1

Local Interactions for Cooperative ITS: Opportunities and Constraints

Jean-Marie BONNIN[1] **and Christophe COUTURIER**[2]
[1] *IMT Atlantique, Rennes, France*
[2] *YoGoKo, Rennes, France*

COPYRIGHTED MATERIAL

1.1. Introduction

Since the advent of wireless communication and its integration into consumer devices, the concept of intelligent environment or pervasive application has emerged. The ability to communicate with all objects in our immediate environment makes it possible to take information or trigger actions. Information collection feeds a context that applications take into account to adapt their behavior to the situation.

For this type of application, direct interaction with objects in the environment greatly facilitates matters, since it is not necessary to rely on a precise location and database to associate information (or objects) with this location. If we need to know the room temperature, all that is needed is to discover a temperature sensor and query it directly. Acquiring the same information when a server is in charge of collecting and exposing the building's temperature data firstly implies discovering the server that has the information at its disposal, then dialoging with it to retrieve

Cooperative Intelligent Transport Systems,
coordinated by Léo MENDIBOURE. © ISTE Ltd 2024.

the temperature of the room in which the sensor is located, and finding consequently a way to determine that the location is necessary. The machinery to be put in place is much more complex and yet it seems more intuitive, as the majority of the industry has been built on this model.

The difficulty when it comes to building services on direct (we will also use the term “local”) interactions is that this implies standardizing the method of communication, the frequency (or frequencies) used and the message format. For road or city applications, it is therefore necessary to bring many actors to agreement, and to impose choices on the entire ecosystem.

Direct interactions are widely used today for service discovery; for example, Wi-Fi devices continuously scan all frequencies used in the 2.4 GHz and 5 GHz bands to determine if there is an access point available in the environment. The presence of such an access point in no way indicates that the terminal will know how to connect to it, and even in the case where it is able to connect, whether it will be able to obtain a service (an Internet connection). The other technology widely used on consumer terminals is Bluetooth. Again, part of the terminals expose their presence by regularly sending messages at a determined frequency. All Bluetooth devices in proximity are able to see these messages and determine whether or not they know the correspondent. They can then either establish a connection to perform the service (e.g. hands-free kit) by taking advantage of the keying material previously established during pairing, or ask to perform a pairing, which requires the user’s intervention.

It should be noted that even when the two correspondents know each other, whether via Wi-Fi or Bluetooth, the discovery and connection establishment time frame is far too long for services with significant time constraints. We will return to this when we examine how the specificities of ITS-G5 make it possible to significantly reduce the time required to exchange information for road safety-related services.

In the second part of this chapter, we will present the concept of ephemeral local interactions, giving examples of services based entirely (or partially) on this type of interaction. We will describe how the first services that will be deployed in the context of cooperative ITS (awareness) are based on this type of interaction and the advantages/constraints of this approach. Lastly, before concluding, we will explore the place infrastructure holds in the implementation of services, based on ephemeral local interactions.

1.2. Ephemeral local interactions: concept and examples

1.2.1. *Examples of services using ephemeral local interactions*

Once it has been established that the different devices in interaction use the same communication technology on a subset of frequencies well known to all, it is necessary to specify the type of interaction targeted. Indeed, we will focus more specifically on interactions where no connection is established. When two devices are in proximity, they can “see” each other because of their technology community; they have at their disposal information that is spontaneously sent by their peers without having to go through the time-consuming establishment of a connection. When the communication technology has a fairly short range, simply being in communication and seeing a device gives an indication of co-spatiality that can form an integral part of the service. Therefore, when a telephone receives an advertisement on one of the three Bluetooth Low-Energy (BLE) channels, it knows that it is in close proximity to the tag whose identity is transmitted in the message, in addition to the information contained in the message itself. In a supermarket, the reception of its advertisements makes it possible to locate the mobile as long as the service provider has the precise placement of the tags in the store at its disposal. However, tags can also directly send information that may be used by the smartphone itself, such as a price, promotions or a link to the page describing a product.

Within the framework of the *TousAntiCovid* backtracking application and other mechanisms for identifying at-risk contacts, developed in the context of the Covid-19 pandemic, this co-spatiality property was used to identify transmission risks (Roca 2022). The complexity of the application comes mainly from the need to protect the privacy of users, while ensuring contact identification that is as accurate as possible. It was therefore necessary to avoid storing the list of contacts but to transmit within the advertisement messages the information required to make it possible to determine a posteriori whether their smartphone had been in contact with that of a contaminated person.

The case of contactless payment applications is rather different, since it instead involves establishing as secure a connection as possible to carry out a monetary transaction. It is therefore absolutely necessary to ensure that we are faced with the right device, and to prove that a valid transaction has taken place. However, the co-spatiality property is used to ensure that the payment card with which the transaction is carried out is in immediate proximity to the payment terminal. NFC (Near Field Contact) technology has been specifically adapted to reduce range and impose “near-contact”. The operation of radio transmissions makes this work quite complex because of the propagation of waves in the frequency bands used. It poses security problems, since it makes it possible, for example, to use relays. It then becomes necessary to go beyond controlling the transmission power to limit the range and to very finely control the transmission time, which also depends on the distance; this makes it possible, when it is excessive, to detect an attempt to relay the signal.

Prior to the emergence of the Bluetooth Low-Energy (BLE) version, applications used RFID technology, which has the great advantage of being able to install devices in the environment at very low cost, capable of "responding" to a request and sending previously configured data. This is generally a simple unique identifier, relatively similar to that of eBeacons in BLE. These RFID tags also have the property of being passive most of the time and of using the energy of the reader, which lights them up to wake up and respond. They therefore do not require a battery but are, however, inactive as long as they are not lit up. Readers also need to consume a fairly significant amount of energy to power the tags remotely.

In the different examples that we have seen, local interactions are essentially used to transmit an identifier, which makes it possible to establish our position by referring to prior knowledge of the position of the various devices. Richer applications make it possible to transmit information that the correspondent can directly use and that is most often linked to the position of the sender (a URL describing a product). This somewhat removes the need to maintain a geographic information system (GIS). In the case of BLE, this information is transmitted regularly, whether or not there is a correspondent to listen to it and to do something with it. The information broadcast in this way forms part of the environment and enriches it. The outlines of what we will call "ephemeral local interactions" are given below.

1.2.2. *Characteristics of ephemeral local interactions*

The first characteristic of local interactions is that they are established in the event of a *close contact* supported by a short- or medium-range wireless communication (BLE, NFC, RFID, ITS-G5, etc.).

The examples presented above highlight the *opportunistic* nature of these contacts. The objects considered evolve within a very large scope. They interact, sometimes ephemerally, with many other objects that they do not know beforehand. As stated above, from the outset, this excludes communication technologies requiring a form of pairing (e.g. Bluetooth) or a connection to a network (e.g. Wi-Fi or cellular networks). Indeed, beyond the fact that the necessary establishment time would often be prohibitive with regards to the applications envisaged, it is simply impossible for objects to memorize specific association parameters for each of these relationships; it would also be even more complicated to memorize the association parameters of all potential interactions beforehand.

As a result, the most suitable technologies to support local interactions are those that allow messages to be exchanged directly *without prior configuration*. It is of course still necessary to have knowledge of low-level parameters such as the type of technology, the operating frequency, the modulation parameters or security elements, as appropriate. On the contrary, the fact that the sender has no prior knowledge about the recipients (and their addresses) generally requires the use of communications in broadcast (sometimes multicast) mode, rather than specifically targeting a correspondent (unicast).

It should be noted that once the initial service discovery phase has been completed, it is possible to establish “traditional” connections in order to deepen exchanges with certain special objects. BLE enables, for example, discovery in opportunistic mode and then switching to dedicated channels in BLE or Bluetooth for more substantial exchanges. The same type of example can be envisaged in V2X, where the detection of a vehicle (or group of vehicles) on the control channel (CCH) can lead to the establishment of special relationships on a service channel (SCH), for example, to process exchanges within a platoon or to carry out a financial transaction (toll).

The characteristics of ephemeral local interactions are therefore as follows:

– The information senders and receivers (which can be the same, or two devices with different functionalities) do not know each other beforehand and – often due to mobility – change over time.

– They require prior knowledge of a technology and the channels (frequencies) used to broadcast the information. This therefore presupposes regulation or standardization.

– There is a spontaneous broadcasting of information – without prior contact – in a predetermined, and therefore most often standardized, format. This information is visible to all devices within communication range and listening.

It follows from these basic characteristics that:

– It is difficult to operate on multiple channels, since this presupposes listening to several channels successively, and significantly complicates the encounter between the sent data and a device that is potentially interested.

– This leads to a risk of bandwidth overload, since the load cannot be distributed over several channels as is done in current technologies. Therefore, applications using ephemeral local interactions must be limited to fairly simple data (we will not transmit a 4k video stream).

– Moreover, since an extension of the range is sought, more robust data encoding is often used, since it is understandable with a lower signal-to-noise ratio and therefore at a longer distance. This reduces the available throughput, so in ITS-G5 an encoding of 6 Mb/s is used, while the technology would allow 27 Mb/s to be reached.

– As generalized diffusion (broadcast) or selective diffusion (multicast) is used in most cases, we cannot have an acknowledgment system. Indeed, if the different receivers had to acknowledge each broadcast message, the responses would need to be spread out over a long period of time to avoid collisions. Moreover, this would not be very useful, given that since the sender does not know the list of recipients beforehand, it could not determine that there have been losses;

– The securing of exchanges is quite complicated insofar as the assumption is made that there is no prior exchange of information between the protagonists and that they do not know each other beforehand. Setting up cryptographic material to authenticate the sender or to sign (or encrypt) the content is therefore difficult as there is no trusted third party that can be reached at all times. This is all the more difficult because all or part of the devices are mobile and associated with users; therefore, the use of permanent identifiers is prohibited as this would make it possible to track the user's journey. We will see how different technologies protect themselves from this risk and how the world of cooperative ITS has addressed the need to secure the exchange of sensitive data.

1.2.3. *Advantages of ephemeral local interactions*

The use of ephemeral local interactions does not make it possible to maintain the usual mode of operation of applications and services; however, it offers advantages that are of great interest.

Therefore, ephemeral local interactions do not require prior knowledge of the protagonists. This mode of interaction is often used in an initial discovery phase before returning to a more conventional mode and establishing a connection. Therefore, a Wi-Fi access point will very regularly send announcements (beacons) that enable the stations to discover its existence. The presence of an access point does not make it possible to determine whether or not the latter can offer a service to the mobile terminal, which, in order to do so, will have to attempt to connect to it and establish a secure session. However, simply receiving beacons in itself enables information to be obtained that is useful to the mobile terminal (Chandra et al. 2007), since this is how smartphones obtain their positioning, through fingerprinting techniques and Geographic Information Systems maintained by service providers. As soon as part of this database is stored locally on the mobile terminal, the latter no longer needs the infrastructure in order to calculate its position.

Bluetooth technologies also use beacons that are transmitted on specific channels listened to by mobile devices (Bluetooth Special Interest Group (SIG) 2016). This enables a terminal to discover the presence of a Bluetooth device, and to connect to it if it has already performed the pairing phase. Here, we are therefore not in the operating principle of ephemeral local interactions, but the diverted use of its beacons to detect the presence of mobile terminals or vehicles (through their hands-free kit) corresponds closely to this logic. Therefore, it is possible, from the roadside, to detect vehicles and the unique identifier of their Bluetooth device, which makes it possible to establish input/output matrices by listening to highway access ramps (Barceló 2013; Boudabous 2021).

One of the main benefits of services based on ephemeral local interactions is that they do not require the prior deployment of a network infrastructure. It is therefore possible to rapidly deploy services without relying on an infrastructure, and to withstand permanent or accidental absences on the network infrastructure. The direct or device-to-device (D2D) mode of 3GPP networks on which cellular versions of V2X technologies are based have also found their first application in the field of emergency tactical networks, which must be able to be set up rapidly, when the telecommunication infrastructure has been harmed by a natural disaster. Depending on the application, we will see that it may occasionally be necessary to rely on an infrastructure to manage the securing of exchanges but without requiring it to be permanently available or involved in the normal operation of the service.

Depending on the needs and the communication technologies employed, using ephemeral local interactions enables very fast interactions that depend solely on the message sending frequency and the traffic capacity of the communication technology used. Therefore, the transmission delay will be higher when using BLE beacons (Yang et al. 2020), which must be able to operate for several months/years on a button battery, and which, as a result, will only send a “beacon” every minute. The maximum detection time of a beacon will therefore be of the order of a minute if we take into account the potential losses and the periods when the receiver is not listening to the correct channel. In the case of ITS G5, CAMs (Cooperative Awareness Messages (ETSI 2014)) are sent by default every 100 ms, which, even considering the potential losses, enables very short latencies.

1.2.4. *Suitability of communication technologies for this type of interaction*

The communication technologies used must enable an interaction model that is consistent with ephemeral local interactions. Therefore, it is very much possible to build above IP a service that functions through the regular broadcasting of messages and the use of this information to provide a service without any further dialog with the sender. However, while this presupposes prior connection to a network (e.g. Wi-Fi or Cellular), a large part of the advantages described previously disappear. The underlying communication technologies therefore need to be aligned with the interaction model and the targeted properties.

Adapted technologies generally use a shared multiple-access channel, which means that to access the communication medium, it is not necessary to obtain prior authorization and that everyone can transmit on the channel. There is therefore competition for access to the radio resource, which is for exclusive use (only one sender at a time). A device seeking to send a frame will listen and wait until the channel is free. There is a risk – and mechanisms to reduce it – that two devices will start sending at the same time. When the messages of two senders overlap in time, there is a collision. Some of the potential receivers do not receive either of the two messages, while the other potential receivers decode one message or the other according to the capturing-effect principle (Roberts 1975; Gezer et al. 2010). However, the senders cannot hear the other transmission and do not notice the collision. Regardless of the organization of the radio channel, as soon as there is no device in charge of organizing the resource (such as a base station in the 4/5G networks), and no prior exchange to decide who is allowed to use the resource (RTS/CTS mode in Wi-Fi), the nodes use the resource and then manage the effects of the collisions. When the transmission is directed towards a specific receiver, it is possible to use an acknowledgment and retransmission system (this is the case for Wi-Fi); however, when it is broadcast, losses cannot be detected by the sender, and this must be taken into account in the very construction of the service.

In the case of ITS-G5, a device listens to the channel and transmits only if it is free for a minimum period of time, thus limiting the occurrence of collisions. This type of self-organized system (CSMA: Carrier Sense Multiple Access) works very well up to a certain level of channel occupancy (approximately 60% of the bandwidth) (Bianchi 2000). It is therefore appropriate to introduce mechanisms to limit the network load. Mechanisms are thus used to vary the message frequency according to the usage scenarios and the load of the radio access network. Of course, reducing the sending frequency increases the average time between two receptions and the time needed to discover a new node; this is why it is important to take into account the usage scenario, such as vehicle speed in the context of ITS. Indeed, the lower the velocity of the vehicle, the less its position changes between two announcements.

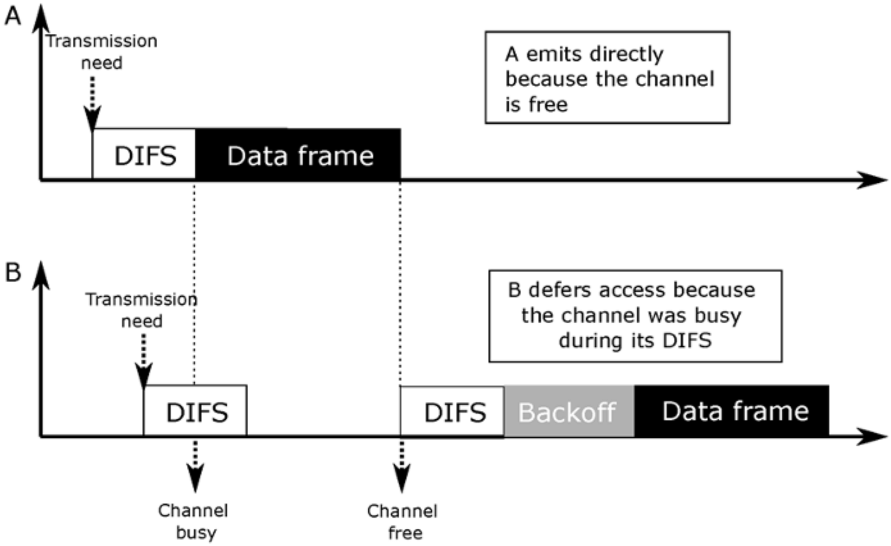

Figure 1.1. *Operation of Wi-Fi CSMA (IEEE 2009)*

In the case of BLE, the very limited bandwidth (typically 1 Mb/s under conventional conditions) will quickly impose constraints on the announcement sending frequency, even if, by design, the messages are limited in size. Since the range is also quite small, this technology could be used for low-velocity applications (pedestrians and VRUs (Vulnerable Road Users) more generally).

In the case of LTE-V2X (Garcia-Roger et al. 2020), the technology developed relatively recently has slightly different properties. Indeed, the radio resource is organized in a frame, with concurrent access to each slot, so that there are several transmissions in parallel on the channel. To limit collisions, due to the very short duration of a slot, it is not possible to listen to decide whether to transmit or not. When the channel is organized by a base station – this is one of the LTE-V2X modes – a station asks to be allowed to transmit before obtaining the resource from the base station. While there can be a collision on the request, the transmission of useful packets is no longer subject to collision. When the channel is self-organized, all the stations share the temporal structure of the frame and must therefore be strictly synchronized. They use semi-persistent scheduling (SPS). This involves listening to the channel and taking advantage of the repetitive nature of regular announcement messages (CAMs) by noting the slots that are occupied in the recent period. For each slot, the station determines the probability that it will be occupied by observing the power level received in that slot for a given duration (1 second by default). It will then select one of the “free” slots for its own transmissions. This selection will then be reviewed regularly. This mechanism works quite well for regular and permanent messages. However, when a collision occurs, it is not detected and lasts until one of the two senders makes the selection again, which becomes critical when the real-time constraints are high.

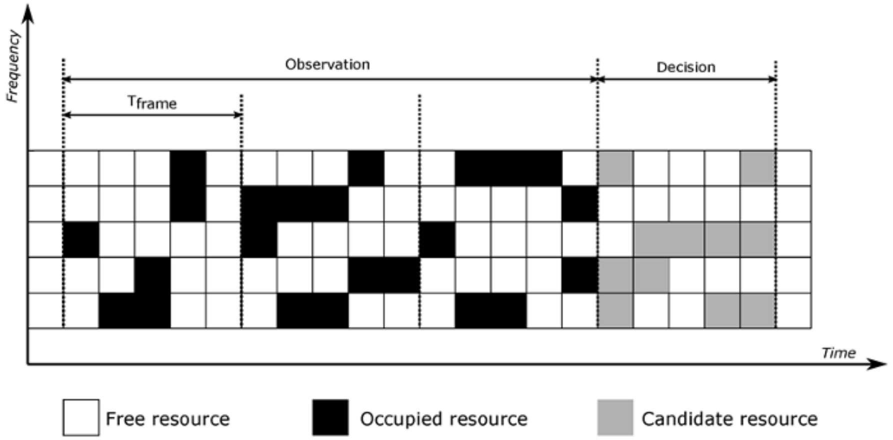

Figure 1.2. *Structure of frames and operation of LTE-V2X semi-persistent scheduling (Haider and Hwang 2019)*

Due to the direct communications between the devices concerned, direct interactions allow very short connection times, given that the announcement messages are frequent and that the receivers constantly listen to the correct channel. Mechanisms to time-multiplex sending and reception extend the time frames and the available bandwidth automatically. When everyone listens to the same channel, the connection time, i.e. the average time required to receive the first message that the receiver is able to decode, is directly related to the message sending period and the distribution of losses on the channel. Indeed, if the losses are not distributed uniformly, the calculation of this average time depends mainly on the maximum duration of the consecutive message loss sequences and on the probability of loss. Losses can be due to collisions, other forms of signal interference or masking. The different forms of interference may be considered to be random. On the contrary, as already mentioned above, collisions are positively correlated with the load submitted to the network, hence the importance of controlling the amount of traffic submitted to the network.

1.3. Local interactions serving cooperative ITS

In this section, we will focus more specifically on the use of ephemeral local interactions in the context of cooperative ITS.

1.3.1. *Cooperative ITS services*

The scope of cooperative ITS (C-ITS) applications is particularly broad. It is traditionally broken down according to the maturity of the technology required. So-called "Day 1" applications are deployable with the technologies currently available. These include the transmission of alerts (slowing down, approaching a priority vehicle, accidents, road works, etc.), signage (on-board display or traffic-light phase) or of presence (position, speed, direction, etc.). In contrast, "Day 2" applications require performance and standardization levels that have not yet been achieved. This covers, for example, driving in convoy ("platooning"), remote driving or vision sharing ("see through"). "Day 1.5" applications are at an intermediate stage: they are feasible for particular cases but their level of standardization does not allow them to be immediately generalized on a large scale. This is the case, for example, with the protection of Vulnerable Road Users (VRU), parking space management or dynamic routing.

As diverse as they are, these applications can be based on the standardization proposed by the "Facilities" layer of the ITS-Station stack. This messaging layer is a kind of middleware between communication layers and applications. This layer is regularly enriched with new functionalities. At this stage, we can cite the following messages as examples:

– CAMs (Cooperative Awareness Messages) (ETSI 2014) are sent regularly (typically every 100 ms) by vehicles to signal their position, speed, direction and physical characteristics. Other vehicles use this information to add the sender to their perception of the environment.

– DENMs (Decentralized Event Notification Messages) (ETSI 2014) are used to signal one-off events such as accidents, construction sites, slowdowns, etc.

– SPAT/SPATEMs (Signal Phase and Time/Extended Messages – ETSI TS 103 301) transmit the traffic-light phase status. They are typically associated with

MAP/MAPEMs (Map Data/Extended Messages) that describe the geometry of roads and intersections.

– IVI (In-Vehicle Information – ETSI TS 103 301) dynamically relays the signage information for on-board display. They replace or complement conventional road signage and are more easily exploitable by the vehicle's automations.

– CPMs (Cooperative Perception Messages – ETSI TR 103 562) enable actors (vehicles and infrastructure) to dynamically exchange information on their perception of the environment (obstacles, vehicles, pedestrians, etc.).

These standardized messages offer an impressive toolkit to accelerate the development and penetration of applications into the market. However, before they start, application designers must analyze the consequences of the choice of message type on the architecture of their solution. Will the application be dependent on an infrastructure or not? Can this infrastructure be decentralized (RSU) or will it require a central server? The answer to these questions will have a strong impact on the cost and ease of deployment of the solution, as well as on its performance (for example, reaction time).

1.3.2. *Benefit of ephemeral local interactions for cooperative ITS*

Here, local interactions offer numerous advantages. They are simple to deploy (as their configuration is very lightweight), require little or no infrastructure (e.g. a light connected to an RSU) and offer very good responsiveness (of the order of several ms to several 100 ms). In addition, limiting wave propagation makes it possible to natively reduce diffusion around areas of interest of the different messages.

The benefit is obviously for collaborative perception applications (based on CAM or CPM messages) or for signage (IVI, SPAT, etc.). In the first case, the speed of transmission is decisive. Also, in all cases, the geographical limitation of broadcasting and the ability to exchange information without the need for prior association constitutes a decisive advantage.

The transmission of warnings (typically by DENM message) represents an interesting case. A network access priority and a sending frequency is associated with the message, based on the emergency associated with the event at the origin of the warning. Therefore, DENM messages relating to an extreme emergency (e.g. in the event of a collision) are sent with maximum priority and at a high frequency to ensure that all approaching vehicles dispose of the information early enough to react (in a few ms).

DENM messages are also used to signal road works or other hazards present on the roadway, in which case, the time constraint is generally more relaxed. For example, it is generally not indispensable to signal the presence of road works in under a second. Moreover, this type of information is sometimes transmitted in V2N (Vehicle to Network) via cellular networks. However, use is often made of V2X – and therefore of local interactions – for these messages too. The reason is twofold: the natural geographical limitation of broadcasting, as well as the fact that the vehicles already have a V2X receiver for other types of messages. In this context, imposing a second receiver only for DENM messages would be counterproductive. Moreover, since it may be necessary to cover a geographical area larger than the range of a V2X transmission, ETSI has provided for the possibility of addressing a geographical area directly in the message header, which is named “geocasting” (ETSI 2009). The messages are thus relayed hop by hop to reach the area of interest without requiring any equipment in the road-side infrastructure.

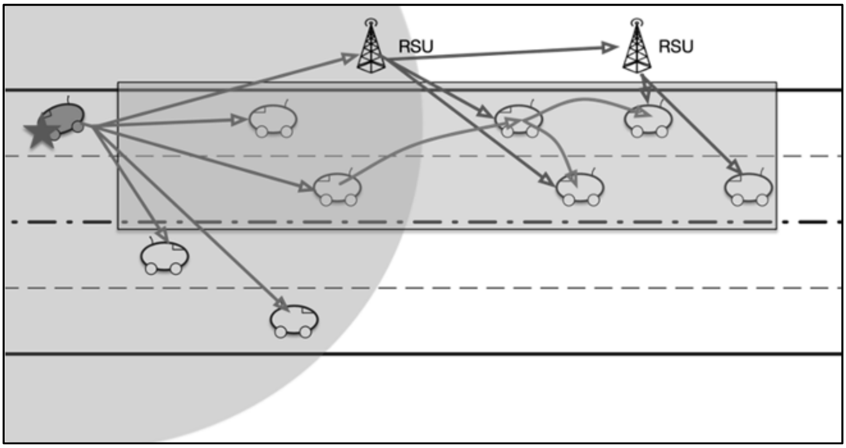

Figure 1.3. *Different modes of DENM message broadcasting. For a color version of this figure, see www.iste.co.uk/mendiboure/transportsystems.zip*

The example of DENMs is also interesting in terms of architecture. It is appropriate to equip a mobile construction site with a mobile RSU to send DENMs, signaling the construction site to approaching vehicles. However, its range will be insufficient to announce the construction site 5 km upstream. For this, the RSU can send the messages in geocasting, but these will not reach their target if there is no vehicle to relay the messages. It is then possible to make use of RSUs that will relay messages as vehicles would do, and without needing to be connected to a network infrastructure; however, this requires RSUs to be specifically deployed if the road is not yet equipped. Lastly, it is possible to make use of a centralized ITS infrastructure and a non-dedicated network infrastructure (e.g. a server that can be reached by a cellular network) so that its message is transferred directly to the vehicles or to the RSUs, which will have to broadcast it downstream. In this case, when no technology meets all the needs, it is useful to combine traditional communications with opportunistic communications.

1.3.3. *V2X communication technologies*

During the work on WAVE architecture (Eichler 2007; Gräfling et al. 2010) in the United States, several types of services were considered, some of which relied on a connected infrastructure. However, covering all roads with a communication infrastructure before the deployment of services is not a reasonable alternative – especially since even if it had been possible, the communication networks of the time did not allow the time constraints to be respected. The choice was made to use direct interactions, requiring the least configuration to minimize the time needed to acquire critical information.

To do this, it was necessary to reserve a communication frequency that everyone can listen to without a connection phase and without complex configuration. The 5 GHz band was chosen and reserved in the United States, and equivalent bands were reserved in Europe and in Japan (with some differences). Once the frequency was selected, it was necessary to agree on the communication technology used and on the organization of radio resources. The initial choice was to start with a well-mastered technology by adapting it to the mobility and needs of ephemeral local interactions. For this purpose, Wi-Fi (IEEE 802.11) was amended (IEEE 802.11p). In Europe, this technology is integrated into the body of ITS standards developed by ETSI under the name ITS-G5.

It should be noted that Wi-Fi, due to its fully distributed channel access control mode, is well suited to ephemeral direct interactions; indeed, by definition, all those who listen to a channel hear all of the messages and decide based on their perception of the channel, whether or not they can send a Wi-Fi frame. Natively, broadcast is used, which makes it possible to mobilize all stations capable of decoding the message. However, in Wi-Fi, even if all of the stations perceive the frames, the communications are relayed by the access point, requiring the prior deployment of an infrastructure, even if the latter does not need to be connected to the Internet to relay the frames between local stations. Among the adaptations made to Wi-Fi, the choice was made to introduce a new operating mode without infrastructure in Wi-Fi: OCB (Outside the Context of a BSS) mode. The other adaptations concern improvements to radio in order to improve the reliability of transmissions in contexts with high-speed differentials (Doppler effect), and with a lot of interference due to fading (urban environment).

For more than 15 years now, numerous projects (SCORE-F, SCOOP@F (Aniss 2016), InDiD, C-Roads and Intercor) have been deploying, experimenting and testing the limits of ITS-G5 in different contexts and for a wide variety of services, so its operating scope is well known.

It should be noted that many other technologies have been (and are still being) considered for direct communications between two vehicles, in particular, to accommodate much higher throughputs (See Through) or even shorter time frames (Platooning and Cooperative Maneuvers). For example, we can mention highly directive technologies such as millimeter waves or visible light communication. For basic services related to security and the perception of other users, as well as the discovery of available services, vehicular Wi-Fi (ITS-G5 in Europe) has long been the only alternative really considered. Today, the situation is a little more complex; two families of incompatible technologies are in the running.

Indeed, cellular network actors have proposed to adapt a variation of LTE's D2D (Device-to-Device) mode to V2X communications (Garcia-Roger et al. 2020; ESTI 2018). Even more recently, 3GPP published standards to offer more advanced services through the adaptation of the new 5G radio interface to V2X (NR-V2X) (ETSI 2020; Storck and Duarte-Figueiredo 2020). The possibility of implementing high value-added and potentially marketable services is one of the challenges of the battle between the two technology families. It should be noted that V2X cellular communications have an infrastructure-free mode that does not rely on the base station to control access and optimize the radio resource. However, they can also use an infrastructure to offer services and, in particular, with the 5G network architecture that promises guaranteed interaction times of the order of milliseconds, which would make it possible, for example, to organize complex maneuvers from servers in proximity to traffic (Mobile Edge Computing).

Technological differences and the debate regarding the choice of technologies is not what interests us in this chapter. It will be necessary, however, to quickly choose a technology, even if it is not perfect, because this is a prerequisite for the deployment of the first services, based on direct interactions. Indeed, everyone must speak at least one common language, if only to discover the presence of others and exchange, without prior complex interactions, messages related to emergency situations.

Other technologies enable direct interactions; for example, they target access control services (wireless car-key) but it requires prior pairing or complex configuration to manage identifications. Note that it is increasingly possible to use a smartphone and standard communication technology (Bluetooth, BLE or Wi-Fi) to implement these services. In any case, these are not the forms of interaction that interest us.

1.3.4. *Properties of C-ITS services built on local interactions*

1.3.4.1. *Latency and reduced responsiveness*

The different C-ITS services do not require the same level of service, but for all, a fairly low latency (less than 100 ms) is sought. It is in fact even shorter for advanced services such as convoy maneuvers (platooning) or cooperative maneuvers. The maximum latency depends on several factors; first and foremost on the communication technology used and how it controls access to the radio resource. Latency also depends on the network load and the state of the radio channel. How the load impacts transmission performance depends directly on the technology used. Therefore, in ITS-G5, the average channel access time increases with the load submitted to the network; however, it is above all the losses due to collisions that end up making the time frames too long. Indeed, the messages are generally transmitted at a certain frequency (10 times per second for CAM messages), which makes it possible to support frame losses while not jeopardizing the service. The losses, which also increase with the load submitted to the network, therefore amount to adding time between messages received successfully.

It should be remembered that due to transmissions in broadcast, it is impossible to use an acknowledgment mechanism and therefore to make transmissions more reliable by retransmitting lost messages. To increase the message transmission rate, LTE-V2X prefers prevention rather than cure, systematically transmitting critical messages twice. While this consumes twice the radio resource, it greatly increases the probability of reception.

The two competing technologies, ITS-G5 and LTE-V2X, use very different mechanisms to control access to the radio resource, and this results in different load behaviors. In both cases, the collision rate increases with the network load, but in the case of ITS-G5, each message competes for access to the channel and can therefore be subject to collisions; in the case of LTE-V2X, the SPS algorithm protects the recurring traffic already established, because the vehicles seeking to send know which resources are occupied. Initial access to the channel is faster in ITS-G5, however, with messages very often delivered in a few milliseconds. In the case of

LTE-V2X, sending a new message requires a certain time frame for choosing the resource (Resource Block) and a collision, the probability of which depends on the network load; this can take place on this resource. In this case, messages are not delivered throughout the duration of the collision (the 100 ms re-selection window), which is a real problem for the most urgent warning messages.

While it is difficult to reduce collision delays in a fully distributed mechanism, it is easier to prioritize access to the radio resource for the most urgent messages. Therefore, ITS-G5 allocates a different priority to the message according to their service class, using the Wi-Fi EDCA (Enhanced Distributed Channel Access) mechanism (ETSI 2019).

1.3.4.2. *Frugality of exchanges and congestion mitigation*

Due to the capacity limits of the radio channel and the number of devices with the potential to send, exchanges must be limited to what is strictly necessary. In addition, it is necessary to favor short messages that free the channel up faster. This is especially true in ITS-G5 because owing to the channel access method (CSMA), a message in the process of being sent cannot be interrupted and prevents vehicles having more urgent messages from accessing the channel. In order to reduce the size of messages and avoid protocol overload due to the TCP/IP stack, the messages have been installed directly above the connection layer with ad hoc protocols[1]. For the same reasons, certificates used to verify the legitimacy of the sender are transmitted only once per second.

Despite these precautions, the vehicle density may be such that it is necessary to prevent channel congestion by limiting the load submitted to the network. In order to evaluate the network load, and because of the lack of centralized coordination, each vehicle can only have, at its disposal, information that it is able to observe by itself, such as: the proportion of time the channel is occupied and the number of vehicles observable in the vicinity. When it measures that the network is loaded, it can play on time by reducing the number of messages and space by limiting the transmission power to reduce the "cost" of a transmission in terms of spectrum occupancy. Some of the mechanisms apply at the radio technology level, while others involve the upper layers (called cross-layer control) to limit the number of messages submitted to the network. This reduction takes into account an assessment – by necessity, simplified – of the usefulness or criticality of the messages. Therefore, the frequency of CAM messages can be reduced to 1 Hz when the vehicle is slow or stationary.

---

[1] The choice of doing without IP in order to limit the protocol overhead is questionable, given that header compression mechanisms exist. When used in the IoT, they are very efficient and reduce the header size to a few bytes (Gomez et al. 2020).

1.3.4.3. *Facilitated privacy*

If the contents of the messages are not directly private in nature, the information transmitted by a vehicle makes it possible to trace the latter and thus reconstruct its journey. More generally speaking, each time a permanent or semi-permanent identifier can be associated with a positioning, there is a risk of allowing tracing.

It is therefore indispensable to mask unique and permanent identifiers. Indeed, radio technologies use unique identifiers (MAC address) that are allocated when manufacturing the radio interfaces and are used as source addresses in the frames. The upper layers also use identifiers (certificate, IP address, etc.) in the different layers of the protocol stack used. For several years now, it has been commonly accepted that the different identifiers used must no longer be able to be associated with a particular terminal. To avoid this, regularly changing random identifiers are used (BT or Wi-Fi). However, care must be taken to change all the identifiers present in a message's different headers at the same time, to avoid two successive identifiers from being associated too easily. Indeed, if the MAC address changes but the identifiers used in the upper layers do not change, an observer will have no trouble attributing the two successive MAC identifiers to the same terminal.

It should be noted that the cost to reconstruct a vehicle's movements is quite significant, since it must be possible to observe the vehicle (listen to messages) at different points of the journey. An infrastructure covering a highway system could thus very easily reconstruct journeys and trip times, as can be done with Bluetooth scanners (Klinkusoom et al. 2014). The fact of masking the identifiers using pseudonyms is relevant in the sense that it greatly complicates the work of the observer seeking to reconstruct the journeys; it is nevertheless not impossible but the effort required to reconstruct journeys depends directly on the pseudonym change rate (Kountché et al. 2017).

In the case of cooperative ITS, the problem is made more complex because of the need to secure exchanges and to ensure a form of control of the legitimacy of the sender to send certain data, and therefore a form of authentication. Authentication and anonymity are generally very difficult to combine, especially when the communications are purely local and therefore without a permanently accessible, trusted third party.

1.3.4.4. *Independence with respect to the functioning of the infrastructure*

It is clear that it will be necessary to have a communication infrastructure to manage deployments and maintain roadside devices. However, once configured, the operation of basic services will depend little on this infrastructure. This makes it possible to imagine very progressive deployments: it is possible to deploy roadside devices only in locations that are hazardous or whose operation can be optimized (complex intersections) and to have devices with only a weak or partial connection to the Internet, the relationship to the management system being used only for device monitoring and configuration. There are therefore few performance constraints weighing on the interconnection network and an already existing non-dedicated network (cellular network) can be used.

This property is significant, given that the economic model to render the communicating infrastructure profitable remains to be found. This is especially true of Day-1 services that are related to road safety aspects and for which a business model based on users' propensity to pay is not easy to find.

1.3.4.5. *Facilitated emergence of new actors*

Due to a naturally open design, the implementation of new services does not depend on the volition of a communication infrastructure operator, since this can be implemented based on direct exchanges.

However, due to security requirements, it may well be necessary to obtain authorizations to be allowed to use messages on frequencies reserved for ITS. Furthermore, signing messages using certificates creates a dependency on the certificate management infrastructure (Haidar et al. 2017). It will therefore be necessary to open the use of these security tools up to other areas (energy, home automation, logistics, etc.) to enable the emergence of new services.

1.3.4.6. *New opportunities in the exploitation of locally produced information (AoA, TOF, RSSI, etc.)*

Local interactions teach us something about the protagonists in interactions, and this information can be used to consolidate or, on the contrary, to question exchanged information. Therefore, for example, the simple fact of being in communication with a BLE beacon teaches us that we are a few meters away from it. The level of the received signal is in itself difficult to use to calculate a distance, but observing the power level of the messages of several protagonists gives us information on their relative positioning. Apart from co-presence (i.e. being within the range of a sender), little use is made of this information today; however, it could, for example, serve to perform a consistency check between the information received and what is observed.

With the evolution of radio technologies, a new type of information is set to become available in the coming years, once active antennas become widespread: the angle of arrival (AoA). Associated with the power level, this information will make it possible to build up an understanding – albeit partial and approximate – of the positioning relative to ourselves of communicating objects within our environment.

1.3.5. Limitations and constraints of implementing services built on local interactions

Local and ephemeral interactions make it possible to do a lot at low cost, but they also suffer from limitations that complicate their implementation and impose hybrid modes in which there is less use made of a communication infrastructure; however, the latter remains just as necessary. The benefit then lies in reducing the constraints weighing on the communication infrastructure in order to use pre-existing, non-dedicated infrastructures.

1.3.5.1. *The need to standardize communication technologies and data exchange*

The first "obvious limitation" is that the implementation of service based on this type of interaction assumes that all devices use the same technology on a reduced set of frequency bands known to all. When the interaction time has to be kept very short (services related to road safety), it is even preferable to reduce the meeting time to a minimum and therefore have a single frequency that everyone listens to. The more sophisticated services can use other channels, or even other technologies, once the appointment has been made on the common channel.

Beyond communication technology and its intrinsic limitations, the fact that everyone listens to the same channel at all times implies that the content of the messages is intelligible to all those who may be concerned. In the case of cooperative ITS, all vehicles and road users, as well as the communicating elements of road infrastructure are concerned. An additional difficulty comes from the fact that messages can contain information intended for users, and they therefore have to be understandable in several languages. The standardization groups have developed message formats that adapt to the uses of the different countries and are translatable through a dictionary mechanism in the different languages.

Lastly, it was necessary to provide a minimum subset of standard messages for vehicles coming from other geographical areas and circulating on European roads through harmonization work between the standardization bodies dedicated to cooperative ITS (e.g. WAVE in the USA, ETSI/CEN ITS in Europe, etc.).

1.3.5.2. *Management of security and trust in distributed mode*

When services are connected, the mechanisms to ensure the security of exchanges is now well mastered and rely on the same solutions as those implemented for conventional Internet services. In particular, it is possible to use the certificate mechanism, which relies on a trusted authority in charge of guaranteeing the identity of a correspondent. The problem worsens when the operation is purely local without the possibility of verifying the identity of a correspondent with a trusted third party – for example, via a public-key infrastructure (PKI).

In the case of cooperative ITS, the issue of security is extremely important as messages may feed automated processes (autonomous driving or advanced driver-assist) that could take full or partial control of a vehicle (emergency braking). Therefore, the simple fact of sending a DENM message to signal emergency braking on a highway at a busy time could create a significant traffic jam. It is therefore necessary to give the message receiver the ability to verify, one way or another, that its content has not been modified and that the sender is legitimate. Verifying the identity of a sender with whom there has been no prior relationship most often relies on a trusted third party. However, as seen, it is not possible to make the assumption that a trusted third party will always be reachable; in any case, the time frames would have been far too lengthy to perform this verification before taking the message content into account.

In the context of cooperative ITS, ETSI has opted to use a mechanism based on certificates signed by a well-known authority. It is thus possible to have confidence in the certificate without first checking with the authority that signed it. However, this does not entirely solve the problem, since this certificate contains an identity and we saw that permanent identities had to be hidden to avoid exposing users' journeys. Therefore, in the same way that pseudonyms are used instead of the permanent identifiers of the different network protocols, pseudonymous certificates are used instead of certificates containing the immutable identity of vehicles and roadside devices. These certificates are produced by a dedicated PKI. Vehicles request a pool of pseudonymous certificates (several hundred) and renew it from the PKI when the current pool is exhausted. These are then used to sign messages and are changed very regularly to avoid the tracing of journeys. In addition to the identity of the referring authority, pseudonymous certificates contain the validity period (lifetime) and a temporary identity. They also include information regarding the role of the sender, thus enabling an emergency vehicle or a road-side unit (traffic lights) to send messages that a simple vehicle will not be allowed to broadcast.

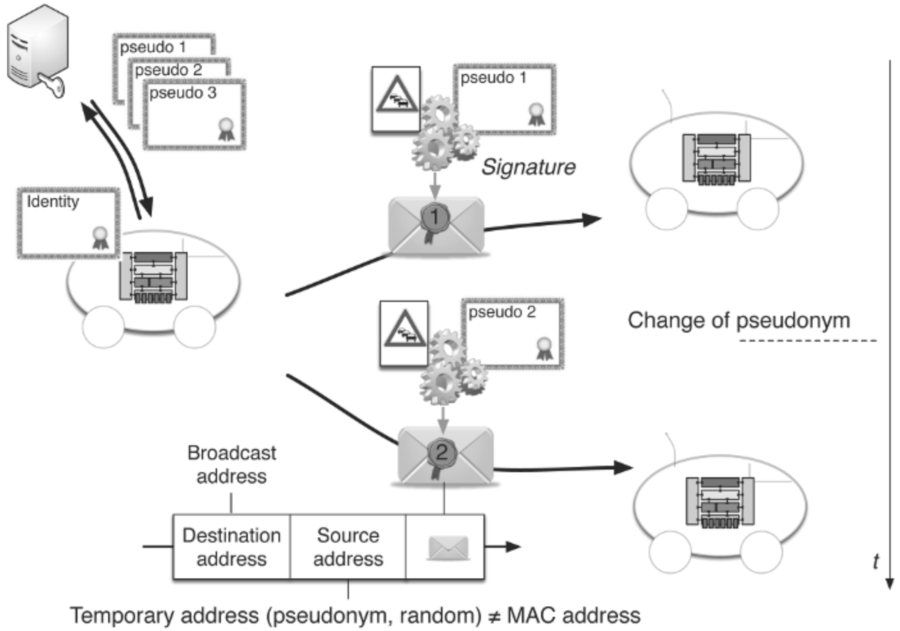

Figure 1.4. *Functioning of pseudonymous certificates. For a color version of this figure, see www.iste.co.uk/mendiboure/transportsystems.zip*

It is worth retaining the concept of a pseudonymous certificate used for a short period of time to protect location privacy, and that they contain a brief description of the actions/messages that a device may legitimately perform. The trusted third party exists but its mobilization is disassociated from the emergency on the field.

The fact that the public-key architecture is necessary implies the need to have a permanent identity provided by the authorities in charge of cooperative ITS for all devices capable of emitting on the reserved frequency band. This introduces significant rigidity compared to the general context of services based on ephemeral local interactions and is a burden for the deployment of new services. While listening to messages is still possible, signature verification presupposes significant resources and dedicated hardware, whenever it is necessary to process a certain message volume. The sent messages will need to be signed in order to be considered valid by the receivers, which presupposes the acquisition of a permanent certificate and a temporary certificate from the public-key architecture dedicated to cooperative ITS.

1.3.5.3. *Interoperability management*

As we have already mentioned, the problem of interoperability between devices that do not have the same technologies is difficult to address. From the point of view of protocols relating to communication, format or semantics of messages, methods exist to mitigate its impacts and it is always possible to update in-vehicle systems to support a new message format and/or a new version of a protocol. For this purpose, the use in networks is to clearly indicate to the receiver which version of the protocol or format of the messages the transmission uses and possibly to provide an extension mechanism that is readable only by those who recognize its identifier. This is very important in a context where standards are very regularly updated and enriched with new functionalities. Moreover, they are not all stabilized yet. Unfortunately, the first versions of the protocols proposed by ETSI did not have these mechanisms.

However, it is important to bear in mind the objective of the first protocols, which was to provide a basic information (awareness) service, in which both vehicles and roadside devices could participate. For these basic services, the objective is to minimize the load and therefore the size and complexity of messages. The benefit of having options that only a few receivers can understand could legitimately be questioned. The more sophisticated services then pass through a dedicated session, thanks to the appointment made on the common channel. This makes it much easier to manage service versions.

Regardless, once deployments have begun, it becomes very complicated to deploy an update that is incompatible with the existing one. It is necessary to provide/allow the possibility of updating the devices already deployed (over the air), and to organize coexistence between different versions of the standards for an indefinite period. This problem of updating vehicle embedded software in deployed objects is a critical subject beyond cooperative ITS. A large part of the communicating objects (IoT) deployed today are rarely, if ever, updated beyond the initial deployment period. Security vulnerabilities are therefore present long after the vulnerabilities have been discovered and documented.

The deployment of several communication technologies incompatible with one another in the same frequency band is very difficult to manage for V2X communications. It is necessary, on the one hand, to organize the coexistence, i.e. sharing of the radio resource; and, on the other hand, to manage the fact that not all vehicles or roadside devices will see all the messages. The problem arises both between two families of technologies and between two generations in the same family. This debate is all the more critical today because there are two families competing, operating in very different ways. However, it would have arisen at one time or another regardless, if only upon the deployment of a new generation of V2X technology, which will inevitably occur at some point. It is completely unrealistic to modify all the devices over a very short period of time, especially considering that some of the devices scattered about in nature will not be connected. It is therefore necessary to anticipate the ways of managing the cohabitation between the different generations.

Sharing the radio resource: organizing sharing of the same radio resource (the same ITS channel) amounts to organizing usage over time. Even if this worked well, it would only solve part of the problem, since devices with one of the technologies would still be deaf to messages broadcast using another technology. In addition, it would have the major defect of reducing the bandwidth available for each of the technologies, especially since the organization of the resource would consume part of the time. Several proposals have been made, and work is underway for ITS-G5 to "hear" the transmissions of C-V2X and take them into account when it decides to emit, and vice versa. However, the semi-persistent scheduling used in C-V2X would be rendered inoperative, since CSMA technology is unable to take it into account.

Managing heterogeneity: the simplest solution would no doubt be to reserve different channels for each of the technologies, but the messages should probably be broadcast on both channels by devices with both technologies and possibly relayed by these devices when the source has only one of them at its disposal. The organization of this relaying poses similar problems to multi-hop broadcasting in self-organized (ad-hoc) networks and is not trivial to solve. It is indeed necessary to choose who relays the message when several devices are capable of doing so in order to maximize the number of receivers, while not over-occupying the channel with multiple copies of the same message.

1.4. Role of infrastructure in cooperative ITS services

1.4.1. *Infrastructures dedicated to cooperative ITS*

If we consider the need to deploy infrastructures dedicated to certain services – in the following, we will discuss mainly cooperative ITS services and more generally services related to the mobility of goods and people – it is important to consider the distribution of the cost of deployment and operation of its infrastructures. While at the start of WAVE architecture standardization in the United States, it was envisaged for all roads to be covered with a dedicated infrastructure (based on the IEEE 802.11p amendment), this idea did not survive the various financial crises. In any case, it is unrealistic and does not solve any of the engineering problems related to the necessary support of the discontinuity of coverage; if only because it is impossible to achieve full coverage before deploying the first services.

It is therefore essential that the various services operate opportunistically to take advantage of existing infrastructure when available, whilst otherwise maintaining autonomous operation. For a large part of the services developed within the framework of cooperative ITS, the V2X mode without infrastructure involving only vehicles is therefore the favored mode. Augmented modes with more functionalities or better performance are considered when the infrastructure is available. Hybrid modes using Internet connectivity (often cellular) are also envisaged for information services with low time constraints.

The presence of active devices in the infrastructure does not necessarily mean that these devices are interconnected, nor that they are connected to the Internet, and even less that they offer vehicles the possibility of interacting with servers, whether they are centralized (cloud) or remote as close to usage as possible (edge computing). However, these are configurations that each offer different possibilities:

– Independent infrastructure devices: in this configuration, it is possible to simply deploy devices that will serve to support certain services and that do not need to be connected to the Internet (or only for remote maintenance matters). The device will use V2X technologies and behave like a vehicle to listen to and transmit information. As an example of this type of device, we can cite the traffic lights that announce the phase of the lights and the configuration of the intersection to approaching vehicles. Another example is the replacement of the current passive signage and a simple small device can announce a priority to the right or a speed limit. Lastly, these devices can play a very important role in extending the scope of DENM messages by relaying them. For more advanced uses, a micro-server placed in an intersection or on a highway entrance ramp, can be in charge of facilitating communications and possibly organizing traffic. The possibilities offered by this type of deployment are already very numerous and the deployment can be very gradual, since it is possible to instrument only the places that require it (hazardous intersections), and vehicles using the information that is available to make traffic more efficient.

– Connected infrastructure devices: the services offered can be much more dynamic here; for example, it is possible to announce coming hazards or deviations. Announcements made can replace variable-message signs. This type of infrastructure is also of great interest in offering much more advanced services, such as platooning assistance, if it is possible to follow vehicle convoys along their journey. Lastly, thanks to roadside stations, it is possible to collect messages transmitted by vehicles and transmit them to central servers that will be able to calculate journey times, identify distributed-attack attempts and relay warning messages sent locally by the vehicles on a larger scale. Some of the observations that are made by cameras today could thus be made through messages regularly transmitted by vehicles.

– Infrastructure devices relaying the traffic to central servers: in this configuration, we leave the world of ephemeral local interactions in the sense that interactions do not remain local. Vehicles learn by listening to roadside stations that they are able to offer Internet connectivity. A vehicle needing to download a list of pseudonymous certificates, for example, can establish a session through the connectivity offered by the roadside station. The difficulty lies in maintaining connectivity long enough to establish a secure session with a server and to exchange data. It is thus much simpler to use conventional cellular communications to achieve this type of service or to wait to be static for a while.

1.4.2. *Towards an active infrastructure*

When we talk about V2X communication technologies, we think first of all of inter-vehicular communications, but it also includes communications between vehicles and the nearby infrastructure: RSUs (Road-Side Units). The latter can relay or directly host a very large number of services intended for both TOAs (Transport Organizing Authorities) and infrastructure managers to collect information, vehicles to offer information services (traffic-light phase) and collaborative perception or support services, such as the organization of traffic in a complex intersection. They can also serve other users, such as cyclists or pedestrians, and form a link between different user categories. We will then speak of active infrastructure, and in the following, we give an example of two service categories.

1.4.2.1. *Collaborative perception*

An active infrastructure is very useful for increasing the perception capacity of vehicles in complex environments. Therefore, surveillance cameras positioned in an intersection can announce a description of the intersection, including moving objects and pedestrians. Consequently, a vehicle will be able to perceive pedestrians that are masked from it and take them into account in its trajectory and speed decisions. The question of confidence in the information announced is crucial here and will need to be addressed; indeed, an autonomous vehicle could only pass at full speed through a blind intersection if the infrastructure tells it that the lane is clear, insofar as the vehicle trusts it.

1.4.2.2. *Heterogeneity support*

This same active infrastructure could take charge of relaying information between two incompatible technologies, provided that it has the various communication technologies at its disposal. In the same way, it can draw on its ability to perceive non-communicating objects (pedestrians, cyclists, as well as non-equipped cars) to instead send CAM messages, which will enable equipped vehicles to take them into account (Tsukada et al. 2020). The active infrastructure becomes a means of facilitating deployments by reintegrating non-communicating objects into the C-ITS mechanisms.

1.5. Conclusion and prospects

Services based on ephemeral local interactions are not yet frequent if potential partner discovery mechanisms present in many wireless technologies are excluded. Once the discovery is made, direct interactions are used to establish a connection and offer a service (connection to a hands-free kit in BT).

In this chapter, we reviewed the properties of services relying on this type of interaction and demonstrated the benefit of relying on them in the field of cooperative ITS.

One of the difficulties is then to put in place standards – this is largely done at ETSI, ISO and CEN – to define a language and a mode of interaction common to all objects that can cooperate. Since this mode of interaction is relatively new, it is important to experiment on a large scale what has been done for several years now with major European initiatives. The projects SCOOP@F (Aniss 2016), INDID, C-road, etc., aim to precisely organize the ecosystem under the aegis of the French Ministry of Transport to evaluate the functioning of the services that will be deployed in the coming years. This pooling of resources within a national experimental platform is necessary in that devices, whether in-vehicle, deployed along roads or in central systems, will have to cooperate with each other. The tests, in particular, of interoperability, that could be performed by a group of actors would necessarily have too little coverage to be representative of the complexity of real deployment.

Moreover, the question of whether it is appropriate to deploy the vehicles or the infrastructure first has delayed the process for a long time, the former waiting for the services offered by the infrastructure to become available in order to justify the additional cost related to the implementation of OBUs (On-Board Units) in vehicles. While the simplest approach would probably be for a regulation to require all new vehicles to have V2X communications, another approach consists of gradually deploying infrastructure devices first for the needs of infrastructure managers and then gradually offering new services to equipped vehicles. Existing services (traffic-light control) can then be modified to use V2X communications rather than proprietary solutions. They would immediately benefit from all protocols and messages already defined to further improve the service. For example, SPAT/MAP messages can be used to regulate approach speed and prevent a bus from coming to a complete stop.

The progressive enrichment of the infrastructure with RSUs (Road-Side Units) equipped with V2X technology enables the environment to be enriched with data that may be used by a wide variety of services. These same devices can also broadcast the same information using other media to reach other classes of users: for example, smartphones. This will make it possible to apply the same basic technologies, operating principles and exchange protocols to other fields, and thus reduce the costs of deploying new innovative services.

1.6. References

Aniss, H. (2016). Overview of an ITS project: SCOOP@ F. In *Communication Technologies for Vehicles: 10th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2016,* San Sebastián, 6–7 June, 131–135. Springer, Cham.

Barceló, J., Montero, L., Bullejos, M., Serch, O., Carmona, C. (2013). A Kalman filter approach for exploiting bluetooth traffic data when estimating time-dependent OD matrices. *Journal of Intelligent Transportation Systems*, 17(2), 123–141.

Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3), 535–547.

Bluetooth Special Interest Group (SIG) (2016). Specifications and documents [Online]. Available at: https://www.bluetooth.com/specifications/bluetooth-core-specification [Accessed July 2021].

Boudabous, S. (2021). Vehicular traffic analysis based on Bluetooth sensors traces. Doctoral Dissertation, Institut polytechnique de Paris.

Chandra, R., Padhye, J., Ravindranath, L., Wolman, A. (2007). Beacon-stuffing: Wi-fi without associations. In *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, 53–57.

Eichler, S. (2007). Performance evaluation of the IEEE 802.11 p WAVE communication standard. In *2007 IEEE 66th Vehicular Technology Conference*, 2199–2203.

ETSI (2009). TR 102 638 V1.1.1; Intelligent Transport Systems (ITS); Vehicular communications; Basic set of applications; Definitions. ETSI Technical Report, Sophia Antipolis.

ETSI (2011). TR 102 863 V1.1.1; Intelligent Transport Systems (ITS); Vehicular communications; Basic set of applications; Local dynamic map (LDM); Rationale for and guidance on standardization. ETSI Technical Report, Sophia Antipolis.

ETSI (2014). EN 302 637-2 V1.3.1; Intelligent Transport Systems (ITS); Vehicular communications; Basic set of applications; Part 2: Specification of cooperative awareness basic service. ETSI Standard, Sophia Antipolis.

ETSI (2018). TS 103 574 – V1.1.1; Intelligent Transport Systems (ITS); Congestion control mechanisms for the C-V2X PC5 interface; Access layer part. ETSI Standard, Sophia Antipolis.

ETSI (2019). EN 302 663 – V1.3.1; Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. ETSI Standard, Sophia Antipolis.

ETSI (2021). TS 124 587 – V16.0.9; 5G; Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3 (3GPP TS 24.587 version 17.8.0 Release 17). ETSI Standard, Sophia Antipolis.

Garcia-Roger, D., González, E.E., Martín-Sacristán, D., Monserrat, J.F. (2020). V2X support in 3GPP specifications: From 4G to 5G and beyond. *IEEE Access*, 8, 190946–190963.

Gezer, C., Buratti, C., Verdone, R. (2010). Capture effect in IEEE 802.15. 4 networks: Modelling and experimentation. In *2010 IEEE 5th International Symposium on Wireless Pervasive Computing*, 204–209.

Gomez, C., Minaburo, A., Toutain, L., Barthel, D., Zuniga, J.C. (2020). IPv6 over LPWANs: Connecting low-power WANs to the Internet (of Things). *IEEE Wireless Communications*, 27(1), 206–213. doi: 10.1109/mwc.001.1900215.

Gräfling, S., Mähönen, P., Riihijärvi, J. (2010). Performance evaluation of IEEE 1609 WAVE and IEEE 802.11 p for vehicular communications. In *2010 Second International Conference on Ubiquitous and Future Networks (ICUFN)*, 344–348.

Haider, A. and Hwang, S.H. (2019). Adaptive transmit power control algorithm for sensing-based semi-persistent scheduling in C-V2X mode 4 communication. *Electronics*, 8(8), 846.

Haidar, F., Kaiser, A., Lonc, B. (2017). On the performance evaluation of vehicular PKI protocol for V2X communications security. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 1–5.

IEEE 802 LAN/MAN Standards Committee (2009). IEEE Standard for Information Technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs [Online]. Available at: http://standards.ieee.org/getieee802/download/802.11n-2009.pdf.

Klinkusoom, L., Aswakul, C., Janpugdee, P. (2014). Bluetooth sensors for vehicular traffic monitoring. In *The 29th International Technical Conference on Circuit/Systems Computers and Communications*, Phuket.

Kountché, D.A., Bonnin, J.M., Labiod, H. (2017). The problem of privacy in cooperative intelligent transportation systems (C-ITS). In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 482–486.

Roberts, L.G. (1975). ALOHA packet system with and without slots and capture. *ACM SIGCOMM Computer Communication Review*, 5(2), 28–42.

Roca, V. (2022). TousAntiCovid : gros plan sur les deux protocoles de traçage numérique de l'application. In *Médecine et intelligence artificielle*, Nordlinger, B., Villani, C., de Fresnoye, O. (eds). CNRS Editions, Paris.

Storck, C.R. and Duarte-Figueiredo, F. (2020). A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE Access*, 8, 117593–117614.

Tsukada, M., Oi, T., Kitazawa, M., Esaki, H. (2020). Networked roadside perception units for autonomous driving. *Sensors*, 20(18), 5320.

Yang, J., Poellabauer, C., Mitra, P., Neubecker, C. (2020). Beyond beaconing: Emerging applications and challenges of BLE. *Ad Hoc Networks*, 97, 102015.