Chapter 8. Vehicle to Vehicle interactions (V2V)

Table of Contents

Nowadays the developed countries are increasingly characterized by a pervasive computing environment. The people's living environments are emerging based upon information resource provided by the connections of various communication networks. New handheld devices like smartphones and tablets enhance information processing and global access of users. During the last decade, advances in both hardware and software technologies have resulted in the need for connecting the vehicles with each other. In this chapter first the basic theory of the Mobile Ad Hoc Networks are introduced, then the available functions and the advantages of the vehicle to vehicle interactions are detailed.

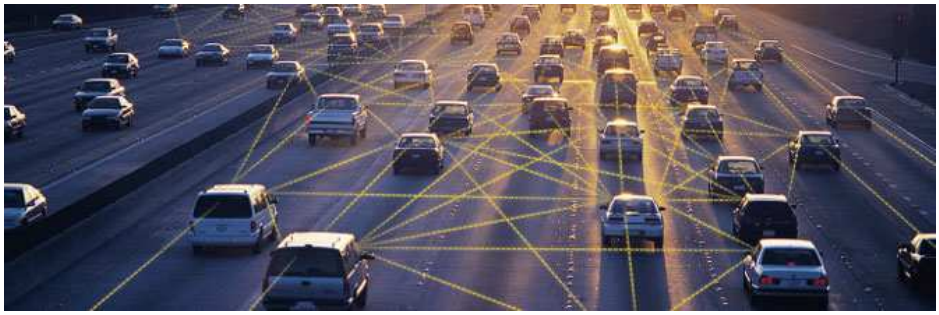

Figure 8.1. V2V interactions (Source: http://www.kapsch.net)

8.1. Mobile Ad Hoc Network Theory

Mobile networking is one of the most important technologies supporting pervasive computing, and it is the essential technology for the vehicular ad-hoc network development. The basic theory of MANETs is discussed based on the PhD thesis in *[109]*.

Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other: infrastructure-based and ad hoc.

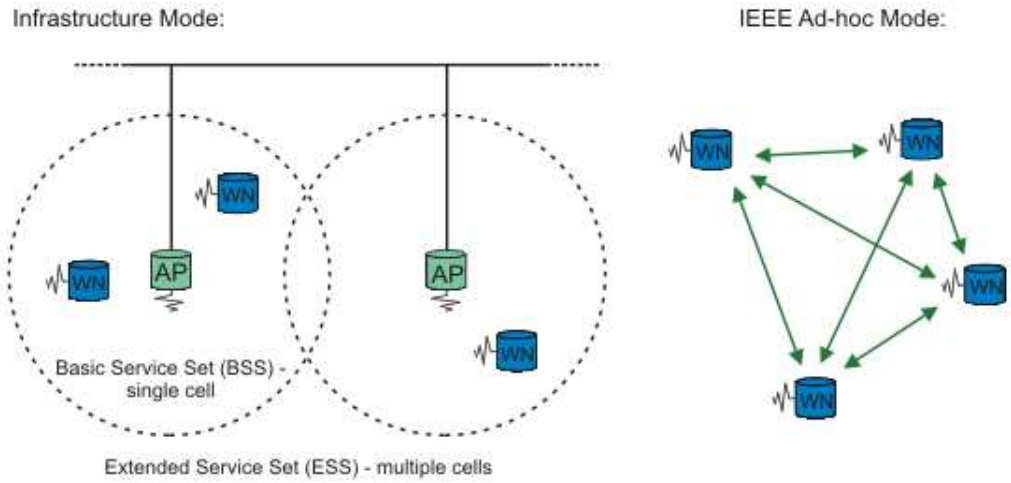

Figure 8.2. Infrastructure-based and Ad hoc networks example (Source: http://www.tldp.org)

Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points (or base stations) connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, UMTS, WLL, WLAN, etc.

In recent years the widespread availability of wireless communication and handheld devices has stimulated research on self-organizing networks that do not require a pre-established infrastructure. These ad hoc networks consist of autonomous nodes that collaborate in order to transfer information. Usually these nodes act as end systems and routers at the same time. Ad hoc networks can be subdivided into two classes: static and mobile. In static ad hoc networks the position of a node may not change once it has become part of the network.

In mobile ad hoc networks, systems may move arbitrarily. A Mobile Ad Hoc Network is commonly called a MANET. Mobile Ad Hoc Networks creates the basis for connectivity between vehicles which is called Vehicular Ad Hoc Network. It is a variation of MANETs, with the emphasis being now the node is the vehicle.

A MANET is a collection of wireless mobile nodes that dynamically form a network to exchange information without using any pre-existing fixed network infrastructure or a centralized administration. MANET nodes are equipped with wireless transmitters and receivers using antennas, which may be omni-directional (broadcast), highly -directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or ad hoc network formulates between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

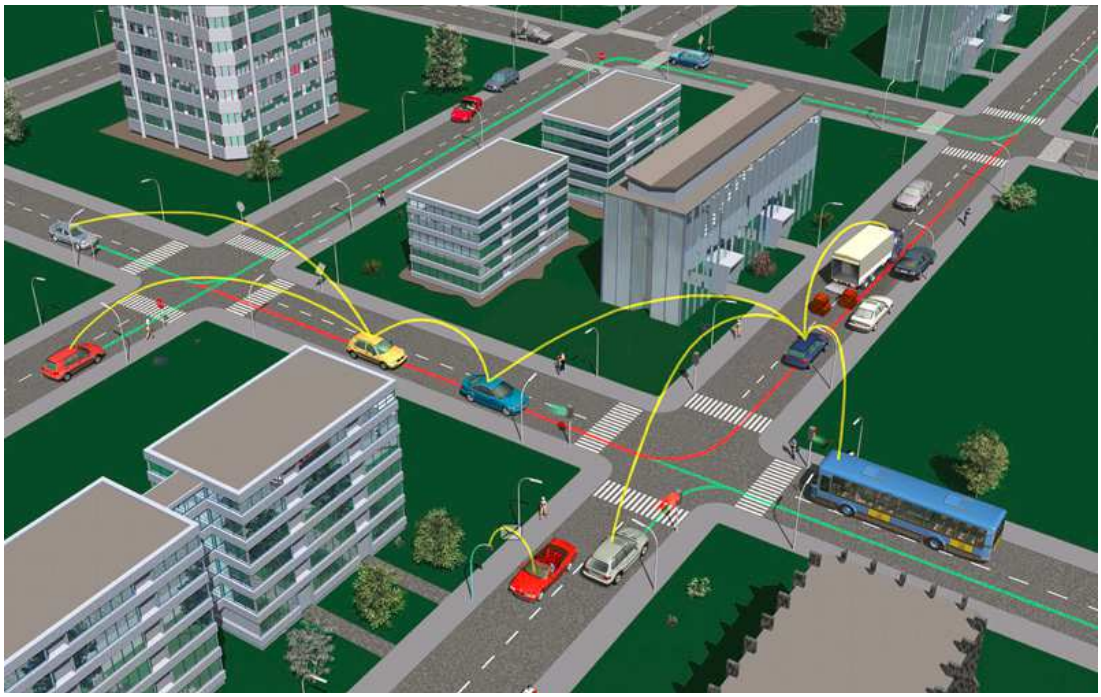

Figure 8.3. Vehicular Ad Hoc Network, VANET (source: http://car-to-car.org)

In such an environment, it may be necessary for one mobile host to use the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions.

MANETs are a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of wireless connection. Next generation of mobile communications will include both infrastructure wireless networks and infrastructureless Mobile Ad Hoc Networks (MANETs).

The special features of MANET bring this technology great opportunity together with severe challenges. Since mobile ad hoc networks change their topology frequently and without prior notice, routing in such networks is a challenging task. A MANET is some way like an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time.

The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network, including:

- Peer-to-Peer. Communication between two nodes that are within one hop. Network traffic is usually consistent.
- Remote-to-Remote. Communication between two nodes beyond a single hop but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.
- Dynamic Traffic. This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.

A MANET has the following special characteristics (See *[109]* and *[110]*).

- Autonomous terminal. In a MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
- Distributed operation. Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.
- Dynamic network topology. Since the nodes are mobile, the network topology (which is typically multi-hop) may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network.
- Multi-hop routing. Basic types of ad hoc routing algorithms can be single -hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multi-hop in terms of structure and implementation, with the cost of less functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
- Bandwidth-constrained, fluctuating capacity links. The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently.
- Energy and processing constrained operation. In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage compared to desktop or fixed devices. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

- Limited physical security: Mobile wireless networks are generally more disposed to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

Summarizing a mobile ad hoc network is a collection of autonomous mobile nodes that form a dynamic, purpose-specific, multi-hop radio network in a decentralized manner. The nature of such networks is the absence of a fixed support infrastructure (such as mobile switching centres, base stations, access points) traditionally seen in wireless networks. The network topology is constantly changing as a result of nodes joining in and moving out. Packet forwarding, routing, and other network operations are carried out by the individual nodes themselves. The features of MANET introduce several challenges which are detailed in the following subsections.

8.1.1. Routing

Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. In a MANET routers (i.e. hosts) can be mobile and inter -router connectivity can change frequently during normal operation. In contrast the Internet (like most of the telecom networks) possesses a quasi-fixed infrastructure consisting of routers or switches that forward data over hardwired links. Traditionally end-user devices, such as host computers or telephones, attach to these networks at fixed locations. As a consequence they are assigned addresses based on their location in a fixed network-addressing hierarchy. It simplifies routing in these systems, as a user's location does not change.

The end devices are increasingly mobile, meaning that they can change their point of attachment to the fixed infrastructure. This is the paradigm of cellular telephony and its Internet equivalent, mobile data network. In this approach a user's identity depends upon whether the user adopts a location-dependent (temporary) or location-independent (permanent) identifier. Users with temporary identifiers are sometimes referred to as nomadic, whereas users with permanent identifiers are referred to as mobile. The distinction is that although nomadic users may move, they carry out most network related functions in a fixed location. Mobile users must work "on the go" changing points of attachment as necessary. In either case additional networking support may be required to track a user's location in the network so that information can be forwarded to its current location using the routing support within the more traditional fixed hierarchy.

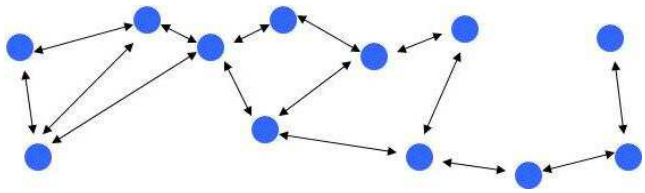

Figure 8.4. Multi-hop routing (Source: http://sar.informatik.hu-berlin.de)

Internet is hardly tuned to allow mobility during the data transfers because protocols are not conceived for devices that frequently change their point of attachment in the topology. There is typically a change of the physical IP address each time a mobile node changes its point of attachment and thus its reachability to the Internet topology. This results in losing packets in transit and breaking transport protocols connections if mobility is not handled by specific services. The protocol stack must therefore be upgraded with the ability to cross networks during data transfers, without breaking the communication session and with minimum transmission delays and signalling overhead. This is commonly referred to as mobility support. Host mobility support is handled by Mobile IPv6.

In contrast, the goal of mobile ad hoc networking is to extend mobility into the field of autonomous, mobile, wireless domains, where a set of nodes, which may be combined routers and hosts, themselves form the network routing infrastructure in an ad hoc way. With Mobile Ad Hoc Networking, the routing infrastructure can move along with the end devices. Thus the infrastructure's routing topology can change, and the addressing within the topology can change. In this paradigm an end-user's association with a mobile router (its point of attachment) determines its location in the MANET. As mentioned above a user's identity may be temporary or permanent. The fundamental differences in the composition of the routing infrastructure (fixed, hardwired, and bandwidth-rich opposite to dynamic, wireless, and bandwidth-constrained) causes that much of the fixed infrastructure's control technology is no longer useful. The infrastructure's routing algorithms and much of the networking suite must be reworked to function efficiently and effectively in mobile environment.

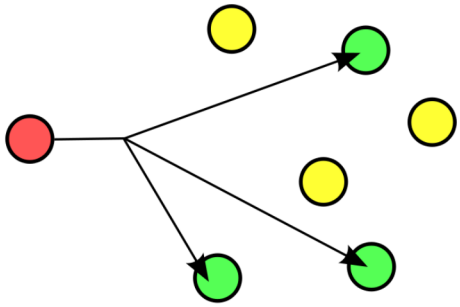

Figure 8.5. Multicast communication (Source: http://en.wikipedia.org/wiki/File:Multicast.svg)

Multicast routing (delivery of information to a group of destination devices simultaneously in a single transmission) is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

8.1.2. Security

In addition to the common vulnerabilities of wireless connection an ad hoc network has its particular security problems. Mobile hosts join in on the fly and create a network on their own. With the network topology changing dynamically and the lack of a centralized network management functionality, these networks tend to be vulnerable to a number of attacks. If such networks are to succeed in the transportation, the security aspect naturally assumes importance. The unreliability of wireless links between nodes, constantly changing topology owing to the movement of nodes in and out of the network and lack of incorporation of security features in statically configured wireless routing protocols not meant for ad hoc environments all lead to increased vulnerability and exposure to attacks.

Security in wireless ad hoc networks is particularly difficult to achieve, because of the vulnerability of the links, the limited physical protection of each of the nodes, the sporadic nature of connectivity, the dynamically changing topology, and the absence of a certification authority and the lack of a centralized monitoring or management point. This underscores the need for intrusion detection, intrusion prevention, and related countermeasures. The wireless links between nodes are highly susceptible to link attacks, which include the following threats (See *[111]*).

- Passive eavesdropping
- Active interfering
- Leakage of secret information
- Data tampering
- Impersonation
- Message replay or distortion
- Denial of service (DoS)

Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation (these and other security needs are discussed in the next section). Ad hoc networks do not have a centralized piece of machinery such as a name server, which could lead to a single point of failure and thus, make the network that much more vulnerable.

An additional problem related to the compromised nodes is the potential byzantine failures encountered within Mobile Ad hoc Network (MANET) routing protocols wherein a set of the nodes could be compromised in such a way that the incorrect and malicious behaviour cannot be directly noted at all. The compromised nodes may seemingly operate correctly, but, at the same time, they may make use of the flaws and inconsistencies in the routing protocol to undetectably distort the routing fabric of the network. In addition such malicious nodes can also create new routing messages and advertise non-existent links, provide incorrect link state information and flood other nodes with routing traffic, thus inflicting byzantine failures on the system. Such failures are severe, because they may come from seemingly trusted nodes. Even if the compromised nodes were noticed and prevented from performing incorrect actions, the erroneous information generated by the byzantine failures might have already

been propagated through the network.

Finally scalability is another issue that has to be addressed when security solutions are being devised, for the simple reason that an ad hoc network may consist of hundreds or even thousands of nodes. The scalability requirements directly affect the scalability requirements targeted to various security services such as key management. Standard security solutions would not be good enough since they are essentially for statically configured systems. This gives rise to the need for security solutions that adapt to the dynamically changing topology and movement of nodes in and out of the network.

These vulnerabilities allow a lot of special attacks in the vehicular networks including but not limited to the following examples:

- Bogus information (Figure 124): Attackers diffuse wrong information in the network to affect the behaviour of other drivers (e.g., to divert traffic from a given road and thus free it for themselves).

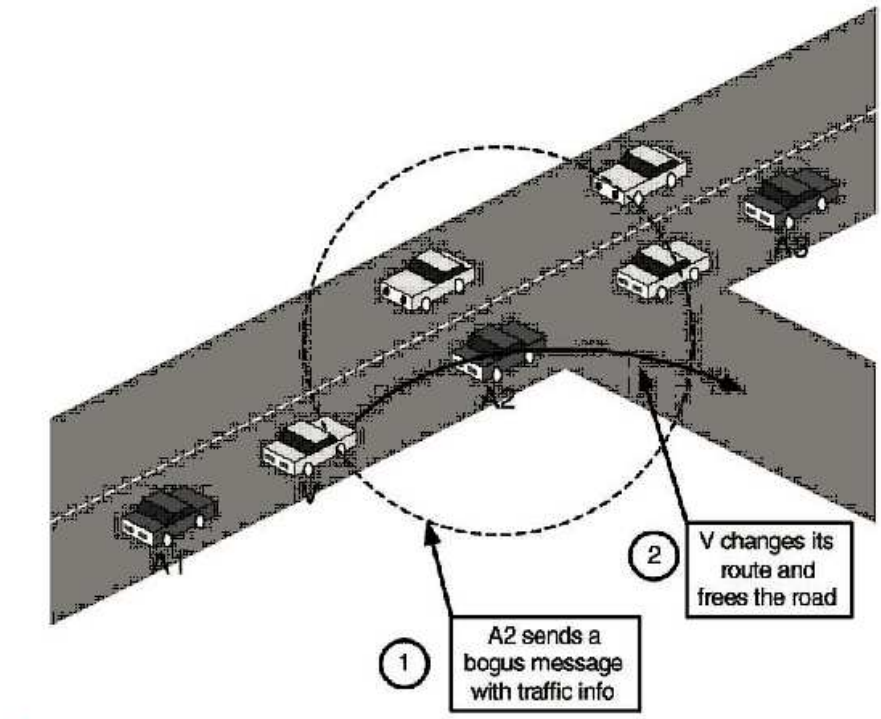

Figure 8.6. Bogus information attack

- Cheating with sensor information: Attackers in this case use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other and having full trust between the attackers.
- ID disclosure of other vehicles in order to track their location. This is the “Big Brother” scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). To monitor the global observer can leverage on the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbours of the target and collects the required data).
- Denial of Service: The attacker may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages.
- Masquerading: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.

As apparent from the above the security aspects are the most critical challenges before the wide spreading of the vehicular networks.

8.1.3. Quality of Service (QoS)

The goal of QoS support is to achieve a more deterministic communication behaviour, so that information carried by the network can be better prioritized and network resources can be better utilized. The notion of QoS is an

agreement or a guarantee by the network to provide a set of measurable pre-specified service attributes to the user in terms of network delay, delay variance (jitter), available bandwidth, probability of packet loss (loss rate), etc. The IETF RFC 2386 characterizes QoS as a set of service requirements to be met by the network while transporting a packet stream from source to destination. A network's ability to provide a specific QoS depends upon the properties of the network itself, which span over all the elements in the network. For the transmission link, the properties include link delay, throughput, loss rate, and error rate. For the nodes, the properties include hardware capability, such as processing speed and memory size. Above the physical qualities of nodes and transmission links, the QoS control algorithms operating at different layers of the network also contribute to the QoS support in networks. Unfortunately the features of MANETs show weak support for QoS. The wireless link has low, time-varying raw transmission capacity with relatively high error rate and loss rate. In addition, the possible various wireless physical technologies that nodes may use simultaneously to communicate make MANETs heterogeneous in nature. Each technology will require a MAC layer protocol to support QoS. Therefore the QoS mechanisms above the MAC layer should be flexible to fit the heterogeneous underlying wireless technologies. Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device.

8.1.4. Internetworking

In addition to the communication within an ad hoc network, internetworking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

8.1.5. Power Consumption

For most of the light-weight (handheld) mobile terminals and also the built-in automotive ECUs, the communication-related functions should be optimised for low power consumption. Conservation of power and power-aware routing must be taken into account.

8.2. V2V standards

Three categories of standards deal with the vehicular networks. The IEEE 802.11 standard body is currently working on a new amendment, IEEE 802.11p, to satisfy the above mentioned requirements. This document is named Wireless Access in Vehicular Environment, also known as WAVE.

As shown in Figure 125 *[112]* IEEE 802.11p WAVE is only a part of a group of standards related to all layers of protocols for V2V operations. The IEEE 802.11p standard is limited by the scope of IEEE 802.11, which is strictly a MAC and PHY level standard that is meant to work within a single logical channel.

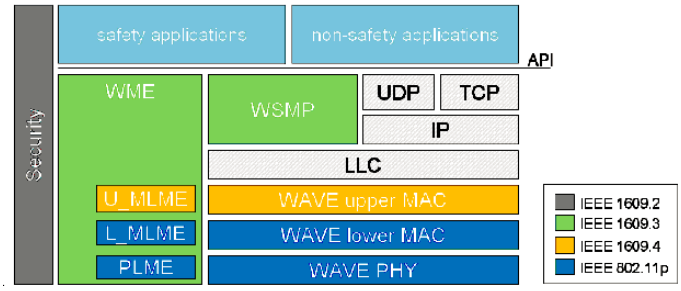

Figure 8.7. V2V standards and communication stacks (Source: Jiang, D. and Delgrossi, L.)

All knowledge and complexities related to the V2V operational concept are taken care of by the upper layer IEEE 1609 standards. It is intended to operate with IEEE 802.11p.

The third standard is developed by the Society of Automotive Engineers (SAE). Their J2735 standard can be placed in the application layer. It defines message sets, data frames and elements which are used for V2V and V2I safety exchanges.

8.2.1. IEEE 802.11p (WAVE)

The IEEE 802.11p WAVE standardization process originates from the allocation of the Dedicated Short Range Communications (DSRC) spectrum band in the United States and the effort to define the technology for usage in

the DSRC band. The evolutions and the basics are explained in the following chapters from *[112]*.

In 1999 the U.S. Federal Communication Commission allocated 75MHz of Dedicated Short Range Communications (DSRC) spectrum at 5.9 GHz to be used exclusively for vehicle-to-vehicle and infrastructure-to-vehicle communications. The primary goal is to enable public safety applications that can save lives and improve traffic flow. Private services are also permitted in order to spread the deployment costs and to encourage the quick development and adoption of DSRC technologies and applications.

As shown in Figure 126 the DSRC *[113]* spectrum is structured into seven 10 MHz wide channels. Channel 178 is the control channel (CCH), which is restricted to safety communications only. The two channels at the ends of the spectrum band are reserved for special uses. The rest are service channels (SCH) available for both safety and non-safety usage.

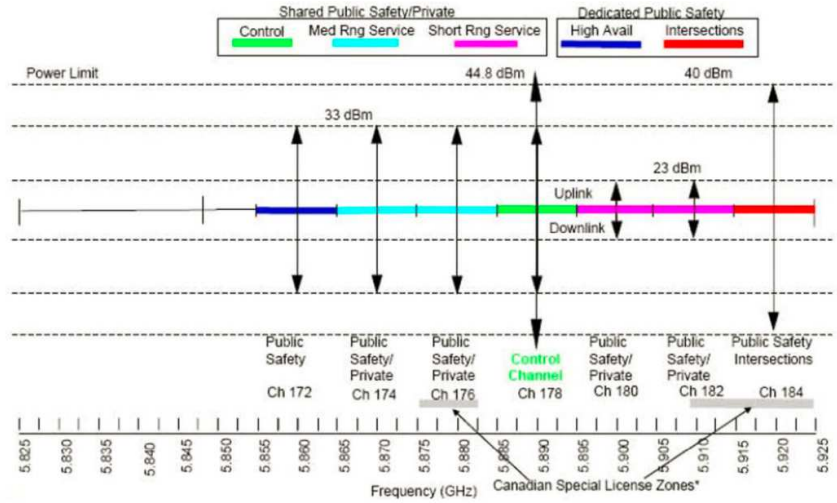

Figure 8.8. DSRC spectrum band and channels in the U.S.

The DSRC band is a free but licensed spectrum. It is free because the Federal Communications Commission (FCC) does not charge a fee for the spectrum usage. Yet it should not be confused with the unlicensed bands in 900 MHz, 2.4 GHz and 5 GHz that are also free in usage. These unlicensed bands, which are increasingly populated with WiFi, Bluetooth and other devices, place no restrictions on the technologies other than some emission and co-existence rules. The DSRC band, on the other hand, is more restricted in terms of the usages and technologies. FCC rulings regulate usage within certain channels and limit all radios to be compliant to a standard. In other words one cannot develop a different radio technology (e.g. that uses all 75 MHz of spectrum) for usage in the DSRC band even if it is limited in transmission power as related to the unlicensed band.

Similar efforts are occurring in Europe to set spectrum aside for vehicular usage. Since 2008 European Commission's decision provides a single EU-wide frequency band that can be used for immediate and reliable communication between cars, and between cars and roadside infrastructure. It is 30 MHz of spectrum in the 5.9 Gigahertz (GHz) band which is allocated by national authorities across Europe to road safety applications, without barring other services already in place (such as radio amateur services). The intention is that compatibility with the USA will be ensured even if the allocation is not exactly the same; frequencies will be sufficiently close to enable the use of the same antenna and radio transmitter/receiver. (Source: *[114]*)

The worldwide DSRC spectrum allocation is shown in Figure 127 *[113]*.

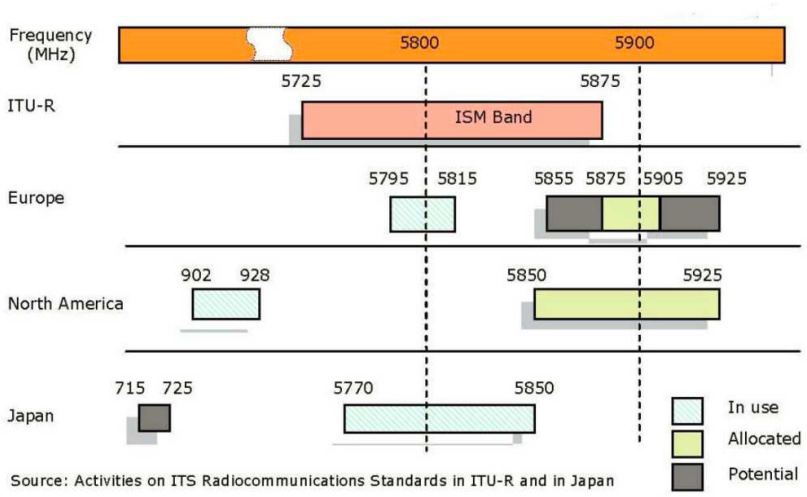

Figure 8.9. DSRC spectrum allocation worldwide

In the U.S. the initial effort at standardizing DSRC radio technology took place in an American Society for Testing and Materials (ASTM) working group. In particular the FCC rule and order specifically referenced this document for DSRC spectrum usage rules. In 2004 this effort migrated to the IEEE 802.11 standard group as DSRC radio technology is essentially IEEE 802.11a adjusted for low overhead operations in the DSRC spectrum. Within IEEE 802.11 DSRC is known as IEEE 802.11p WAVE. IEEE 802.11p is not a standalone standard. It is intended to amend the overall IEEE 802.11 standard.

One particular implication of moving the DSRC radio technology standard into the IEEE 802.11 space is that now WAVE is fully intended to serve as an international standard applicable in other parts of the world as well as in the U.S. The IEEE 802.11p standard is meant to:

- Describe the functions and services required by WAVE-conformant stations to operate in a rapidly varying environment and exchange messages without having to join a Basic Service Set (BSS), as in the traditional IEEE 802.11 use case.
- Define the WAVE signalling technique and interface functions that are controlled by the IEEE 802.11 MAC.

8.2.2. IEEE 1609

The IEEE 1609 family of standards defines the following parts (see *[113]*):

- architecture,
- communication model,
- management structure,
- security mechanisms and
- physical access for high speed (<27 Mb/s), short range (<1000m) and low latency wireless communications in the vehicular environment.

The primary architectural components defined by these standards are the On Board Unit (OBU), Road Side Unit (RSU) and WAVE interface.

The IEEE 1609.3 standard covers the WAVE connection setup and management. The IEEE 1609.4 standard sits right on top of the IEEE 802.11p and enables operation of upper layers across multiple channels, without requiring knowledge of PHY parameters. The standards also define how applications that utilize WAVE will function in WAVE environment. They provide extensions to the physical channel access defined in WAVE.

8.2.3. SAE J2735

The third important standard related to vehicle communication is the J2735, Dedicated Short Range Communications (DSRC) Message Set Dictionary, maintained by the Society of Automotive Engineershttp://www.sae.org). This SAE Standard specifies a message set, its data frames and data elements specifically for use by applications intended to utilize the (DSRC/WAVE) communications systems. Although the scope of this Standard is focused on the message set and data frames of DSRC. This standard therefore specifies

the definitive message structure and provides sufficient background information for the proper interpretation of the message definitions from the point of view of an application developer implementing the messages according to the DSRC standards.

It supports interoperability among DSRC applications through the use of standardized message sets, data frames and data elements. The message sets specified in J2735 define the message content delivered by the communication system at the application layer and thus defines the message payload at the physical layer. The J2735 message sets depend on the lower layers of the DSRC protocol stack to deliver the messages from applications at one end of the communication system (OBU of the vehicle) to the other end (a roadside unit). The lower layers are addressed by IEEE 802.11p, and the upper layer protocols are covered in the IEEE 1609.x series of standards.

The message set dictionary contains:

- 15 Messages
- 72 Data Frames
- 146 Data Elements
- 11 External Data Entries

The most important message type is the basic safety message (often informally called “heartbeat” message because it is constantly being exchanged with nearby vehicles). Frequent transmission of “heartbeat” messages extends the vehicle’s information about the nearby vehicles complementing autonomous vehicle sensors. Its major attributes are the following *[115]*:

- Temporary ID
- Time
- Latitude
- Longitude
- Elevation
- Positional Accuracy
- Speed and Transmission
- Heading
- Acceleration
- Steering Wheel Angle
- Brake System Status
- Vehicle Size

The other kinds of messages are the following (See *[113]*):

- A la carte message -- composed entirely of message elements determined by the sender, allowing for flexible data exchange.
- Emergency vehicle alert message -- used for broadcasting warnings to surrounding vehicles that an emergency vehicle is operating in the vicinity.
- Generic transfer message -- provides a basic means to exchange data across the vehicle-to-roadside interface.
- Probe vehicle data message -- contains status information about the vehicle to enable applications that examine traveling conditions on road segments.
- Common safety request message -- used when a vehicle participating in the exchange of the basic safety message can make specific requests to other vehicles for additional information required by safety applications.

8.3. V2V applications

V2V communication enables a great number of use cases mostly in relation to improve driving safety or traffic efficiency and provide information or entertainment to the driver. The definitions of the below mentioned use cases are based on CAR 2 CAR Communication Consortium Manifesto *[116]*.

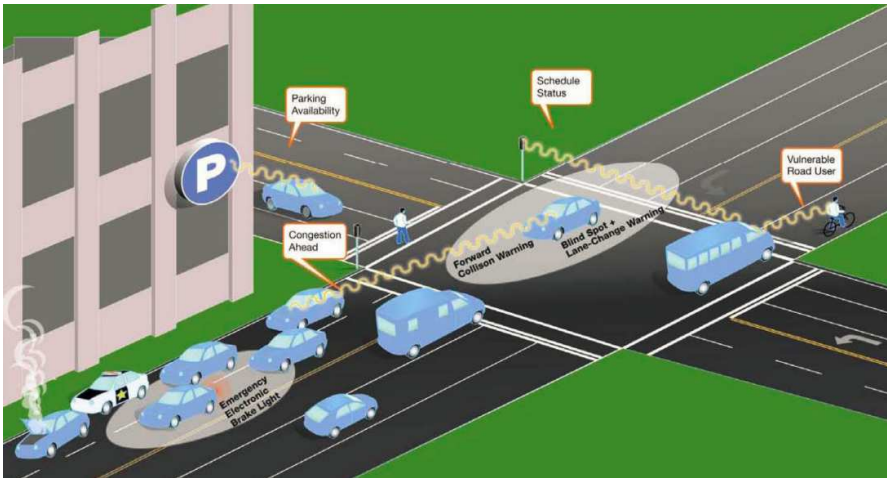

Figure 8.10. V2V application examples (forrás:http://gsi.nist.gov/global/docs/sit/2010/its/GConoverFriday.pdf)

8.3.1. Traffic Safety

Safety use cases are those where a safety benefit exists when the vehicle enters into a scenario applicable to the use case. The following safety applications can be relevant with the help of V2V communication.

- Warnings on entering intersections or departing highways
- Hazardous location warning: obstacle discovery, reporting accidents
- Sudden stop warnings: forward collision warning, pre-crash sensing or warning
- Lane change/keeping warnings/assistance
- Privileging ambulances, fire trucks, and police cars

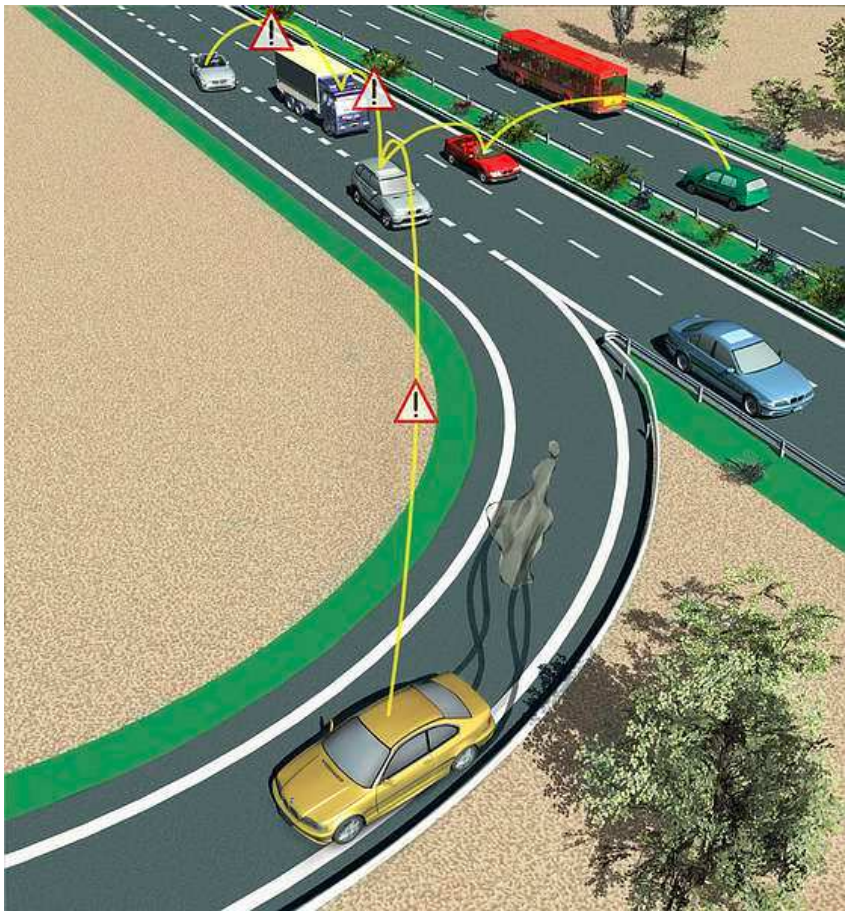

Figure 8.11. Hazardous location warning (source: http://car-to-car.org)

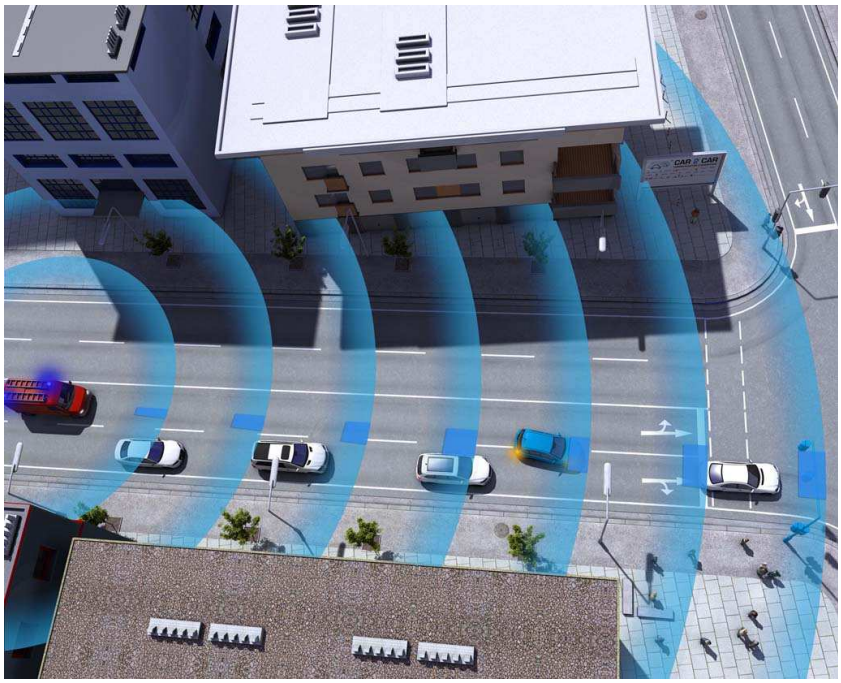

Figure 8.12. Privileging fire truck (source: http://car-to-car.org)

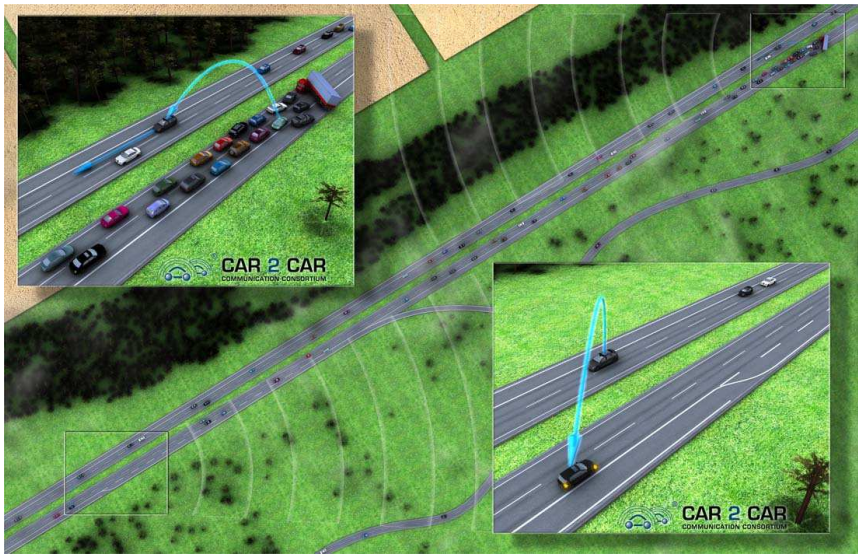

Figure 8.13. Reporting accidents (source: http://car-to-car.org)

8.3.2. Traffic Efficiency

Traffic Efficiency use cases are those meant to improve efficiency of the transportation network by providing information either to the owners of the transportation network or to the drivers on the network.

- Enhanced Route Guidance and Navigation
- Intelligent intersections: Adaptable traffic lights, Automated traffic intersection control, Green Light Optimal Speed Advisory
- Merging Assistance: enters an on-ramp to a limited access roadway (it is also a safety application)
- Variable speed limits

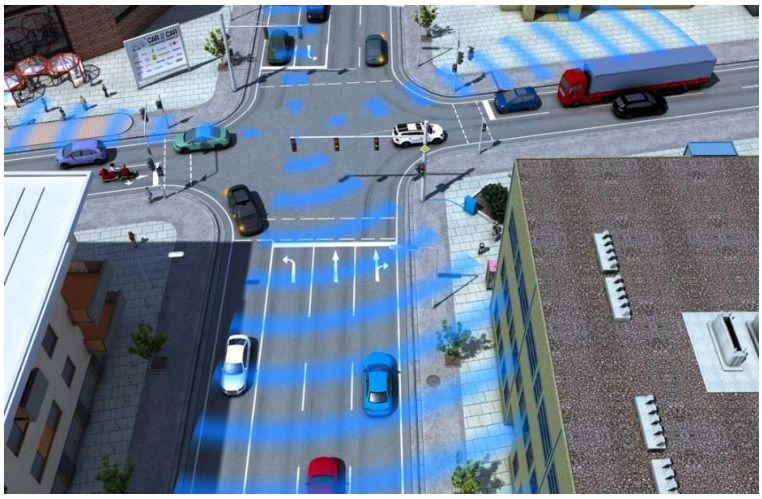

Figure 8.14. Intelligent intersection (source: http://car-to-car.org)

8.3.3. Infotainment and payments

This category does not contain direct traffic related applications, rather comfort services. Many of these use cases interact more directly with the vehicle owner on daily basis providing entertainment or information on a regular basis. Others are transparent to the driver but still perform a valuable function such as increasing fuel economy.

The electronic payment applications result in convenient payments and avoiding congestions caused by toll collection and makes pricing more manageable and flexible.

- Internet access
- POI notification

- Toll collecting
- Parking payment

8.3.4. Other applications

The V2V communication system can support the currently available driver assistance systems. With help of the broadcasted vehicle parameters the adaptive cruise control and park pilot functions can be improved.

Figure 8.15. V2V based Cooperative-adaptive Cruise Control test vehicle. (Source: Toyota)

With special low-cost roadside units (RSU) the road sign recognition function can be supported and the reliability can be improved. In special cases it could offer safety functions in case of bridge or tunnel height or gate width.

Another important field of usage could be the policing and enforcement. Police could use the V2V communication in several ways especially checking the traffic rules such as:

- Surveillance (e.g. finding stolen vehicles)
- Speed measurements
- Pull-over commands
- Red light drive through
- Restricted entries

Prev
Chapter 7. Intelligent actuators

Home

Next
Chapter 9. Vehicle to Infrastructure interaction (V2I)