocast is considered efficient if the information is forwarded in both sparse and dense geographical areas, while efficiently leveraging the available bandwidth. This criterion, scalability, was introduced in (70), and it was defined as the ability to handle the addition of nodes or objects without suffering a noticeable loss in performance or increase in administrative complexity.

2.4 VANETs' common communication schemes

Connectivity necessities of vehicles can be divided in two main groups: vehicle to *vehicle communications (V2V)* or *inter-vehicle communications (InV)*, and *communications with the infrastructure (V2I)*. In the literature, many authors use V2I to denote both data flow directions, however, according to the specific use of several technologies for one or the other communication pattern, it is more correct to distinguish between V2I and I2V (infrastructure to vehicle communications). It is important to consider this whole set of communication possibilities for vehicles because, depending on the application or service necessities, we will have to decide among one of the available wireless network technologies. Apart from the communication pattern covered, wireless communication technologies can be divided into those which establish 1-to-1 physical links, and those which consider 1-to-n broadcast ones. In this last case, some kind of access point is in charge of sharing out the available bandwidth among the clients. This bandwidth, thus, could become insufficient when the number of served nodes increase inside the coverage area. Due to this, the tendency in short-range wireless technologies is taking advantage of the available bandwidth, sharing it among a small number of

users because, anyway, the coverage is small. On the contrary, wide-range technologies must share the available bandwidth among much more users. However, short-range wireless media lack on stability, due to the small accessible area. It is also important to remark how V2V communications are obtained by means of 1-to-1 technologies, and communications with the infrastructure are commonly created using the 1-to-n ones. A brief overview of main wireless technologies used in the vehicular domain is given in Table 2.6. For communications with the infrastructure, it is said that WLAN, DSRC, WiMAX, cellular and satellite are feasible. However it is important to remark the different application they cover in this domain. In the case of WLAN/DSRC, vehicles usually connect with local roadside units, what usually is called vehicle to road side communication.

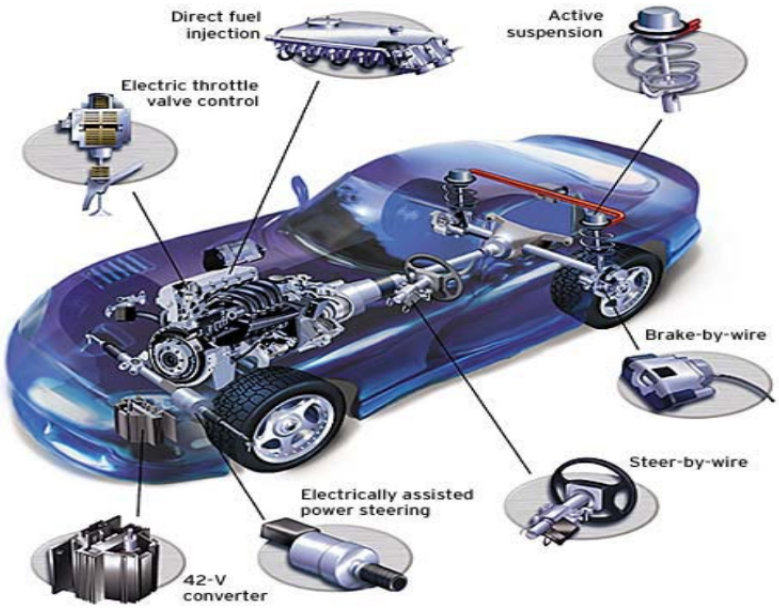

Figure 2.3: InV communications. The InV communication scheme is mainly used to create a specialized sensor networks within the vehicle. It is very useful when you want to control vehicle's on board devices and, at the same time, act on the motion behaviour in response to a received emergency message. (Mercedes Benz, SL 500 - source: Daimler Benz)

On the other hand, in the WiMAX/cellular case it is used a medium range 1-to-n network, and in satellite communications a wide range 1-to-n model is applied. In the

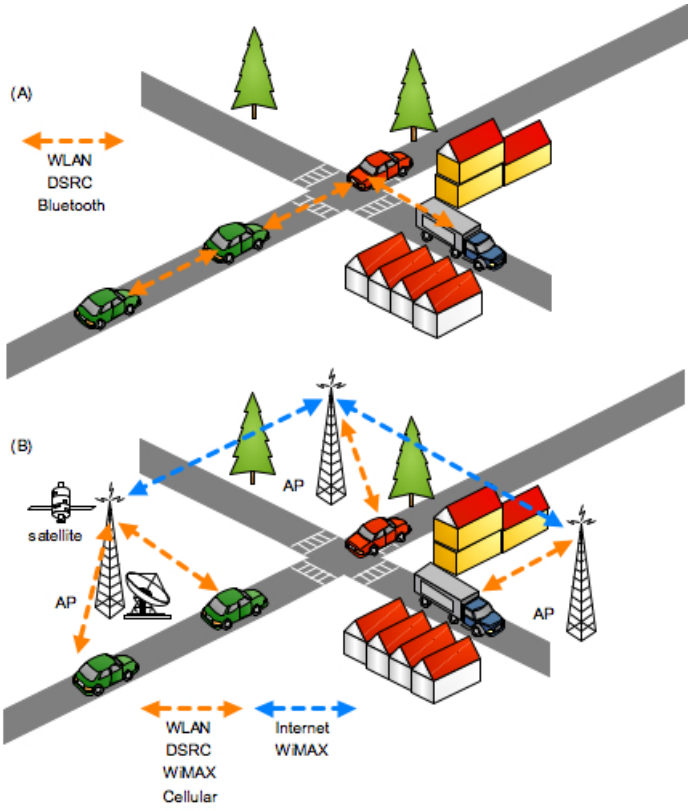

Figure 2.4: Communication schemes in VANETs. The figure shows the communication schemes typically used in a VANET: (a) Vehicle-to-Vehicle (V2V), (b) Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V).

cellular and satellite cases the design of the network is even more fixed than with any other technology, because we have to use the operators installations. This way, service providers usually consider the direct Internet connection offered by the operator, and there is no possibility to manage data traffic inside the operators network.

2.5 Communication technology in VANETs

With the rapid development of information technologies, there are a number of wireless technologies which are potential for wireless InV, V2V and V2I communications, (cfr. Table 2.2). These new technologies could be used for data exchange between users devices and vehicles, among vehicles, and between vehicles and infrastructure. The details of application scenarios of data exchange with each technology are listed in two

tables as well. DSRC is the recent technological trends to provide real time traffic information for effective implementation of ITS. Thus, in the following subsection, we focus on introducing the new technologies of DSRC for vehicular networks.

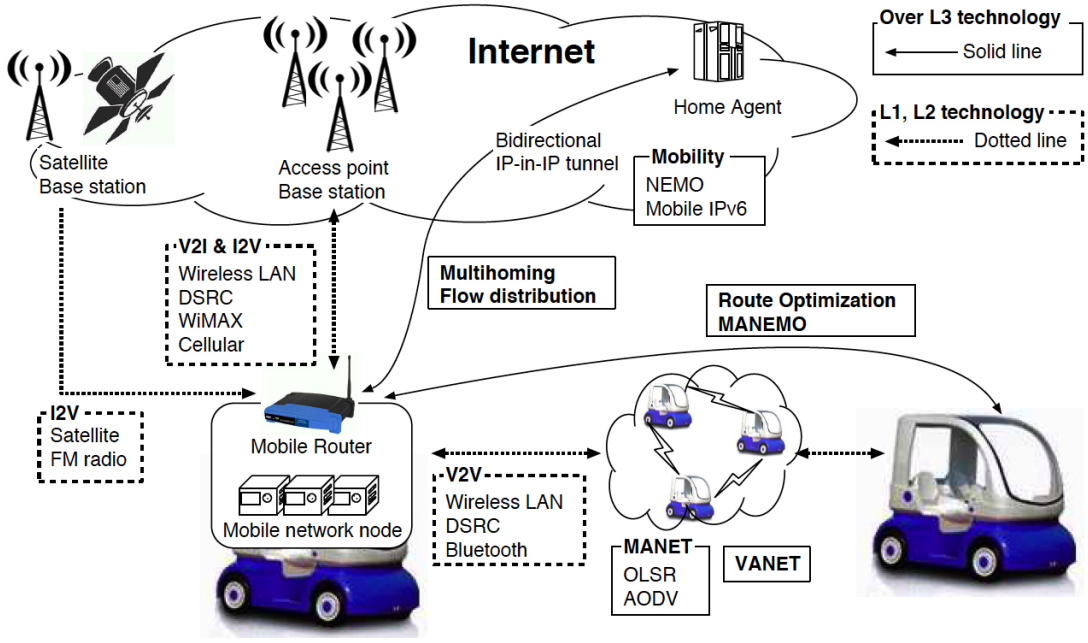

Figure 2.5: Overview of the application of network technologies used in vehicle ad-hoc networks. The figure shows a vehicular networking scheme where the most important technologies at level-three are included in an integral communication solution. Finally, an overlay architecture using cellular networks shows the feasibility of this technology to enable vehicular communications.

2.5.1 WLAN - IEEE 802.11

At the end of the 1990s the first devices appeared on the market using a new wireless local area network technology that is commonly referred to today as WLAN (Wireless LAN) or Wi-Fi.

Wi-Fi is specified by the IEEE in the 802.11 standard and mantained by the IEEE LAN/MAN Standards Committee (IEEE 802)[1]: it is very similar to the 802.3 fixed line Ethernet standard and reuses all protocol layers down to layer 2. The major difference between the two protocols is on layer 1, where the fixed line medium access has been

[1]http:\\www.ieee.org

	ZigBee	UWB (ultra-wide band)	Bluetooth	Wireless USB (Universal Serial Port)	Wireless CAN
Standard/ Technology	Ratified in December 2004	Transmitting information spread over a large bandwidth (>500 MHz)	First launched (1998)	Short-range, high-bandwidth based on the WiMedia Alliance's UWB	CANRF (CAN over RF)/ CAN Bridge
Coverage	10 and 75 meters	< 60 cm for a 500 MHz wide pulse, < 23 cm for a 1.3 GHz bandwidth pulse	1 meter, 10 meters, 100 meters	480 Mbit/s at up to 3 meters and 110 Mbit/ s at up to 10 meters	/ 500 feet (152.4M)
Bit Rate	20-250 kbit/s per channel	extremely high data rates 1000+ Mbps	3 Mbit/s (Version 2.0 + EDR) 53-480 Mbps (WiMedia Alliance (proposed)	480 Mbit/s at distances up to 3 meters and 110 Mbit/s at up to 10 meters	20kbps/ 52.8kbps-164.4kbps
Applications	Entertainment, smart Lighting control, advanced temperature control, safety & security, sensors, etc	Used at very low energy levels for short-range high-bandwidth communications by using a larger portion of the radio spectrum	Connect and exchange information between devices such as mobile phones, laptops, personal computers, video game consoles, etc	Game controllers, digital cameras, MP3 players, hard disks and flash drives. Also suitable for transferring parallel video streams.	Communication among sensors and ECUs

Figure 2.6: Wireless technologies for InV communications.

replaced with several wireless variants. Furthermore, some additional management features were specified that address the specific needs of wireless transmissions that do not exist in fixed line networks, such as network announcements, automatic packet retransmission, authentication procedures and encryption. Over the years, several physical layer standards were added to increase transmission speeds and to introduce additional features. Devices are usually backwards-compatible and support all previous standards to enable newer and older devices to communicate with each other.

Initially, Wi-Fi was not very popular or widely known as network interface cards were expensive and transmission speeds ranged between 1 and 2 Mbit/s. Things changed significantly with the introduction of 802.11b, which specified a physical layer for transmission speeds of up to 11 Mbit/s. Network interface cards became cheaper and devices appeared that could be connected to PCs and notebooks over the new high-speed USB (Universal Serial Bus) interface. Prices fell significantly and Intel decided to include Wi-Fi capabilities in their Centrino notebook chipsets. At the same time, the growing popularity of high-speed DSL and TV cable Internet connectivity made wireless networking more interesting to consumers, since the telephone or TV outlet was and still is often not close to where a PC or notebook is located. Wi-Fi was the ideal solution to this problem and Wi-Fi access points were soon integrated into DSL and cable

modems. Likewise, Internet access in public places such as cafes, hotels, airports and so on became popular, again enabled by Wi-Fi and cheap high-speed Internet access at the other end of the wireless connection via DSL. Today, Wi-Fi has become ubiquitous in notebooks and many other mobile and portable devices such as game consoles, mobile phones, Internet tablets and Mobile Internet Devices (MID).
Over time, two additional physical layer specifications were added to further increase transmission speeds. The 802.11g standard increased data transfer speeds to up to 54 Mbit/s on the air interface, and the recent 802.11n standard has the potential for up to 300 Mbit/s. It should be noted at this point that these speeds are only theoretical and not measured on the air interface. In practice, protocol overhead reduces the achievable speeds at the application layer to about half those values and, especially when applied to vehicular networks, this may lead to very poor communication efficiency. Standard 802.11a is another Wi-Fi air interface variant, but has never gained much popularity because it does not use the same standard frequency band as the other 802.11 variants. Very important topic (which are out of the scope of this work) are *Wi-Fi security* and, due to the popularity of Wi-Fi and the growing use of the technology for real-time applications such as VoIP and video streaming, *quality of service (QoS)*.
As vehicular networks make intensive use of this technology, it is worth to see in more detail the 802.11 protocol family:

802.11-legacy

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band. Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

802.11a

This standard uses the same data link layer protocol and frame format as the

original standard, but an OFDM[1] based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput of 20 Mbit/s. Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However,

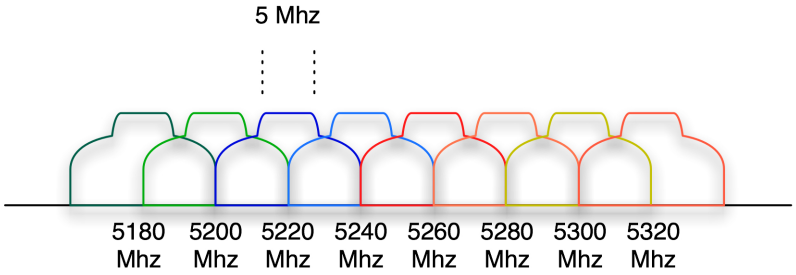

Figure 2.7: 802.11a channels.

this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference. *In Italy it is forbidden to use 802.11a techonology due to high RF intereferences with militar radars and strategical devices.*

[1] *Orthogonal frequency-division multiplexing (OFDM)* is a frequency-division multiplexing (FDM) scheme utilized as a digital multi-carrier modulation method. A large number of closely-spaced orthogonal sub-carriers are used to carry data. The data is divided into several parallel data streams or channels, one for each sub-carrier. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase-shift keying) at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth. OFDM has developed into a popular scheme for wideband digital communication, whether wireless or over copper wires, used in applications such as digital television and audio broadcasting, wireless networking and broadband internet access. The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions (for example, attenuation of high frequencies in a long copper wire, narrowband interference and frequency-selective fading due to multipath) without complex equalization filters. (source: http://www.wikipedia.com)

802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology. 802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by $\sim$ 21%. The then-proposed 802.11g standard was rapidly

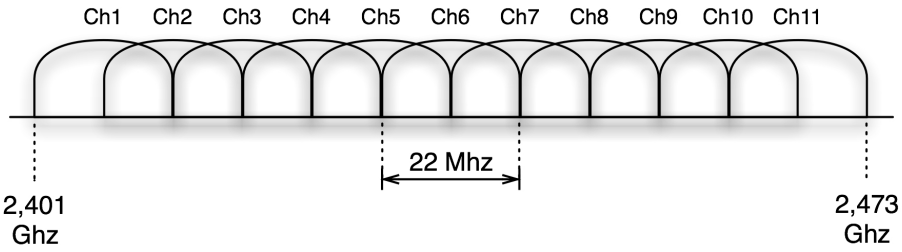

Figure 2.8: 802.11b/g channels.

adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical

process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network. Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band.

802.11-2007

In 2003, task group TGma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REVma or 802.11ma, as it was called, created a single document that merged 8 amendments (802.11a,b,d,e,g,h,i,j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the current base standard IEEE 802.11-2007.

802.11n - MIMO

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment and it was published in October 2009.(8) [1] MIMO technology offers tremendous performance gains for WLANs at relatively low cost. Any system with multiple inputs into the receiver and multiple outputs to the transmitter is a MIMO system, but implementing such a system involves several distinctly different radio techniques. Some of these techniques are beneficial and fully compatible with todays standard WLAN equipment, while others do not improve performance when used with existing equipment.

In MIMO, multiple antennas are used to coherently resolve more information than possible using a single antenna. One way it provides this is through *Spatial Division Multiplexing (SDM)*. SDM spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver. In addition, MIMO technology requires a separate radio frequency chain and analog-to-digital converter for each MIMO antenna which translates to higher implementation costs compared to non-MIMO systems.[2]

[1] `http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html`

[2] https://mentor.ieee.org/802.11/dcn/09/11-09-0576-03-000n-sp2-40mhz-coexistence-cids-presentation.ppt

40 MHz channels is another feature incorporated into 802.11n which doubles the channel width from 20 MHz in previous 802.11 PHYs to transmit data. This allows for a doubling of the PHY data rate over a single 20 MHz channel. It can be enabled in the 5 GHz mode, or within the 2.4 GHz if there is knowledge that it will not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using those same frequencies.

In order to better understand how the antennas are used in a MIMO communication system, we can say that the number of simultaneous data streams is limited by the minimum number of antennas in use on both sides of the link. However, the individual radios often further limit the number of spatial streams that may carry unique data. The notation $a \times b : c$ helps identify what a given radio is capable of. The first number (a) is the maximum number of transmit antennas or RF chains that can be used by the radio. The second number (b) is the maximum number of receive antennas or RF chains that can be used by the radio. The third number (c) is the maximum number of data spatial streams the radio can use. For example, a radio that can transmit on two antennas and receive on three, but can only send or receive two data streams would be $2 \times 3 : 2$. The 802.11n draft allows up to $4 \times 4 : 4$. Common configurations of 11n devices are $2 \times 2 : 2$, $2 \times 3 : 2$, and $3 \times 3 : 3$. All three configurations have the same maximum throughputs and features, and differ only in the amount of diversity the antenna systems provide. In addition, a fourth configuration, is becoming common, which has a higher throughput, due to the additional data stream. The 802.11n MIMO was so promising since its debut that even before the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the said technology.

The most popular standards are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. 802.11n is a new multi-streaming modulation technique. Other standards in the family (cf, h, j) are service amendments and extensions or corrections to the previous specifications. Given that both 802.11b and 802.11g use the 2.4 GHz ISM band, the relevant equipment may occasionally suffer interference from microwave ovens, cordless

telephones and Bluetooth devices. Both 802.11 and Bluetooth control their interference and susceptibility to interference by using spread spectrum modulation. Bluetooth uses a frequency hopping spread spectrum signaling method (FHSS), while 802.11b and 802.11g use the direct sequence spread spectrum signaling (DSSS) and orthogonal frequency division multiplexing (OFDM) methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment. The used segment of the radio frequency spectrum varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption. In Italy, according to the ETS 300-328-2, it is forbidden to exceed the 100 mW EIRP threshold[1], which is equivalent to 20 dBm gain. Furthermore, radio devices for private use can transmit with a maximum electrical power of 50 mW (equivalent to 17 dBm) because, usually, even the simplest antenna has a transmission gain of 2.5 dBi, which makes possible to reach an EIRP of 80 mW (equivalent to 19.2 dBm). For this reason, in European Union it is strictly forbidden to use antennas with an high gain (higher than 5 dBi), because it could be possible to raise the EIRP beyond the 100 mW threshold (20 dBm).

2.5.2 WiMAX

WiMAX, or *Worldwide Interoperability for Microwave Access*, is a communication technology which try to fill the gap between 3G and WLAN standards, and it is the first implementation which appears to comply with the MAN (Metropolitan Area Network) concept, in a wireless manner. Two main standards are currently considered: 802.16d

[1] *Equivalent isotropically radiated power (EIRP)* or, alternatively, *Effective isotropically radiated power* is the amount of power that a theoretical isotropic antenna (which evenly distributes power in all directions) would emit to produce the peak power density observed in the direction of maximum antenna gain. EIRP can take into account the losses in transmission line and connectors and includes the gain of the antenna. The EIRP is often stated in terms of decibels over a reference power emitted by an isotropic radiator with an equivalent signal strength.

and 802.16e. The first one is used at fixed locations, and it is a perfect solution for connecting different buildings of a company at a low cost, for example. This specification offers up to 48 Km of coverage and data rates of 70 Mbps.
The 802.16e standard, specifically designed for mobile users connected to a base station. The OFDM (*Orthogonal Frequency Division Multiple access*) technology is used in this standard to serve multiple users, and the final physical interface considered copes with mobility issues, such as interferences, multipath and delays. 802.16e is, hence, the most appropriate specification of WiMAX for the vehicular field. Tens of Mbps, mobility speed up to 100 Km/h, and 10 km of coverage to the base station, make 802.16e a good option for urban scenarios, where vehicles can be connected at a high data rate using a WiMAX deployment.
Currently it is possible to obtain some Pre-WiMAX devices, but it is expected that, as soon as the final specifications are ready, the spectrum of vehicular services which could be deployed with WiMAX grow rapidly. This technology was stressed in order to analyze the its performance in a mobile environment and the results showed that a mean of 2 Mbps and 5.3 Mbps can be obtained in real scenarios (up to 90 Km/h), with an average RTT[1] of 100 ms.

2.5.3 Bluetooth

Bluetooth technology aims at allowing wireless short-range communications between several devices. Developed originally by Ericsson, Bluetooth undergoes an evolution of its specications maintained and developed by the Special Lobby Special Interest Group (SIG) of Bluetooth and is accessorily standardized by the IEEE under the reference IEEE 802.15.1. Today IEEE 802.15 subgroups and other forums such as the Wimedia Alliance are competing for the same eld of operation. The governing idea behind Bluetooth consisted in specifying a wide scale integrated circuit to be deployed on a very large scale on various types of equipments with a very reduced energy consumption and thus announcing very low prices.
In 1994, Ericsson Mobile Communications launched a feasibility study of low-cost low-consumption radio interface to be used between mobile telephones and their accessories.

[1]RTT stands for *Round Trip Time* and it is the time required to send a signal in both directions over a particular communication link. This is the soonest that it is possible to receive an acknowledgement of a message.

In February 1998, IBM, INTEL, Nokia and Toshiba joined the Swedish company and in May they created the SIG. It was widened by the arrival of 3Com, Agere (Lucent Technologies), Microsoft and Motorola during 2000 and does not cease increasing thus gathering actors who cover several elds of expertise such as cellular telephony, portable computers, cars and digital processing. Being an opened industrial specication, all the members of Bluetooth SIG can use it free in their products and services. Today, the SIG counts more than 2500 manufacturers. It carries out a true ght to promote this world standard despite the large number of concurrent technologies essentially headed by Wi-Fi.

Thanks to Bluetooth, however, it is possible to create a personal area network (PAN) where several devices can be connected. It operates in the 2.4 GHz band and, due to the low power consumption features, allow communications in a typical range of tens of meters. Bluetooth terminals are grouped in piconets, and these piconets can also be connected by means of scatternets.

The properties of Bluetooth make it perfect for invehicle networks (72). Some researchers also advocate the usage of Bluetooth for V2V applications (92). However, this technology is limited by the necessary time to form piconets and scatternets (in the order of seconds) (86) and, overall, the limited communication range.

2.5.3.1 Bluetooth Architecture

Bluetooth communication requires two preliminary things: rst we have to know the devices in the neighbourhood (discovery) and second there must be a preestablished circuit. Communication is also based on a masterslave principle. A group of equipments forms a cell called piconet. A piconet comprises a master and seven slaves at the maximum. Several piconets can overlap and form a *scatternet* (see Fig.2.9). In a piconet the communication is based on the master to harmonize the frequencies and channels. We know the neighbours through the discovery phase while in a scatternet there is a need to route data between masters and relay nodes. Scatternets in Bluetooth is not well developed. It has been improved by specic routing procedures in later standards such as ZigBee. Two slave devices cannot talk directly to each other except during the discovery phase. Channel allocation and communication establishment are under the responsibility of the master. Although there was a limitation in earlier versions of Bluetooth on the number of simultaneous channels in a piconet, it is removed from the

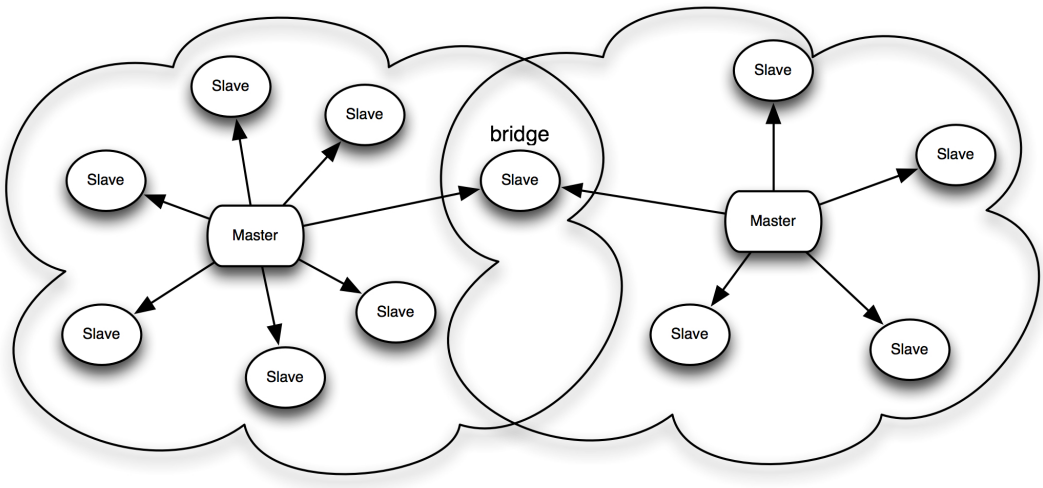

Figure 2.9: Example of a bluetooth scatternet.

current version as the cell capacity has increased signicantly. The standard supports also broadcast by simply removing the destination from the messages. The master is responsible of polling nodes and also allocating/blocking new connection bandwidth. It is responsible for setting the piconet synchronization clock and as we will see decides for the *frequency hopping sequence (FHS)*. A slave can be part of several piconets.
One major interesting feature of Bluetooth is that it is not dependent on the IP. This courageous design decision eases the deployment of devices that do not need to worry about upper layer problems such as address allocation, default router, netmask, etc. Auto conguration is hence much easier.

2.5.4 ZigBee

This is an In-Vehicle (InV) wireless sensor network which offers lower data rate but can be used for many embedded applications. ZigBee is an industry alliance that promotes a set of rules which builds on top of the IEEE 802.15.4 standards; it is a low-cost, low-power, wireless mesh networking standard. It operates in three ISM radio bands: 868 MHz in Europe, 915 MHz in countries such as USA and Australia, and 2.4 GHz (16 channels) in most jurisdictions worldwide. The modulation uses direct-sequence spread spectrum coding, which is managed by the digital stream into the modulator

and the data rate is 250 Kbps per channel in the 2.4 GHz band (40 Kbps in the 915 MHz band and 20 Kbps in the 868 MHz band). Transmission range is between 10 and 75 meters, although it is heavily dependent on the particular environment. The maximum output power of the radios is generally 0 dBm (1 mW). CSMA/CA is the usually channel access mode, except three cases (beacons, acknowledgment, messages for beacon oriented network devices).
As ZigBee provides network speeds of up to 250 Kbps, it is expected to be largely used as a sensor network for monitoring and control purposes (air conditioning, heating, ventilation, lighting control, etc.).
In general, the experiments and measured results indicate that ZigBee is a viable and promising technology for implementing an intra-car wireless sensor network (10). However, the communication between sensor nodes and a base station in the car will depend on several factors, such as the power loss, coherence bandwidth, and coherence time of the underlying communication channels between the sensor nodes and the base station.
Other high data rate technologies are available such as IEEE 802.15.3a (UWB) which is a competitor to the other IEEE 802.11 solutions. It can provide speeds of up to hundred of Mbps/s and it can be likely used in multimedia applications. However, UWB components and boards are not actually still available.

2.5.5 DSRC and 802.11p (or *"WAVE"*)

DSRC (Dedicated Short Range Communications) is a short to medium range communications service operating at 5.9 GHz that supports both public safety and private operations in I2V and V2V communication environments. DSRC is meant to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important. DSRC program is intended to support a wide range of applications, of which only a small subset are presently defined. The intent is to support a wide range of I2V and V2V communications, for which most of the explicit applications cannot even be envisioned today.
The roots of DSRC may be formally traced to 2003 in the United States, when the Federal Communications Commission (FCC) adopted what is termed a Report and Order that provided licensing and service rules for DSRC in the ITS Radio Service. This enabled free, licensed use of the 5.8505.925 GHz frequency range, primarily for use in

safety but also for other transportation and commerce applications. It was originally conceived as a general purpose Radio Frequency Identification (RFID) technology. In making implementation decisions, however, it was quickly recognized that the Orthogonal Frequency Division Multiplexing (OFDM) was the best protocol at the time, as it allows for closely spaced orthogonal subcarriers to carry separate streams of data in parallel. There existed an emergent consumer base for wireless office LAN (Local Area Network) under IEEE 802.11a standard, based on the Atheros 5141 chipset and using OFDM. Because of the similar operating frequencies of 802.11a and the DSRC spectrum granted by the FCC, the economies of scale in using chipsets already commercially available made this case compelling during the standards discussions at the time.

For highly mobile transportation applications, a major problem to be solved in the normal operation of chipsets designed for wireless office LAN is the time, measured in seconds, required for a mobile wireless station (e.g., a laptop) to associate with a wireless access point. The nature of the channel scanning and security mechanisms in the IEEE 802.11a devices necessitates this delay, which made the existing standard association protocols unsuitable for use with safety applications that require a vehicle moving at high speed to quickly exchange information with another vehicle or RSE while in range. Changes were required at both the basic channel connection level and at the level where decisions are made to accept messages and route to their destination in order to solve this problem. There emerged three sets of standards development and associated application ideas. First, an amendment was required to the IEEE 802.11 Wireless LAN standard, to define the DSRC spectrum and band plan and to allow fast association, comprising the physical layer IEEE 802.11p. The changes at the IEEE 802.11 layer require providing new security and channel selection services at a higher layer and specifically in the control channel and multiple service channels. These are enabled, in addition to other network services, in the IEEE 1609 standards for *Wireless Access in Vehicular Environments (WAVE)* (101):

1. the resource manager, or 1609.1;

2. security services and management, or 1609.2;

3. networking services, or 1609.3;

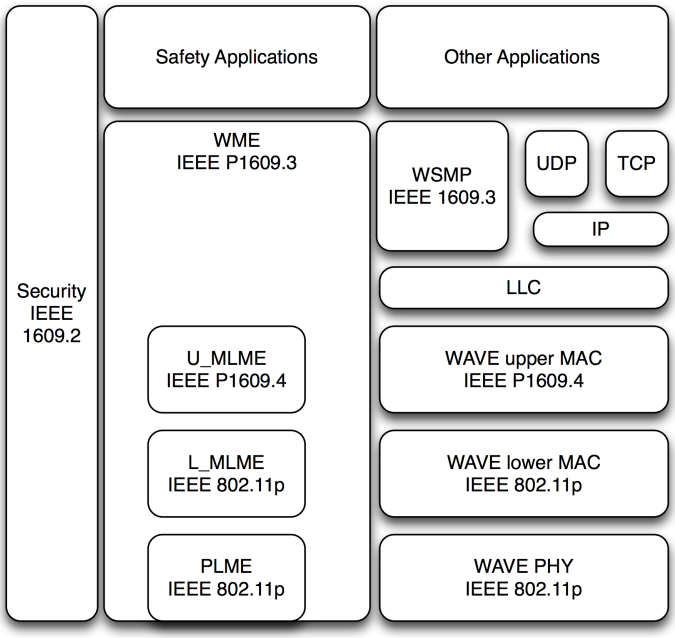

Figure 2.10: DSRC Standards DSRC standards and communication stack.

4. multichannel operations, or 1609.4.

These standards enable a system in which vehicles can connect immediately on a common channel in the DSRC band for safety applications, while other channels are available for less urgent communications. The final or top layer standard would be the application layer, (so called SAE J2735, under development by the Society of Automotive Engineers, DSRC Technical Committee).

At this point it should be valuable to spend few additional words on WAVE.
The standard IEEE 802.11p (as we have seen, also referred to as WAVE) denes enhancements to IEEE 802.11 required to support intelligent transportation systems (ITS) applications. This includes data exchange between high-speed vehicles and between these vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz. The communications provided by WAVE generally occur over distances up to 1000 m between roadside stations and mostly high speed, but occasionally stopped and slow moving, vehicles or between high-speed vehicles. WAVE includes a number of new classes of