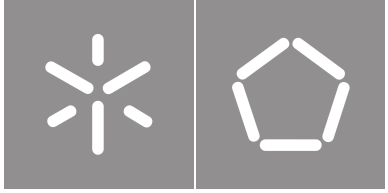
Universidade do Minho
Escola de Engenharia

John Very Longname Doe

A Very Long and Impressive Thesis Title with a Forced Line Break

month, year

A Very Long and Impressive Thesis Title with a Forced Line Break
John Doe
UMinho | year



Universidade do Minho
Escola de Engenharia

John Very Longname Doe

A Very Long and Impressive Thesis Title with a Forced Line Break

Master Thesis
Master in Study Program Name

Work developed under the supervision of:
Mary Doe Adviser Name
John Doe Co-Adviser Name
John Doe other Co-Adviser Name

month, year

This document was created with the (pdf/Xe/Lua)LaTeX processor and the NOVAthesis template (v7.1.18) [1].

Acknowledgements

Acknowledgments are personal text and should be a free expression of the author.

However, without any intention of conditioning the form or content of this text, I would like to add that it usually starts with academic thanks (instructors, etc.); then institutional thanks (Research Center, Department, Faculty, University, FCT / MEC scholarships, etc.) and, finally, the personal ones (friends, family, etc.).

But I insist that there are no fixed rules for this text, and it must, above all, express what the author feels.

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the Universidade do Minho.

_____, _____

(Place) (Date)

_____

(John Very Longname Doe)

”

“You cannot teach a man anything; you can only help him discover it in himself.”

— Galileo, Somewhere in a book or speach
(Astronomer, physicist and engineer)

Resumo

Um Título de Tese Longo e com uma Mudança de Linha Forçada

Relativamente ao seu conteúdo, os resumos não devem ultrapassar uma página e frequentemente tentam responder às seguintes questões (é imprescindível a adaptação às práticas habituais da sua área científica):

1. Qual é o problema?
2. Porque é que é um problema interessante/desafiante?
3. Qual é a proposta de abordagem/solução?
4. Quais são as consequências/resultados da solução proposta?

Palavras-chave: Redes vehiculares, Redes definidas por software

Abstract

A Very Long and Impressive Thesis Title with a Forced Line Break

Concerning its contents, the abstracts should not exceed one page and may answer the following questions (it is essential to adapt to the usual practices of your scientific area):

1. What is the problem?
2. Why is this problem interesting/challenging?
3. What is the proposed approach/solution/contribution?
4. What results (implications/consequences) from the solution?

Keywords: Vehicular networks, Software defined networks

Contents

List of Figures

List of Tables

Glossary

This document is incomplete. The external file associated with the glossary 'main' (which should be called `template.gls`) hasn't been created.

This has probably happened because there are no entries defined in this glossary. If you don't want this glossary, add `nomain` to your package option list when you load `glossaries-extra.sty`. For example:

```
\usepackage[nomain,acronym]{glossaries-extra}
```

This message will be removed once the problem has been fixed.

Acronyms

This document is incomplete. The external file associated with the glossary 'acronym' (which should be called `template.acr`) hasn't been created.

Check the contents of the file `template.acn`. If it's empty, that means you haven't indexed any of your entries in this glossary (using commands like `\gls` or `\glsadd`) so this list can't be generated. If the file isn't empty, the document build process hasn't been completed.

Try one of the following:

- Add `automake` to your package option list when you load `glossaries-extra.sty`. For example:

  ```
  \usepackage[automake]{glossaries-extra}
  ```

- Run the external (Lua) application:

  ```
  makeglossaries-lite.lua "template"
  ```

- Run the external (Perl) application:

  ```
  makeglossaries "template"
  ```

Then rerun LaTeX on this document.

This message will be removed once the problem has been fixed.

Symbols

This document is incomplete. The external file associated with the glossary 'symbols' (which should be called `template.sls`) hasn't been created.

This has probably happened because there are no entries defined in this glossary. Did you forget to use `type=symbols` when you defined your entries? If you tried to load entries into this glossary with `\loadglsentries` did you remember to use `[symbols]` as the optional argument? If you did, check that the definitions in the file you loaded all had the type set to `\glsdefaulttype`.

This message will be removed once the problem has been fixed.

1 Introduction

This chapter is an introduction to this paper, where the context, motivation, objectives and methodology of this thesis is explained.

1.1 Contextualization

The internet is considered to be one of the most revolutionary inventions in the history of humanity, and it´s widespread adoption has brought about countless benefits and has forever changed the way we live and communicate. Despite its many strengths, the way internet works today shows some limitations in the face of an increasingly mobile world. With the wide spread adoption of automobiles, it was noticed that connecting these vehicles to each other over the internet could offer some major benefits to road security and could bring quality of life improvements to drivers. However, due to its static nature, the internet cant handle moving communications, and therefore is not ready for this transformation. Software defined networks is a new technology that centralizes control of a network in a single device, promising more control over the network and greater flexibility. To address the limitations of the internet and to facilitate further growth, researchers have turned to this new and exciting field. SDN offer a promising solution to many of the challenges faced by the current internet landscape. Therefore, a lot of recent studies have applied SDNs to vehicular networks in order to create better solutions for the future.

1.2 Motivation

In recent years, there has been a growing interest in the application of SDN technology in vehicular networks, with a large number of projects in SDVNs being created. Even doe these projects aim to be used in the real world, the large majority of them is restricted to simulation-based testing which reduces the veracity of the results. Therefore, this highlights a pressing need for the availability of real hardware testing platforms, in order to achieve more accurate and reliable results in such a critically important area. The development of a real hardware testing platform for SDVN projects will allow for a more comprehensive evaluation of the technology, which is a step further for this technology to become accepted and used.

1.3 Objectives

Our main goal in this thesis is to design and assemble a hardware device similar to an OBU, utilizing open-source software where possible. This device must be SND compatible, so its routing tables must be configurable by a local or remote SDN controller. To meet these requirements, the device will run an open-source V2X protocol stack on a Linux-based OS.

1.4 Methodology

Initially, an investigation will be done to find the software required for the implementation of an OBU controlled by a free controller. Subsequently, a new OBU device will be designed and assembled, using modern hardware. Finally, performance and security vulnerabilities will both be tested.

1.5 Document structure

Chapter 2 is divided into three main sections. Section 2.1. aims to provide a broad context about vehicular networks, in order to understand the main challenges in this field. In section 2.2., a very detailed overview of SDN is made, with a large emphasis on the data and control plane, to show the power and potential of this technology. Section 2.3. serves to address what are the advantages and shortcomings of using SDN in a vehicular context. In Chapter 3, a state of play is made, where the plan to achieve the goals of this thesis is highlighted.

2

Vehicular ad hoc Networks

The automobile was one of the most revolutionary inventions in human history, for most cities around the world are dependent on cars for the transportation of goods and people and, therefore, the prevalence of vehicles in our daily lives is greater than ever before. Even though it is impossible to predict if future vehicle usage will continue to be as dominant as today, it is reasonable to assume that this technology will never disappear completely. Even today, in cities dominated by alternative modes of transportation, the use of motorized vehicles is still present and, in some cases, a necessity.

It has been a long-time goal for car manufacturers and researchers to bring internet connectivity to automobiles, as the benefits are enormous. The Internet is an extremely powerful technology, not only for the countless services it provides but also for the ability of two endpoints to communicate almost instantly. Moreover, recent improvements to wireless communication technologies not only make this goal more realistic but also even more attractive, as integrating network interfaces with GPS receivers and sensors only increases the potential of allowing cars to communicate with each other [2].

The efforts to bring connectivity to automobiles resulted in the emergence of the technology named VANET, which is an adaptation of the Mobile ad hoc Network (MANET) technology, specialized for automobiles [3] [4]. In contrast to wired networks, where all devices are connected to the infrastructure at all times to communicate with each other, this technology allows devices to transmit data directly to other devices inside its range, as illustrated in Figure 1. As a result, networks are generated spontaneously between nodes that are in range of each other, which makes topologies unstable and requires each node in the network to act as both a transmitter and a receiver.

As the Internet was not designed with mobility in mind, most protocols and standards were not developed to support the high-speed scenarios of VANET. A tremendous amount of work and research efforts has already been conducted in this area, amounting to decades of research, development, and standardization. However, the development of VANET technology began without any major centralized entity to standardize its implementation worldwide, resulting in various architectures emerging simultaneously all around the globe. It is common for different regions of the world to develop different standards for infrastructure-related technologies and these solutions tend to converge as they seek to solve the same problems in the most optimal way.

The leaders in global research on VANETs are considered to be the United States, Japan, and the

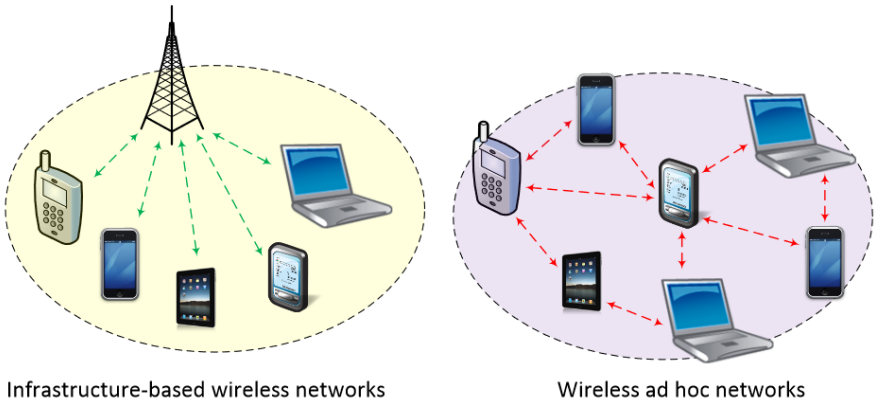


Figure 1: Comparison between infrastructure networks [5]

European Union. These regions are noteworthy as they have provided the majority of the technological foundations and advancements in the field. For the sake of clarity and relevance, this paper focuses on the European VANETs architecture through the discussion of the C2C-CC and the European Telecommunications Standards Institute (ETSI), two prominent and influential institutions in the field.

The C2C-CC architecture proposal is designed with a high level of abstraction and is therefore fairly easy to understand. In contrast, the ETSI standards are significantly more detailed and technical, since they provide the official standard for the European Union. ETSI uses the term ITS to refer to VANETs, as their efforts to connect vehicles together goes beyond cars and aims to interconnect planes, trains, boats, etc.

There are other conventions in this field, such as the C-ROADS platform, which are important for the development of this technology. In fact, several conventions have influenced the ETSI standards and would be worth discussing. However, in order to avoid overcomplicating the subject, only the ETSI and C2C-CC architectures will be covered.

2.1 VANET characteristics

The VANET technological domain was established as a specialized subset of the MANET research field based on some unique characteristics, and thus VANET shares most of its properties with MANET. Some key differences require the development of novel solutions, and in this section, we will go through all the characteristics of VANET while shedding light on what sets this technology apart from its origin.

2.1.1 High mobility

MANET topologies are highly dynamic, driven by the mobility of nodes. High mobility leads to uncertain connectivity, which makes ad-hoc topologies extremely volatile and unpredictable, with a high chance of partitions[6]. VANETs not only inherit this characteristic but also amplify its volatility since VANET nodes are vehicles capable of traveling at extremely high speeds.

For instance, two cars traveling in opposite directions on the same road will only be within range of each other for a few seconds. In this short time, the vehicles must attempt to establish a connection before attempting to exchange valuable information, which means some links may be disconnected before there is a chance to use them [4]. On the other hand, two cars traveling in the same direction can maintain a connection indefinitely as long as they keep on the same path at the same speed. These two scenarios are polar opposites, making the reliability of connections inconsistent.

2.1.2 Predicted mobility

Beyond being more dynamic, MANET topologies are also random, as nodes can move arbitrarily and at unpredictable times, with virtually no restraint. VANET topologies diverge from MANET in this matter, as it is possible to reliably predict the path of nodes in an ad-hoc network. Vehicles are primarily used on pre-built infrastructure [4], like roads and motorways, and have to follow predetermined paths to reach their destination, which makes it possible to predict their future location. Vehicles are also forced to obey road signs and traffic lights and have to respond to other vehicles' movements[3], making topologies even more predictable.

On top of all of that, if drivers disclose their desired destination it becomes possible to predict the complete route of a node with near 100% precision. It is important, however, to keep in mind that this is not always true, and in some instances, drivers may adjust their path in reaction to the information received by the network[4].

A negative consequence of road use can be seen in more linear topologies when compared with MANETs, which inevitably undermines path redundancy[6].

2.1.3 Power and Computational ability

Another relevant change from MANETs is the computational capabilities and power constraints of the nodes. MANET was designed with small devices in mind, which have limited battery capacity and computational power constraints. In contrast, vehicles have access to a reliable power source[4][2], so there are essentially no concerns in this regard. However, cars should not be thought of as an infinite power source, and normal precautions should be taken when optimizing routing algorithms, etc.

2.1.4 Congestion and Scalability issues

VANET suffers from an absurdly variable node density. A vehicle can be on a road in a remote location with the nearest internet connection of other vehicle kilometers away from their location, or in the middle of a traffic jam at an intersection surrounded by hundreds of vehicles all trying to communicate within its range.

Congestion scenarios create a bandwidth problem that is exacerbated by the presence of nearby obstacles like other cars and buildings, which common in an urban environment[6]. Wireless links are significantly more fragile than their wired counterparts because they are subject to fading, noise and

interference[7]. This also forces researchers to come up with effective measures for sharing physical media, as another issue of concern is ensuring Quality of Service (QoS) measures for critical messages, like road hazard warnings, which presents a core issue[6].

Variable network density presents a necessity for the protocols developed to be capable of dealing with any situation thrown at them in the real world.

2.2 VANET components

The first step in the understanding VANET scenarios is the analysis of the basic elements involved. With this in mind, the atomic components of both the C2C-CC and ETSI are explained in this section.

2.2.1 C2C-CC approach

According to the C2C-CC architecture, three main components can be identified, these being the RSU, OBU and Autonomous Unit (AU).

1. Roadside Units are stationary devices placed alongside roads, usually in high-density zones such as junctions, intersections and traffic lights.

   These devices have a reliable connection to the Internet and communicate with all vehicles within their effective range, bridging the gap between vehicle ad hoc networks and the rest of the Internet. RSUs can also be equipped with multiple communication devices for optimal wireless connectivity. In addition, RSUs can also take advantage of the ad hoc characteristics of on-board units by using them as transmitters, thereby extending their effective range, as depicted on Figure 2.

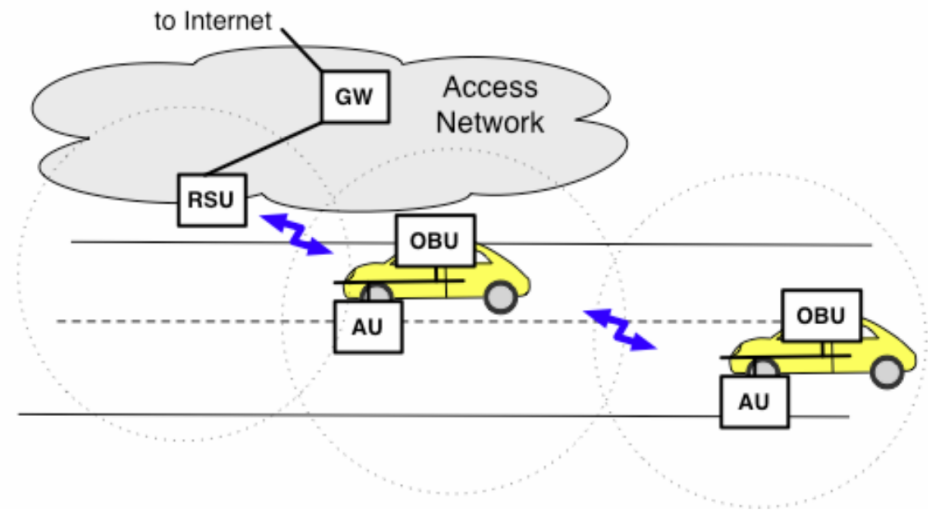


Figure 2: A RSU provides Internet connectivity through an OBU. [8]

RSUs can run safety applications like fixed road hazard warnings (work-zone warnings, bridge warnings, etc.) by broadcasting safety messages to nearby vehicles, making them more than mere connection points for vehicles.

2. On Board Unit is a small device integrated into vehicles that operates in the ad hoc space as they receive, send, and forward messages between each other and with RSUs in an ad hoc manner. OBUs provide it's wireless communication capabilities to any connected device used within the vehicle.

3. The term Autonomous Units refers to all the various devices that run a single or a set of applications that connect to the OBU and harness its wireless capabilities. The AUs can be physically integrated or permanently wired to the OBU being an integrated part of the vehicle. These types of AUs are typically safety-related applications. AUs can also be wireless devices like laptops or smartphones, wirelessly connecting to an OBU and utilizing its capabilities for leisure applications.

4. In addition to these three main components, this institution acknowledges the potential presence of other network entities, like public hotspots, instances of a Mobile Internet Protocol (IP) infrastructure, application servers, control centers, etc. However, these are not categorized and are therefore outside of the scope of this Consortium.

2.2.2 ETSI approach

The ETSI standard diverges from the simple and straightforward definition of the C2C-CC by specifying two categories to define the communication entities of VANETs: the ITS sub-systems and the functional components. The former, comparable to the C2C-CC components, represent similar system categories that exist in the VANET space. The latter are the building blocks that make up the ITS subsystems and are therefore responsible for specific functions or tasks within the overall systems.

2.2.2.1 Functional components

The functional components described in this architecture follow the layered conceptual structure of the OSI model [9], comprising five such components: the ITS station (ITS-S) host, the ITS-S gateway, the ITS-S router, the ITS-S border router and the ITS-S interceptor.

The most significant component of this architecture is the ITS-S host, since it provides the minimum level of functionality required to run ITS applications. It represents the basic reference architecture for any device wishing to communicate in the VANET space, and is present on all ITS sub-systems. This architecture is described in depth in section 2.5

In addition, all other components are a variant of the ITS-S host, adding communication capabilities to it. The ITS-S gateway converts messages from the Internet to the ITS domain at layers 5 to 7 of the OSI model. The ITS-S router converts various ITS protocols at layer 3, and the ITS-S border router performs a similar task, doing the same as the router, but with a more generic network, without management or

security awareness. The ITS-S interceptor is a generic term equivalent to any of the previous three components, plus it can represent an implementation-specific connection of the ITS station-internal network to another network.

2.2.2.2 Sub-systems

As previously introduced, all functional components come together to form various sub-systems, of which there are four. These sub-systems represent a specific context in which the functional components combine to attempt to provide wireless communication capabilities, either in the form of direct contact with the ad hoc environment or indirectly.

All ITS sub-systems consist of the unique context they support and a specific ITS station to meet the needs of that unique situation. These stations can also be implemented in a single physical unit or in multiple physical units.

1. Personal ITS sub-system:

   The Personal ITS sub-system represents a mobile or other personal device that can connect to the vehicle's internal network and use its ad-hoc wireless capabilities. It includes the user's device and a Personal ITS Station. This station is the simplest of the four, consisting of a single ITS host. This can be observed in Figure 3.

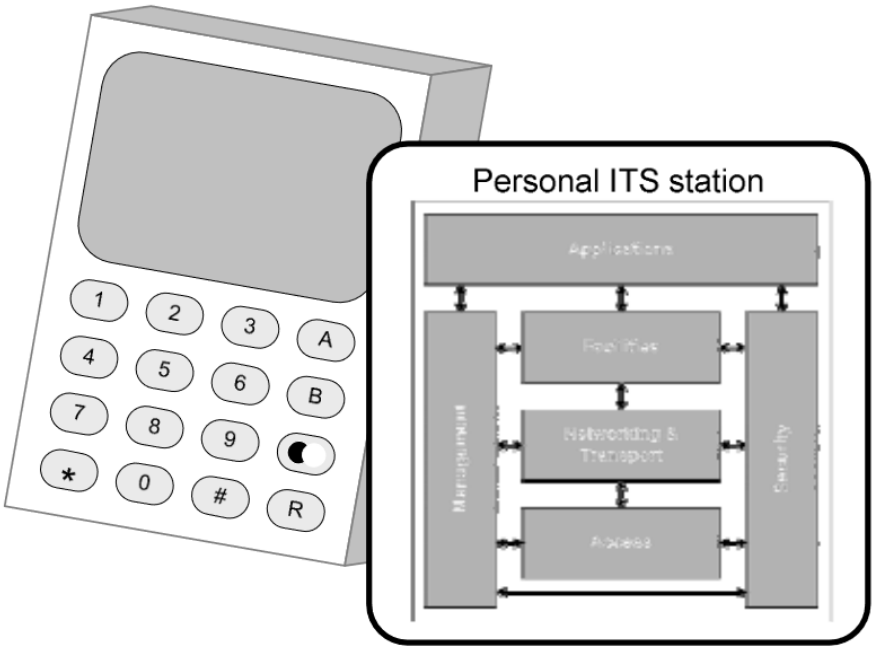


Figure 3: Personal ITS station in a Personal ITS sub-system [9]

This sub-system is comparable to an AU, with a narrower definition. The ETSI architecture defines the existence of an ECU, which also falls under the AU definition created by the C2C-CC. The ECU will be described along with the vehicle ITS sub-system.

2. Central ITS sub-system; The purpose of the Central ITS sub-system is to provide centralized ITS applications, like traffic operations or content delivery, to VANET users. It is composed of a central ITS station that can be located anywhere. Examples of a Central ITS sub-system are traffic management centers and road operator centers.

   The Central ITS station contains an ITS host and two optional ITS interceptors, being an ITS gateway and border router. The Central ITS sub-system is represented in Figure 4.

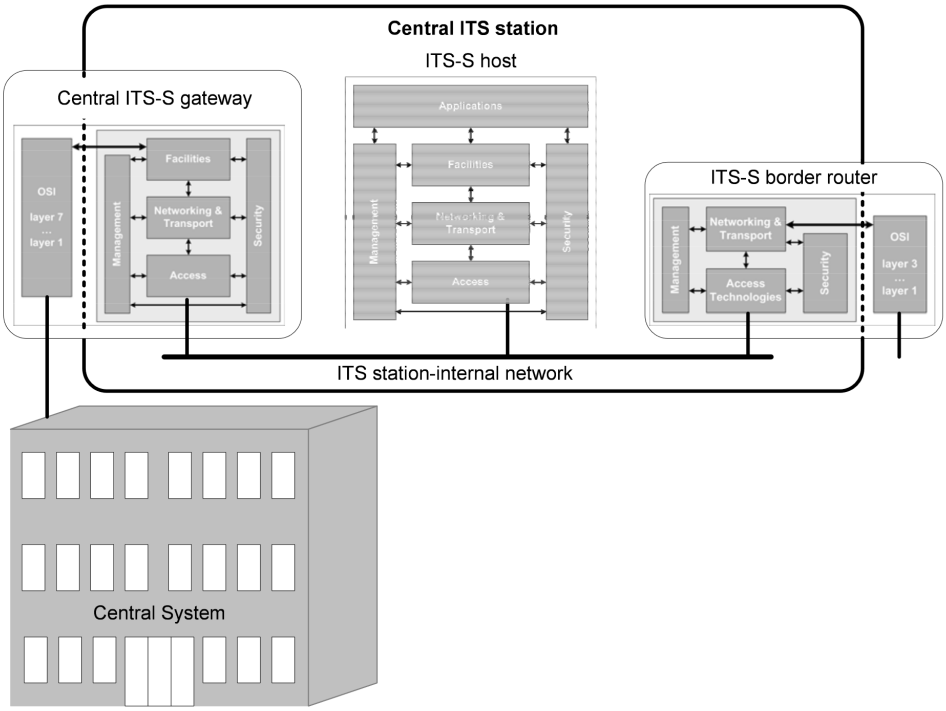


Figure 4: Central ITS station in a Central ITS sub-system [9]

The border router communicates with any other ITS system via any external network, while the gateway provides a more standardized connection.

3. Vehicle ITS sub-system:

   The Vehicle ITS sub-system represents the cars, buses, trains, trucks, airplanes, and any other vehicle or means of transportation that can communicate wirelessly in an ad hoc manner and belongs to the VANET space. This definition is very similar to the OBU definition made by the C2C-CC, but there are some important minor differences that make it more rigorous.

   This subsystem is made up of the Vehicle ITS station and the internal vehicle network, which is connected to a variety of Electronic Control Units (ECUs). ECUs represent any kind of system or application that requires a connection to the Internet or to any other vehicle. Examples of such applications are GPS, traffic control, road hazard warnings, etc.

   Like all stations, the Vehicle ITS station is made up of an ITS host with two optional ITS interceptors, nominally an ITS gateway and an ITS router. This sub-system is depicted in Figure 5.

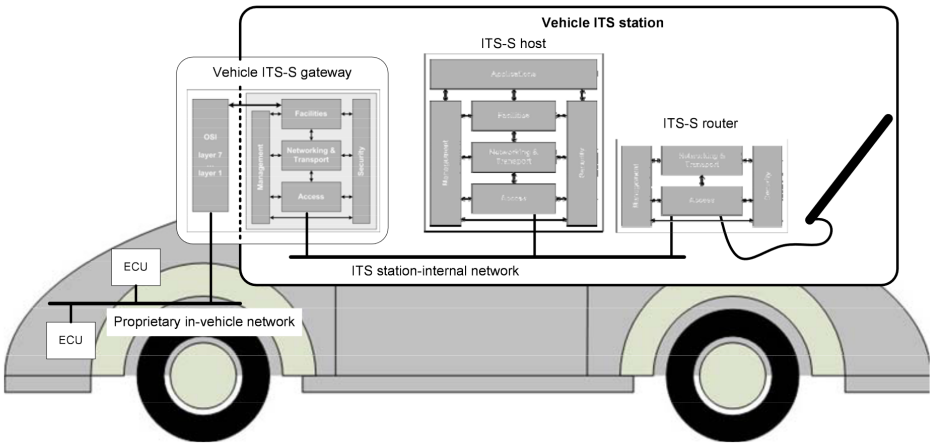


Figure 5: Vehicle ITS station in a Vehicle ITS sub-system [9]

The ITS gateway connects the internal vehicle network, which is proprietary in most cases, to the ITS station. Meanwhile, the ITS router connects to other Vehicle ITS stations and, most importantly, to the Roadside ITS station.

4. Roadside ITS sub-system:

   The final element is the Roadside ITS sub-system. It is the connection point between the vehicle ad hoc network and the rest of the Internet. Like the RSU, it is placed in locations of high vehicle volume next to roads and intersections.

   This sub-system comprises a roadside ITS station and any proprietary roadside network that may exist. It connects to any vehicle ITS station and can provide ITS applications to the vehicle users. This station is also connected to a central ITS station, being the bridge that allows the central ITS station to provide ITS applications to vehicle users.

   The roadside station is made up of an ITS host with optional ITS interceptors. These interceptors can be any of the other types of functional components beyond the ITS host. The Roadside ITS sub-system is better depicted in Figure 6.

   The ITS router connects the station to the ITS vehicle station, the border router connects to an ITS central station and the gateway connects to any existing proprietary existing networks.

2.3 Communication Domains

With the main building blocks of both architectures laid out, we can divide communications into various domains. Both the C2C-CC and ETSI have different ways to tackle this question.

2.3.1 C2C-CC approach

The C2C-CC focuses on the VANET space and divides it into three areas: the in-vehicle domain, the ad hoc domain, and the infrastructure domain. The first represents the network inside a vehicle, composed of an

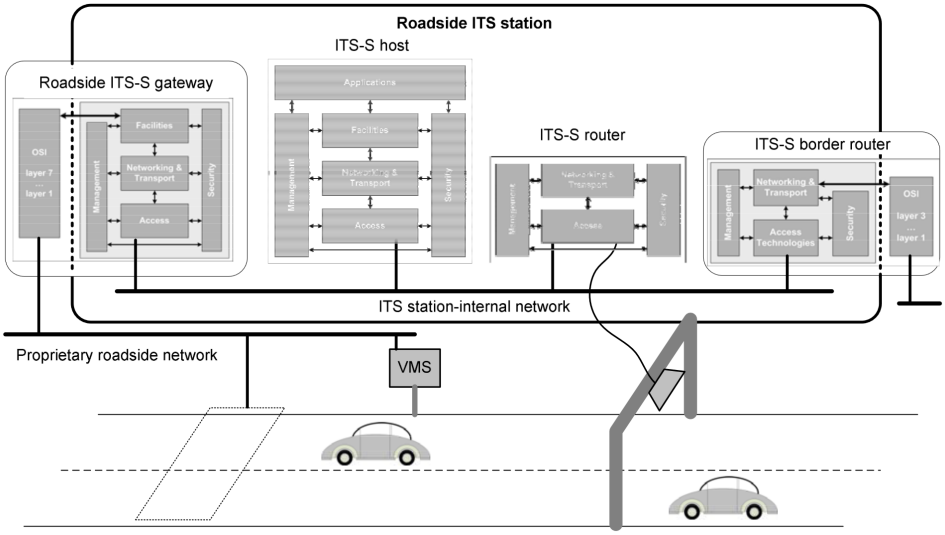


Figure 6: Roadside ITS station in a Roadside ITS sub-system [9]

OBU and the multitude of AUs connected to it. It encompasses all communications between the different AUs and the OBU. The ad hoc domain involves all ad hoc communications between different OBUs and between vehicles' OBUs with RSUs. The remaining components of the Internet that don't directly affect it, but help provide connectivity to vehicles, are included in the Infrastructure domain.

All of these domains, as well as the functional components of the C2C-CC architecture can be observed on Figure 7.

2.3.2 ETSI approach

The ETSI architecture proposes a broader categorization by establishing two domains. The first and most important is the ITS domain, since it contains all the elements and communication engaged by the ITS/Architecture of Communications in ITS (ITSC) standards. Everything else is encompassed by the generic domain, including everything in the rest of the Internet that might interact and communicate with the ITS domain.

2.4 Communication categories

In addition to communication domains, most authors use a classification based on communication types. This communication-oriented view of architecture aims to classify the multitude of types of communication that can occur between all the different entities that exist.

Different categories have emerged and evolved throughout the years as they have been used by most of the relevant researchers in the field. It is therefore difficult to find an origin for these concepts, and the following are most commonly used terms.

1. Intra-Vehicle communication This term encompasses all communications that occur inside the vehicle between different vehicle components.

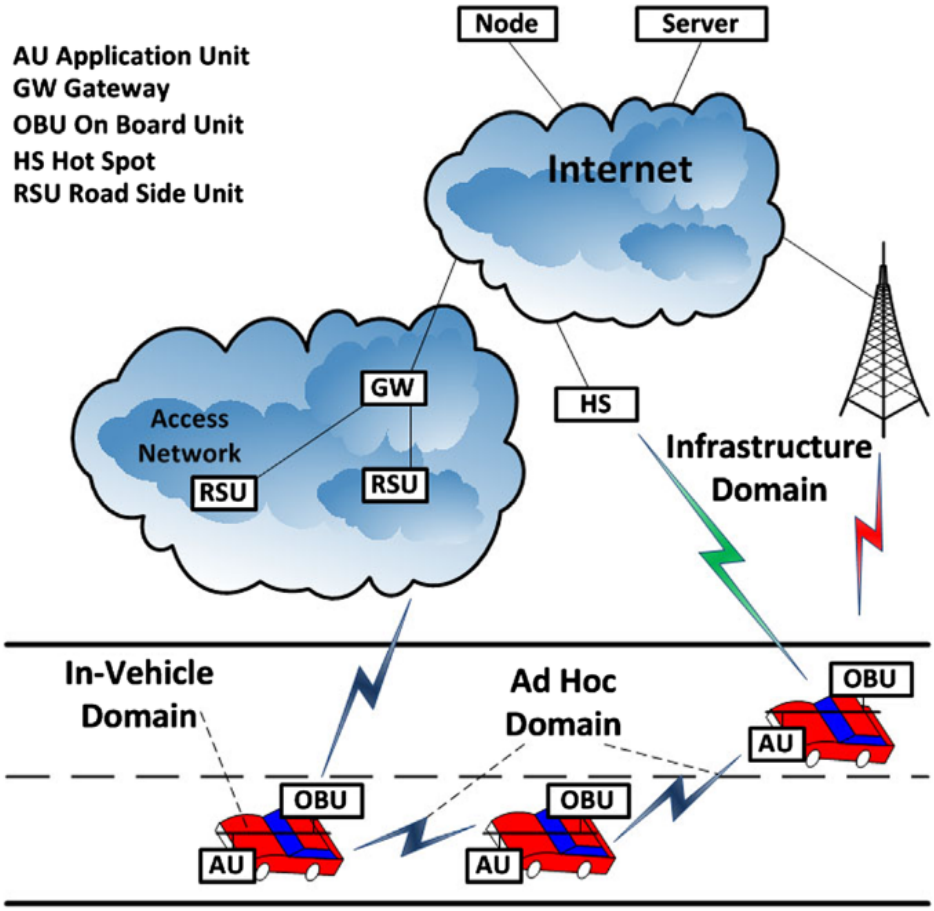


Figure 7: Communication domains in VANET as categorized by the C2C-CC [3]

2. Vehicle to Vehicle communication (V2V) communication V2V communication refers to the ad hoc communication between vehicles.

3. Vehicle to Infrastructure communication (V2I) communication V2I communication refers to ad hoc communication between vehicles and roadside infrastructure. These communications dont encompass all messages that get exchanged between vehicles and the roadside infrastructure, and only include messages whose source and destination are a vehicle and a roadside station.

4. Vehicle to Everything communication (V2X) The last type of communication is the most encompassing. V2X communication includes all communication that can occur in the VANET space between a vehicle and anything else. It is generally used to refer to the previous two types of communication.

2.5 VANET architecture

The architecture of an ITS host can be visualized on Figure 8. This section will dissect this architecture layer by layer in order to explain the functionalities and capabilities expected from it. The last layer, called Applications, will not be described as it represent ITS applications that use the services provided by the rest of the stack to connect one or more applications together and provide services to users[9].

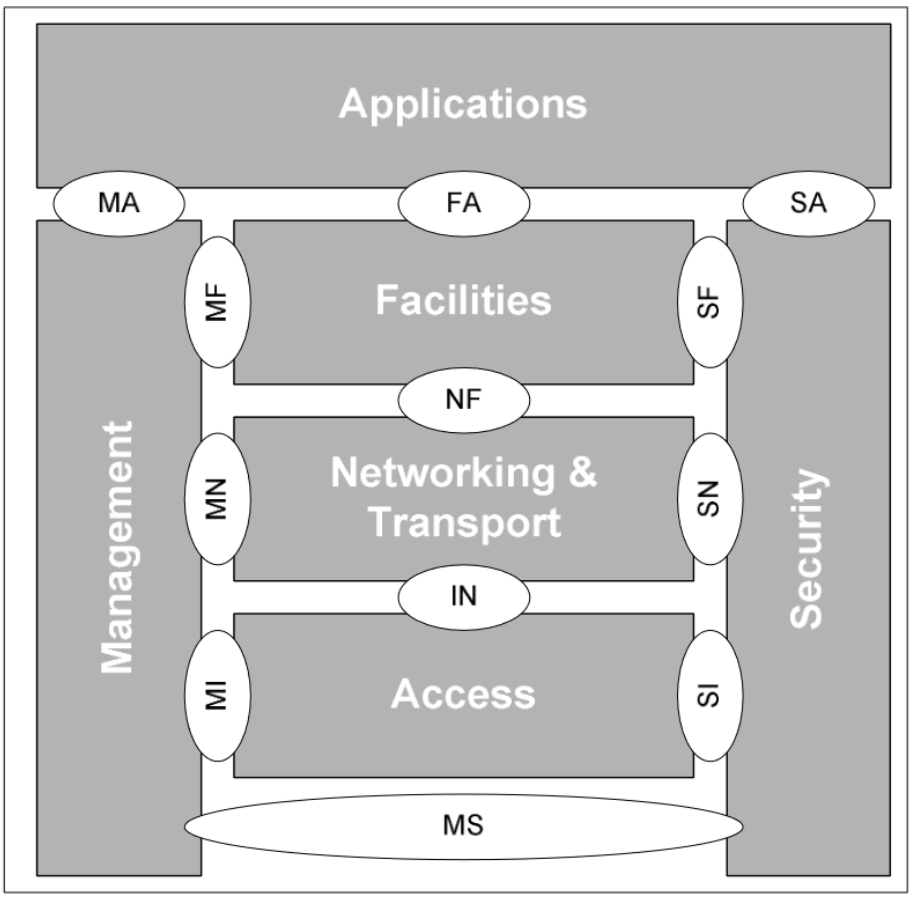


Figure 8: ITS station reference architecture [9]

The functionalities described in every layer are not necessarily function to be implemented in every instance of the architecture, as it depends on the specific implementation of the ITS station[9].

2.5.1 Access Layer

The Access Layer, which is illustrated in the architecture of an ITS host in Figure 8, corresponds to the first two layers of the OSI model, the Physical (PHY) Layer and the Data Link (MAC) Layer[10].

Among all the existing Access Layer technologies, the best suited to meet the necessary requirements for use in VANETs were the existing wireless access technologies[3]. These technologies ranged from long range signaling technologies such as Microwave and WiMAX to short range technologies such as Infrared or Bluetooth[11].

Over the years, most of these technologies have been studied and tested as possible solutions for use in VANET communications, and in most cases they were deemed unsuitable for the VANET environment. For instance, short-range communication protocols such as the examples above were discarded due to lack of range, throughput, and reliability and as a result, medium and long range communications took center stage.

While unable to fully address the demanding scenarios of VANETs, a few of these technologies showed

promise as possible solutions. Over the years since VANET research began, new standards and protocols have been developed based on these existing technologies, focusing on solving the problems posed by the characteristics of VANETs. In addition, these technologies themselves have evolved to meet the high data rates required by today's Internet.

Today, the IEEE 802.11 WiFi and Cellular technologies are considered as the two primary solutions for VANETs worldwide.

2.5.1.1 IEEE-based technologies

The Institute of Electrical and Electronics Engineers (IEEE) is an American organization dedicated to promoting innovation and technological excellence for the benefit of humanity. Founded in 1963, it is the world's largest professional society of engineers, scientists, and other technical professionals. IEEEs primary areas of contribution are the electrical, electronic, and computing fields[12].

The IEEE 802.11 family of standards, an Access layer technology, was considered a promising solution for VANETs from the start. Not only would the existing 802.11 standards be cheaper to adopt due to being already established technologies, but WiFi also already met many ITS requirements due to its compatibility with mobile environments[13].

Despite these significant advantages, the existing IEEE 802.11 standards were not able to meet all the requirements imposed by the unique characteristics of VANETs, necessitating the creation of a new variant that would be better suited for such scenarios. Thus, 802.11p was created as an adaptation of the existing 802.11 standards. Given its American origin and contribution to the development of V2X communication technologies, it is important to mention that IEEE 802.11p was conceived in the context of Wireless Access in Vehicular Environments (WAVE)[14]. The EU, while initially open to many different access technologies, eventually converged on a IEEE 802.11p based solution dubbed ITS-G5.

IEEE's main motivation behind the development of IEEE 802.11p was to enable effective communication capable of handling the rapidly changing environments of VANETs[14], while making the minimum necessary changes to the IEEE 802.11 PHY layer. Modifying the MAC layer is akin to a software update, while a PHY level amendment would require the design of an entirely new wireless airlink technology[14], which would be expensive and time consuming.

With this in mind, the IEEE began work on a variant of the 802.11 standard that would be feasible for V2X, capable of operating at speeds up to 200 km/h and ranges up to 1 km[2]. Experimental work began with the full deck of 802.11 technologies[6], but soon narrowed down to IEEE 802.11a because it operates at 5 GHz, which is closest to 5.9 GHz, the desired frequency for ITS operations in the US. This made it easier to configure devices to operate at the desired frequency[14].

IEEE 802.11p uses orthogonal frequency division multiplexing. The 802.11 family of standards offers three channel bandwidths of 5, 10, and 20 MHz, and while 802.11a uses the full 20 MHz bandwidth, the 10 MHz bandwidth was chosen for ITS scenarios. This is achieved either by halving the clock/sampling rate or by simply doubling all the standard orthogonal frequency division multiplexing timing parameters[13].

Reducing the channel bandwidth was done in an effort to increase the root mean square delay

spread[6]. Root mean square delay spread measures the time difference in seconds between the first and last signal components. These components represent different versions of the same transmitted signal, with the first to arrive coming from the shortest path which is the light of sight and the remaining coming from reflections and other interactions with the environment.

The standard 20MHz guard used by 11a proved sufficient to stop intersymbol interference between a radio and itself, so measures had to be taken to reduce the interference caused by multipath delays and by the Doppler effect. Halving channels width was the most simple and sensible solution to this problem[14]. Beyond reducing the signal bandwidth, the data throughput ranges were also reduced to 3 to 27 Mb/s instead of the original 6 to 54 Mb/s[6].

With the goal of enabling effective communications that can cope with rapidly changing environments, 802.11p communications needed to get faster in order to better utilize the sometimes narrow windows available for communication. Such a feat demanded a reduction in the overhead required before actual data transmission, which was achieved by simplifying the Basic Service Set (BSS) operations present in 802.11a[14].

The BSS represents a group of stations that are wirelessly connected to the same access point. It is created by an access point, and any device requesting to join it can exchange information with it after proper authorization. A BSS variant for ad hoc environments exists, called Independent Basic Service Set (IBSS), which works without the need for infrastructure. However, it also proved to be insufficient to deal with the peculiarities of VANETs.

As a solution, IEEE 802.11p uses an ad hoc mode called Out of Context BSS (OCB). OCB simplifies setup operations compared to its counterparts in other 802.11 standards by eliminating management procedures such as channel scanning, authentication, and association. This means that 802.11p has no setup time allowing stations to communicate with each other directly and immediately[15].

Removing all of these processes makes the network less secure. However, these security vulnerabilities are addressed by other standards in the ITS domain.

In Europe, ETSI created a solution for the access layer called ITS-G5. It not only defines the technologies and protocols to be used in communications, but also includes the frequency allocated exclusively for V2V and V2I communications for the whole of the EU.[16] ITS-G5 uses the existing 802.11p standards created for the American WAVE, adapting it for the European region.

In the US, the FCC was responsible for the allocation of the frequency from 5.850 to 5.925 in 1999. In 2003, the FCC divided the American band into seven non-overlapping 10 MHz channels with a 5 MHz unused band at the lower end. These channels were numbered from 172 to 184. This division also allows for operations in the 20 MHz channels 175 and 181, which are the overlap of two 10 MHz channels[17].

In the EU, the Electronic Communications Committee (ECC) is responsible for spectrum regulation and the European Commission is responsible for enforcing the regulated spectrum in all member states. The ECC is made up of radio and telecommunications regulatory authorities from all member countries[17][16].

The spectrum allocation for ITS-G5 began in 2005, with a recommendation from ETSI to the ECC. In its TR 102 492-1[18], ETSI recommended the allocation of 30 MHz in the 5,875 GHz to 5,905 GHz

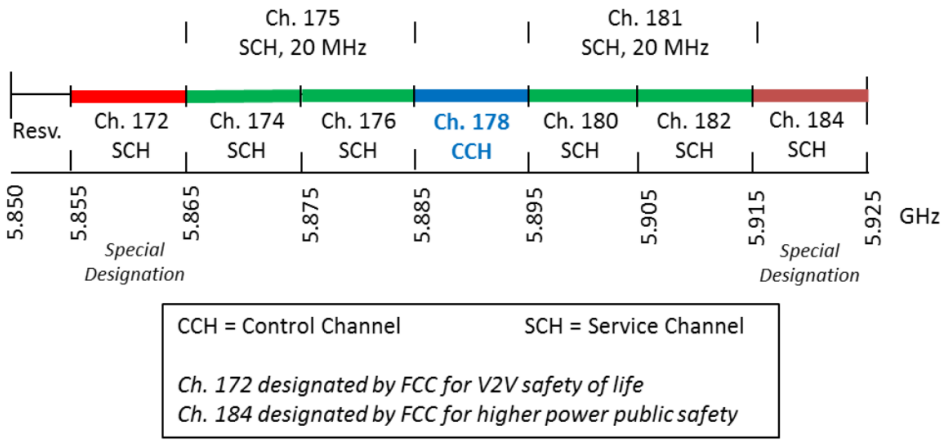


Figure 9: Channels allocated in the US by FCC for ITS [17]

band for safety applications, which would align with the US control channel frequency of 5,885 GHz to 5,895 GHz. This recommendation also expected the allocation of a future 20 MHz band from 5,905 GHz to 5,925 GHz for future ITS extensions[17][16].

ETSI based this recommendation on the allocation in the US frequency band, and also took into account the 5.8GHz toll collection band used in EU countries[17][16].

In 2008, the ECC accepted this recommendation and allocated the requested frequency range plus another 20 MHz frequency band from from 9,855GHz to 9.875GHz intended to be used by non-safety applications[17][16]. All of the spectrum involved for present and future ITS operations can be easily observer in Figure 10.

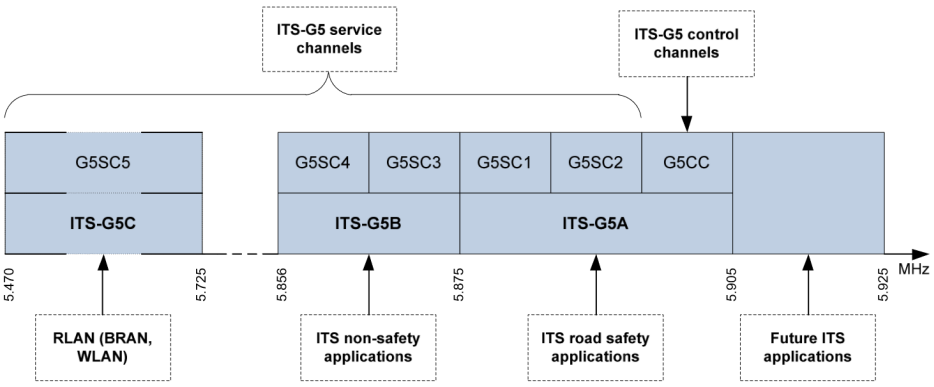


Figure 10: European ITS channel allocation [19]

Even though the American spectrum was taken into consideration, in the end the control channels of both the EU and US solutions were not in the same frequency, with the European channel being 10 MHz higher. This is not a total loss, as the same hardware can still be used in both countries requiring just a software change to work[17][16].

The different allocated frequencies have different standardized transmission power limits based on use cases and interferences on adjacent bands and on the more important control bands[15]. The specific restrictions for each 10 MHz channel can be observed in figure 11.

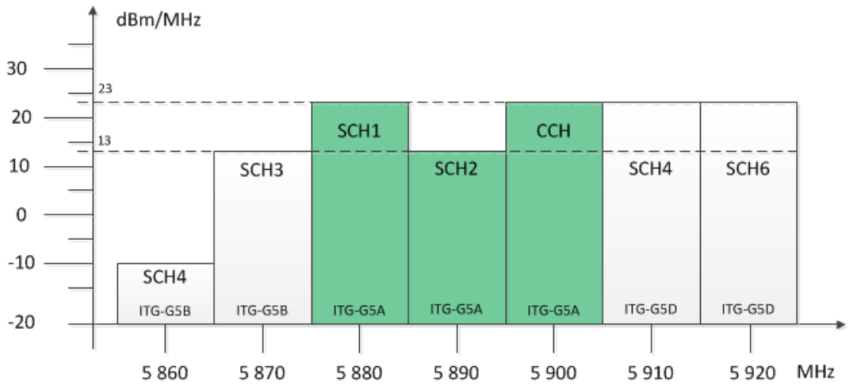


Figure 11: Power spectral limits on each ITS channel [17]

In recent years, the IEEE began work on IEEE 802.11bd, a successor to the 802.11p standard, which was approved in October 2023[20]. As a new standard, it is expected to take several years before it completely replaces 11p, and most automakers will continue to release cars with 802.11p for the foreseeable future.

This new version promises twice the throughput and longer range, while ensuring interoperability, coexistence, backward compatibility and fairness with existing OCB terminals. In addition, it operates beyond the 5.9 GHz band by utilizing the 60 GHz band.

2.5.1.2 Cellular-based technologies

Cellular systems have been used since the 1970s to transmit data over long distances via radio waves[11]. The 3rd Generation Partnership Project (3GPP) is an international consortium established in 1980 with the goal of developing technical specifications and technical reports for 3G mobile systems and is now the leading global reference for mobile standards and is responsible for the development of LTE and 5G[21].

Although most work on VANETs has been based on 802.11p, Cellular V2X (C-V2X) has gained renewed support from academia and industry as this technology has matured[22]. Rival performance to the dominant IEEE 802.11p has led to Cellular technologies being considered by some organizations as a replacement for existing IEEE standards, so its status as the second most important VANET technology is not surprising.

In September 2016, the 5G Automotive Association (5GAA) was established as a global, cross-industry organization of companies from the automotive, technology, and telecommunications industries with its main objective to promote the use of cellular 3GPP standards in ITS scenarios[23].

Most researchers dismissed this new technology because its shortcomings made it seem inadequate compared to the strengths of 802.11. C-V2X's main drawback is its centralized nature. Cellular technology relies on a centralized infrastructure, which introduces latency by forcing all data to pass through a base station.

In addition, the large coverage area of cellular antennas can also pose an issue, as the coverage area of an antenna is typically larger than the zone of relevance of safety messages. This makes broadcast an

inadequate solution, as many vehicles would receive warnings not intended for them. Multicast can be introduced in an attempt to reduce this problem, but it introduces new delays from the overhead required to create these multicast groups[22].

On the other hand, Cellular technologies have several technical and economic advantages for their application in V2X communications. On the technical side, cellular technologies provide wide coverage, support high vehicle speeds, support a large number of connections to a single cell tower and can deliver high data rates. Economically, the wide use of these technologies allows the reuse of already deployed hardware for use in V2X[22].

These benefits, along with the renewed support from the industry created from 5GAA, motivated the 3GPP to begin studying the feasibility of LTE technology for supporting V2X communications[22]. In 2019, 3GPP began work on C-V2X efforts with Release 14, which made great strides in reducing existing drawbacks.

In order to work as a wireless access technology capable of serving all VANET test cases, this technology needed to ditch the necessity of using infrastructure and become ad hoc. Therefore, Release 14 established a new mode of communication, called direct communication.[24] This resulted in LTE and 5G supporting two relevant interfaces for communication in VANETs, the Uu interface and the PC5 interface.

The Uu interface is used for long range communication with cellular infrastructure in the commercial cellular spectrum. It uses existing LTE's large coverage to provide vehicles with all kinds of services[24].

The direct communication mode, also referred to as "Mode 4", utilizes the short range PC5 interface in the ITS 5.9GHz band and allows for direct exchange of information between vehicles without passing through a cell tower.

ETSI initially considered Cellular technologies as possible solutions, and at that time included 2G and 3G as possible access technologies in the initial ITS station reference architecture. As stated earlier, ETSI centralized the Access Layer of its architecture on the 802.11p-based ITS-G5. Recently, however, reflecting on the efforts of 3GPP, 5GAA, and ITS implementation in other countries like China, ETSI made amendments to existing standards in order to achieve compatibility with C-V2X technologies[24]. This indicates that in the C-V2X architecture, the layers above the Access Layer consists of the pre-established standards of different countries, demonstrating significant technological compatibility.

2.5.2 Networking & Transport Layers

The Networking and Transport Layer, as implied by its name, corresponds to the third and fourth layers of the OSI model.

Layer 3 algorithms commonly deployed in traditional networks are unsuitable for use in VANETs[6], and even existing MANETs algorithms have proven to be inadequate for use in VANETs[4]. The characteristics of VANETs, as described in section 2.1, present several unique challenges not only to existing Layer 3 algorithms, but also to Layer 4 protocols, the most important of which are high node mobility and variable node density.

The high mobility of nodes leads to frequent topology partitions, which results in highly unstable routes. Therefore, pre-determining routes in these conditions is often irrelevant and extremely complicated. Additionally, the algorithm must operate under conditions of both extreme congestion and isolation due to variable node density, further increasing its complexity.

Scholars have recognized the adoption of broadcast as the primary communication mode as a great solution to mitigate interference in high congestion scenarios. Nevertheless, this approach alone falls short of the desired outcome. For instance, in case of a crash, it is essential to rapidly disseminate security messages as the number of affected vehicles can rapidly rise. However, if every vehicle broadcasts simultaneously, it will lead to channel congestion, making it more difficult for the event to spread[6]. Therefore, novel approaches are required to curb message duplicates.

Although the challenges presented by these aspects of VANETs affect algorithm reliability, researchers have leveraged other characteristics of VANETs to develop novel solutions to the aforementioned problems. Besides the lack of power constraints, the predictable mobility of nodes allows algorithms to perform more effective link selection, which facilitates network management and opens opportunities to optimize the flow of information, ultimately improving routing protocols.

In Europe, researchers at ETSI developed new algorithms and defined new protocols in an attempt to find an adequate solution to the aforementioned challenges while taking advantage of VANETs newfound opportunities. As part of its architecture, ETSI introduced a new Layer 3 protocol called GeoNetworking[25][26][27][28][29][30], a new Layer 4 protocol called Basic Transport Protocol (BTP)[29] and a sublayer 3 extension called GeoNetworking-IPv6 (GN6)[30].

GeoNetworking is an ad hoc routing protocol that was developed solely for the transmission of safety related messages and therefore it provides the ability to forward packets without the need to exchange any signaling messages beforehand.

The GeoNetworking protocol uses the geographical coordinates of nodes as their address and utilizes location-based data to help make packet forwarding decisions.

By using a device's geographic location as its address, this protocol enables packets to be sent to all nodes within a specific geographical area. Nodes can effortlessly broadcast messages to an entire geometrically shaped area without congesting the entire network. This approach proves to be more efficient than broadcasting because it curbs congestion by minimizing transmissions to unintended destinations. Moreover, it makes the packet relevance area independent of the sender's range.

This protocol was built and optimized for multi-hop communication with geo-addressing, providing more technical features in application support than the alternative in the US. These capabilities come to a cost to protocol complexity and message overhead[31].

The GeoNetworking protocol was designed to be integrated with the BTP protocol. BTP is a transport layer protocol that is similar in function to User Datagram Protocol (UDP), functioning as a connectionless protocol[15].

ETSI has established the GeoNetworking extension GN6 as an alternative to routing packets through BTP. By using the GN6 sub-layer, Internet Protocol version 6 (IPv6) packets can be transmitted over the GeoNetworking protocol without the need to modify the IPv6 protocol[15].

2.5.3 Facilities Layer

The Facilities Layer encompasses layers 5, 6, and 7 of the OSI model, and its standardization defines application-specific functionalities[31]. The development of Facility Layer messages is the responsibility of European institutions such as ETSI, European Committee for Standardization (CEN), and International Organization for Standardization (ISO).

All the messages defined by European standard makers serve safety purposes, and therefore run over the GeoNetworking protocol[31]. Multiple different messages have been defined over the years[15], which makes it difficult to list them all. However, CAMs and DENMs are universally acknowledged as the most significant in the context of ITS.

A CAM[32] is a periodic safety message that contains vital status information about the originating vehicle, with the main goal of enabling other vehicles to take appropriate preemptive measures to avoid potentially dangerous situations[3].

This objective is accomplished by exchanging data, including speed, location, direction, and additional non-safety application data with nearby ITS stations, allowing vehicles to monitor each other's movements.[31].

CAMs begin transmitting as soon as the vehicle enters a safety-relevant context, which is considered to be anytime the vehicle is in operation.[15] The transmission rate of CAMs is subject to specific rules, including both maximum and minimum transmission times between CAMs, relevant changes in position, direction, or velocity, and congestion in the wireless channel[15].

CAM fields are shown in figure 12. It includes an obligatory ITS PDU header, Basic container, and High frequency container, along with optional Low frequency and Special vehicle containers.

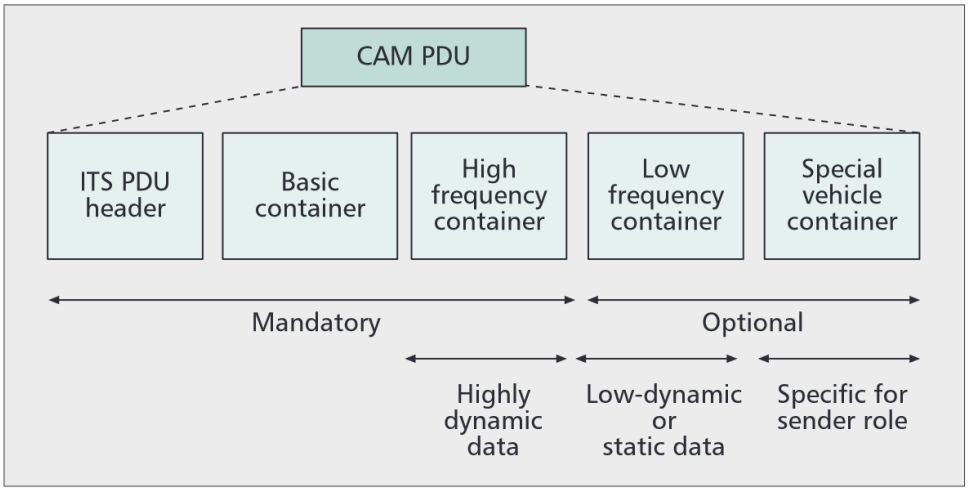


Figure 12: CAM structure [15]

This structure allows for a high degree of flexibility in message format, allowing messages to adapt more effectively to their environment, thereby minimizing congestion on wireless channels[15].

A DENM[33] is an event-driven safety message that can be triggered by an ITS station in the event that hazardous conditions are detected. ITS stations are capable of detecting a wide range of events and

this message type is employed to describe such events to other ITS applications.

DENMs serve the purpose of warning ITS applications to a detected event within a designated geographical area[15]. This type of messages are only relevant in a specific location and therefore are only disseminated in that specific geographical area. These geographical areas are the ones defined by the GeoNetworking protocol.

As an event-triggered message, DENMs are considered high-priority messages, as ensuring a quick delivery is crucial to diminishing the consequences of the events that triggered their generation[3].

Throughout the lifespan of the DENM, a number of techniques are employed to ensure the dissemination of the message in its relevant area. DENMs are repeated, generally at a lower frequency than CAMs, with the intent to allow vehicles entering the relevant area to receive said information. Similarly, if the originator ceases to transmit the DENM message for any reason, another ITS station can replace the originator and continue to transmit the message. DENM messages can also be canceled by the ITS station that created them[15].

DENM fields can be observed on figure 13. The ITS PDU header and the management container are mandatory, while the situation, location and a la carte container are all optional. These message fields mainly contain information about the relevance area of the message, the type of event and the time in which the message remains relevant.[3]

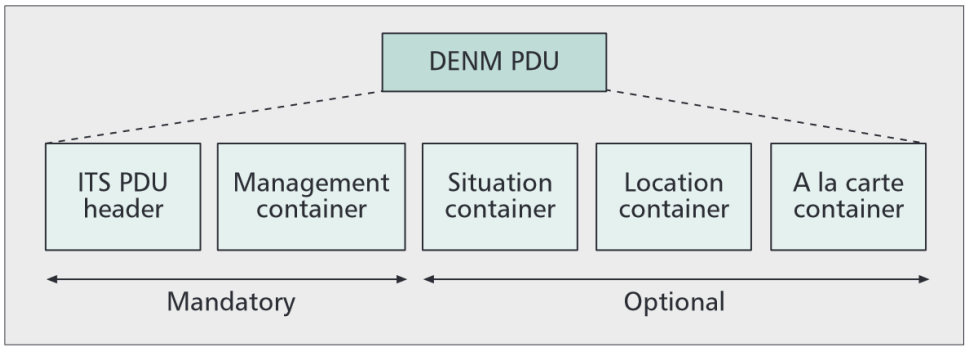


Figure 13: DENM structure [15]

2.5.4 Management Entity

Network management is a critical component of network maintenance as it ensures that a network operates as intended. The unique challenges presented by VANETs contribute to a significantly more unstable network environment than usual, making management even more essential. With this motivation in mind, ETSI incorporated a management entity into its architecture 14.

The ITS management entity is responsible for both configuring and operating its ITS station, while also overseeing cross-layer information exchange between multiple layers. It contains interfaces to every other component in the ITS station and a management information base. [27]

Decentralized congestion control is a cross-layer ITS functionality that is coordinated by the management entity and is one of its most important responsibilities. Its main purpose is to control congestion

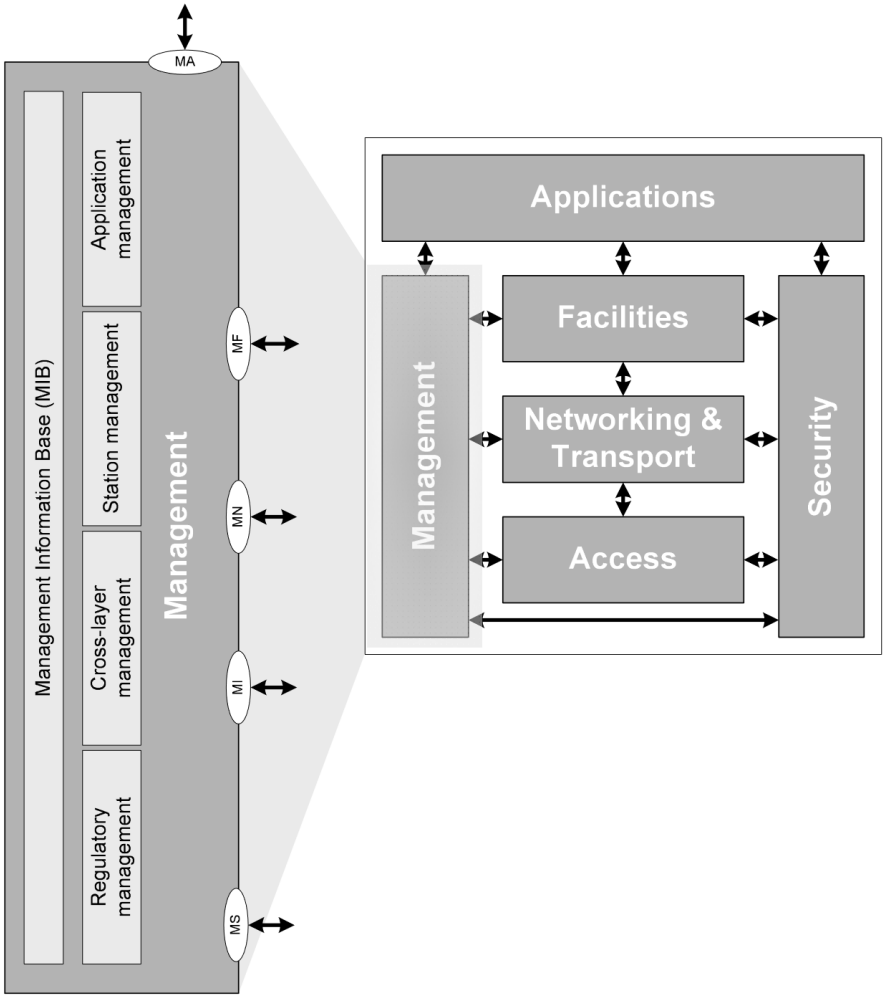


Figure 14: ITSC management entity as part of the ITS station reference architecture [9]

in the channel by managing the amount of messages exchanged, the transmission power and any other useful parameter. The changes to these parameters, being orchestrated by the management entity, are made based on various information extracted from different layers. [15]

2.5.5 Security Entity

Security in VANETs has been one of the biggest concerns and one of the biggest obstacles to its deployment. It is crucial to protect the ITS domain from malicious attacks and network abuse, and as such it has been a high priority for researchers and developers to address security threats prior to deployment. Vehicle messages can contain a large amount of sensitive information, such as vehicle trajectory and location data. This information can be used to deduce the driver's identity, activities, habits, and so on. This type of information must not only be kept private under EU law, but could also be used by bad actors for extortion.[4] [34] Attackers could also exploit safety messages for their own benefit or to the detriment of others. For instance, greedy drivers could broadcast false traffic alerts to reduce traffic on their own routes. In a more extreme case, robbers or terrorists could abuse traffic alerts to clog roads and thereby

delay emergency vehicles. [34] With this motivation in mind, researchers have laid out several security requirements VANETs must meet. The following list contains the most important ones, based on the works of [35] [34]:

1. Authentication: this security requirement ensures that a recipient can identify the sender of all messages received, thereby ensuring that each message is generated by an authenticated user.

2. Non-repudiation: sometimes called auditability, it is a tricky to enforce but essential security requirement. Non-repudiation ensures that once a message is sent, the sender can't deny ownership of the message. In VANETs, this requirement is essential for identifying compromised users.

3. Integrity: this security requirement ensures that the message remains unchanged during transmission.

4. Confidentiality: a security requirement for any type of network, and VANET is no different. Some messages contain important information and therefore should only be accessible to the sender and receiver to prevent eavesdropping.

5. Availability: one of the most important concerns in VANETs, this requirement seeks to ensure the availability of the wireless channel, as a message that is delayed by seconds becomes useless.

6. Access control: this property creates different levels of access for different entities. Access control bars users from accessing any information or sending message types they are not allowed to. Distinguishing multiple levels of access allows for a higher degree of network control and is essential to stop known bad actors from exploiting network dynamics.

7. Privacy: Privacy is the ability of users to hide their personal information from the rest of network users. Implementing mechanisms to protect the privacy of all drivers is a top priority to ensure driver privacy, with the main goal to provide location privacy. Anonymity is the process of hiding one's identity, which is extremely important to achieve privacy.

8. Data verification: this property is essential to avoid false messaging as it allows all messages to be tested by their time relevance. This is necessary to avoid replay attacks in the network.

9. Physical Security: as vehicles are a widely spread technology that will be distributed indiscriminately, it is important to implement hardware security in order to avoid tampering and compromising of the vehicle.

Authentication and privacy are desirable properties of VANETs but ensuring anonymity while enforcing network liability in VANETs is a contradictory property in securing vehicular networks. This comes from the necessity to protect drivers' privacy while being able to track down attackers. [14] [34] Another important consideration to take is that security measures can create performance problems, as they add overhead time in communications and can significantly degrade message quality. [6] ETSI has taken these security concerns into consideration and has incorporated security requirements into its architecture15. These

considerations were taken on a layer by layer approach, resulting in security services being implemented at every layer and between multiple layers, which necessitated the creation of a dedicated entity for security. The ETSI ITS host architecture envisions a Security Entity, which is responsible for providing security services, as seen on figure 25. The security entity can also be considered as a specific part of the management entity. [36]

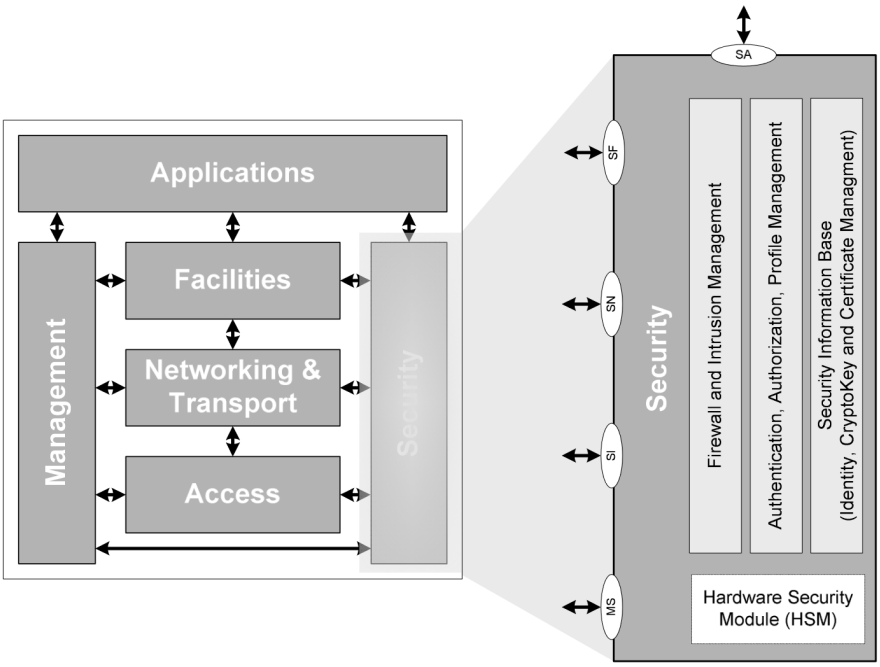


Figure 15: ITSC security entity as part of the ITS station reference architecture [9]

The Security Entity provides a plethora of services to ensure security and privacy. These include a multitude of secure messages at different layers of the communication stack, management of identities and security credentials, and other aspects relevant to secure platforms such as firewalls, security gateways, and tamper-proof hardware. [27]

ETSI developed an ITS communication system that relies on indirect trust relationships, which are built upon trusted third party certificates. It is a solution to the privacy problem and results in the implementation of a so-called authority hierarchy. This hierarchy is composed of manufacturers, enrolment authorities, authorizations authorities and the ITS station.

When a car wishes to begin communicating, it must use its canonical credentials given by the manufacturer to request valid enrolment credentials to an enrolment authority. Then, using the enrolment credentials it must request an authorization authority for authorization credentials. These last ones are the ones that will be used for communications, and as such in order to protect a driver's privacy are only valid in a time frame. After these expire, the ITS host must request new authorization credentials to the authorization authority. From this example, we can observe that the enrollment authority validates that the vehicle has a valid ITS station and that the authorization authority uses the authorizations given by the enrollment authority to allow the ITS station access to the ITS domain and to utilize a specific type of

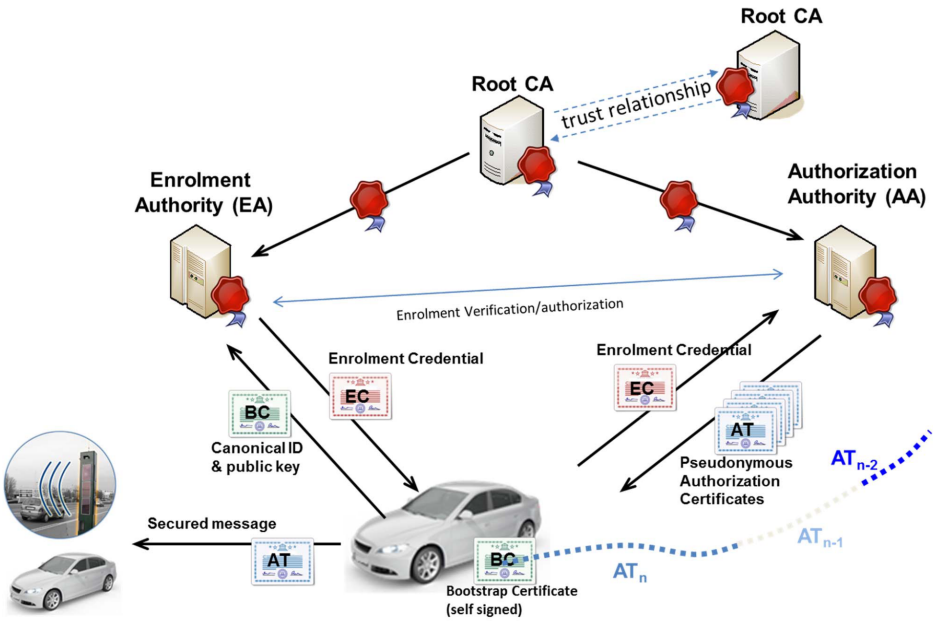


Figure 16: ITS Security Certificate Management System [37]

applications, service or privilege. This process can be observed on Figure 16. [38]

2.6 Applications of VANET

The motivation behind VANET research and development is to provide wireless services to both drivers and vehicles. The goal of these service applications is to improve driving safety, passenger comfort, and traffic efficiency. Hence, VANET applications can be classified into safety and non-safety applications according to their intended goal. Safety applications are considered the main driving force behind the development of VANETs[4] as the main goal of these types of applications is to decrease both road fatalities and road pollution[3]. Safety applications can be divided into two categories: Cooperative road safety and Cooperative traffic efficiency. Certain applications have the potential to improve both of them. Cooperative road safety applications harness the wireless communication capabilities of vehicles to provide useful information to the vehicle and driver, with the ultimate goal of mitigating the likelihood and severity of accidents. Therefore, any application intended to enhance the safety of individuals is classified as an Cooperative road safety application. Examples of such applications are notifications for upcoming hazardous locations and approaching emergency vehicles. Cooperative traffic efficiency applications aim to make road operations more efficient. These efforts can both greatly reduce unnecessary carbon emissions and save the time of drivers. Examples of such applications are off street parking information and green light optimal speed advisory. VANETs could also become a crucial step in the journey to fully autonomous vehicles, by exploiting expected advanced cooperation systems to exchange sensor information and status information among vehicles. These future applications also fall under the cooperative traffic efficiency umbrella. Some of these envisioned safety VANET applications require a certain percentage of road-wide deployment to become useful[2]. Therefore, ETSI has defined a basic set of applications to

be deployed as ITS systems mature, with the aim of deploying them simultaneously at that time. These applications are commonly referred to as Day 1 applications and aim to provide societal and economic benefits to both the private and public road transportation sectors. Remaining safety applications have been grouped into Day 1.5 deployments, with the goal of improving and extending Day 1 applications. These applications can be further divided into bundles, which can be viewed onI. The remaining applications fall under the category of non-safety applications. Such applications, also known as co-operative local services and global internet services, are those designed to enhance the comfort of drivers and passengers by enabling access to internet services from their vehicles[3]. Based on this, any application that provides value-added services is considered non-safety applications[6]. All types of entertainment and information-based applications, such as music, movies, podcasts, online games, or instant messaging platforms, are examples of the applications covered under this category. Essentially, any application that is hosted on the World Wide Web and is accessible via the IP stack falls into this category. Non-safety applications should not interfere with safety applications, and thus they use different physical media and protocols[2]. In detail, non-security applications are typically delivered using IPv6 over C-V2X, while safety applications exclusively use GeoNetworking.

2.7 Future trends and challenges in VANET research

Predicting a date for when the full potential of the VANET technology will be unleashed is incredibly difficult but it is a case of when, not if, as the benefits of VANETs remain attractive and a lot of work has already been done.

Current and future research seeks to update current technologies in use, such as the aforementioned development of 802.11bd 2.5.1. Additionally, efforts are being made to augment this technology with other technologies such as SDN, Edge Computing, and AI to take it to the next level[39].

The deployment of VANET infrastructure in Europe is currently underway, with projects such as TEN-T. In line with the European Green Deal and the renewed focus on the climate crisis, VANETs are expected to help reduce traffic emissions by increasing traffic efficiency. Besides, the goal to reduce traffic fatalities to 0 by 2050 remains a top priority[40]. Figure 17 provides a comprehensive representation of the plans for VANETs in the EU.

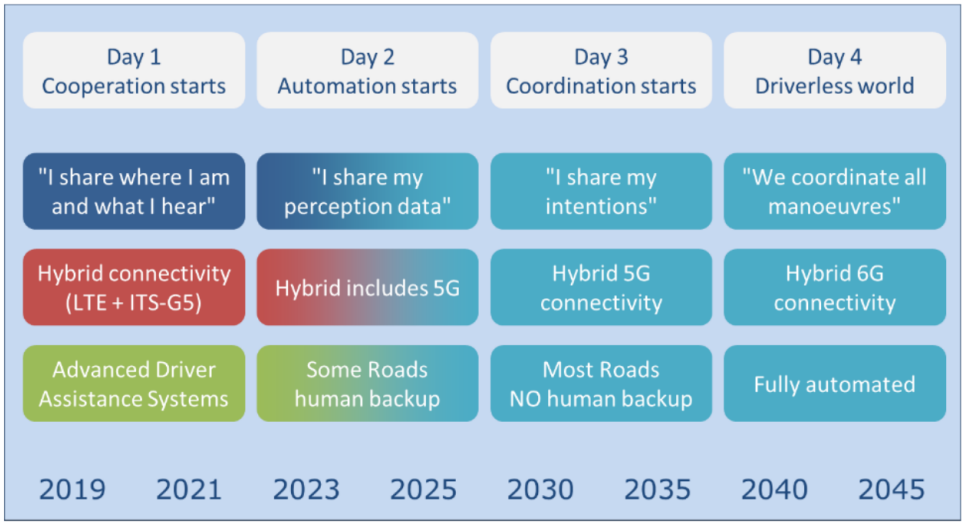


Figure 17: ITS strategy for the European Union [40]

3

Software defined networking

3.1 SDN definition

3.2 Motivation behind Software defined networking (SDN)

3.3 SDN architecture

3.3.0.1 Data plane

3.3.0.2 southbound API

3.3.0.3 control plane

3.3.0.4 Eastbound and Westbound APIs

3.3.0.5 Northbound API

3.3.0.6 Management plane

Bibliography

[1] J. M. Lourenço. *The NOVAthesis LaTeX Template User's Manual*. NOVA University Lisbon. 2021. url: https://github.com/joaomlourenco/novathesis/raw/main/template.pdf (cit. on p. ii).

[2] J. Jakubiak and Y. Koucheryavy. "State of the Art and Research Challenges for VANETs". In: *2008 5th IEEE Consumer Communications and Networking Conference*. 2008 5th IEEE Consumer Communications and Networking Conference. ISSN: 2331-9860. 2008-01, pp. 912–916. doi: 10.1109/ccnc08.2007.212 (cit. on pp. 3, 5, 14, 25, 26).

[3] S. Al-Sultan et al. "A comprehensive survey on vehicular Ad Hoc network". In: *Journal of Network and Computer Applications* 37 (2014-01-01), pp. 380–392. issn: 1084-8045. doi: 10.1016/j.jnca.2013.02.036. url: https://www.sciencedirect.com/science/article/pii/S108480451300074X (visited on 2022-11-02) (cit. on pp. 3, 5, 12, 13, 20, 21, 25, 26).

[4] W. Liang et al. "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends". In: *International Journal of Distributed Sensor Networks* 11.8 (2015-08-01), p. 745303. issn: 1550-1477, 1550-1477. doi: 10.1155/2015/745303. url: http://journals.sagepub.com/doi/10.1155/2015/745303 (visited on 2023-02-22) (cit. on pp. 3, 5, 18, 22, 25).

[5] H. Dinh Thai et al. "Applications of Repeated Games in Wireless Networks: A Survey". In: *IEEE Communications Surveys & Tutorials* 17 (2015-01-11). doi: 10.1109/COMST.2015.2445789 (cit. on p. 4).

[6] Y. Toor et al. "Vehicle Ad Hoc networks: applications and related technical issues". In: *IEEE Communications Surveys & Tutorials* 10.3 (2008). Conference Name: IEEE Communications Surveys & Tutorials, pp. 74–88. issn: 1553-877X. doi: 10.1109/COMST.2008.4625806 (cit. on pp. 4–6, 14, 15, 18, 19, 23, 26).

[7] S. M. Corson and J. P. Macker. *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*. Request for Comments RFC 2501. Num Pages: 12. Internet Engineering Task Force, 1999-01. doi: 10.17487/RFC2501. url: https://datatracker.ietf.org/doc/rfc2501 (visited on 2023-09-28) (cit. on p. 6).

[8] C2C-CC. *CAR 2 CAR Communication Consortium Manifesto - Overview of the C2C-CC System*. 2007-08-28. url: https://www.car-2-car.org/fileadmin/documents/General_Documents/C2C-CC_Manifesto_Aug_2007.pdf (visited on 2023-04-23) (cit. on p. 6).

[9] ETSI. *Intelligent Transport Systems (ITS); Communications Architecture*. 2010-09. url: https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf (visited on 2023-04-27) (cit. on pp. 7–13, 22, 24).

[10] ETSI. *Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*. 2020-01. url: https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf (visited on 2023-11-08) (cit. on p. 13).

[11] M. S. Anwer and C. Guy. "A Survey of VANET Technologies". In: (2014) (cit. on pp. 13, 17).

[12] *History of IEEE*. url: https://www.ieee.org/about/ieee-history.html (visited on 2023-11-14) (cit. on p. 14).

[13] R. Schwarz. "Intelligent Transportation Systems Using IEEE 802.11p". In: (2019-02-14) (cit. on p. 14).

[14] D. Jiang and L. Delgrossi. "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments". In: IEEE Vehicular Technology Conference. 2008-06-14, pp. 2036–2040. doi: 10.1109/VETECS.2008.458 (cit. on pp. 14, 15, 23).

[15] A. Festag. "Cooperative intelligent transport systems standards in europe". In: *IEEE Communications Magazine* 52.12 (2014-12). Conference Name: IEEE Communications Magazine, pp. 166–172. issn: 1558-1896. doi: 10.1109/MCOM.2014.6979970 (cit. on pp. 15, 16, 19–22).

[16] N. Asselin-Miller et al. "Study on the Deployment of C-ITS in Europe: Final Report". In: 1 (2016-05-02) (cit. on pp. 15, 16, 36).

[17] J. Härri and J. Kenney. "Multi-Channel Operations, Coexistence and Spectrum Sharing for Vehicular Communications". In: ed. by C. Campolo, A. Molinaro, and R. Scopigno. Book Title: Vehicular ad hoc Networks. Cham: Springer International Publishing, 2015, pp. 193–218. isbn: 978-3-319-15496-1 978-3-319-15497-8. doi: 10.1007/978-3-319-15497-8_7. url: https://link.springer.com/10.1007/978-3-319-15497-8_7 (visited on 2023-10-05) (cit. on pp. 15–17).

[18] ETSI. *Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 1: Technical characteristics for pan-European harmonized communications equipment operating in the 5 GHz frequency range and intended for critical road-safety applications; System Reference Document*. 2005-06. url: https://www.etsi.org/deliver/etsi_tr/102400_102499/10249201/01.01.01_60/tr_10249201v010101p.pdf (visited on 2023-11-17) (cit. on p. 15).

[19] Ş. ŞORIGA. "ITS-G5 AND MOBILE WIMAX PERFORMANCE IN VEHICLE-TO-INFRASTRUCTURE COMMUNICATIONS". In: *ISSN 1454-234x* (2012). url: https://www.scientificbulletin.upb.ro/rev_docs_arhiva/full4d5_755707.pdf (visited on 2023-10-16) (cit. on p. 16).

[20] "IEEE Standard for Information Technology–Telecommunications 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 5: Enhancements for Next Generation V2X". In: *IEEE Std 802.11bd-2022 (Amendment to IEEE Std 802.11-2020 as amended by IEEE Std 802.11ax-2021, IEEE Std 802.11ay-2021, IEEE Std 802.11ba-2021, IEEE Std 802.11-2020/Cor 1-2022, and IEEE Std 802.11az-2022)* (2023-03). Conference Name: IEEE Std 802.11bd-2022 (Amendment to IEEE Std 802.11-2020 as amended by IEEE Std 802.11ax-2021, IEEE Std 802.11ay-2021, IEEE Std 802.11ba-2021, IEEE Std 802.11-2020/Cor 1-2022, and IEEE Std 802.11az-2022), pp. 1–144. doi: 10.1109/IEEESTD.2023.10063942. url: https://ieeexplore.ieee.org/document/10063942 (visited on 2023-10-25) (cit. on p. 17).

[21] *3GPP – The Mobile Broadband Standard*. 3GPP. url: https://www.3gpp.org/ (visited on 2023-11-16) (cit. on p. 17).

[22] S. Gyawali et al. "Challenges and Solutions for Cellular Based V2X Communications". In: *IEEE Communications Surveys & Tutorials* 23.1 (2021), pp. 222–255. issn: 1553-877X, 2373-745X. doi: 10.1109/COMST.2020.3029723. url: https://ieeexplore.ieee.org/document/9217500/ (visited on 2023-10-16) (cit. on pp. 17, 18).

[23] *5GAA*. 5GAA. url: https://5gaa.org/ (visited on 2023-11-16) (cit. on p. 17).

[24] R. Weber, J. Misener, and V. Park. "C-V2X - A Communication Technology for Cooperative, Connected and Automated Mobility". In: *Mobile Communication - Technologies and Applications; 24. ITG-Symposium*. Mobile Communication - Technologies and Applications; 24. ITG-Symposium. 2019-05, pp. 1–6. url: https://ieeexplore.ieee.org/abstract/document/8731783 (visited on 2023-10-23) (cit. on p. 18).

[25] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements*. 2014-04. url: https://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf (visited on 2023-11-27) (cit. on p. 19).

[26] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios*. 2013-11. url: https://www.etsi.org/deliver/etsi_en/302600_302699/30263602/01.02.01_60/en_30263602v010201p.pdf (visited on 2023-11-27) (cit. on p. 19).

[27] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture*. 2014-12. url: https://www.etsi.org/deliver/etsi_en/302600_302699/30263603/01.02.01_60/en_30263603v010201p.pdf (visited on 2023-10-06) (cit. on pp. 19, 21, 24).

[28] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality*. 2020-01. url: https://www.etsi.org/deliver/etsi_en/302600_302699/3026360401/01.04.01_60/en_3026360401v010401p.pdf (visited on 2023-11-27) (cit. on p. 19).

[29] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol*. 2019-05. url: https://www.etsi.org/deliver/etsi_en/302600_302699/3026360501/02.02.01_60/en_3026360501v020201p.pdf (visited on 2023-11-27) (cit. on p. 19).

[30] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols*. 2014-05. url: https://www.etsi.org/deliver/etsi_en/302600_302699/3026360601/01.02.01_60/en_3026360601v010201p.pdf (visited on 2023-11-27) (cit. on p. 19).

[31] A. Festag. "Standards for vehicular communication—from IEEE 802.11p to 5G". In: *e & i Elektrotechnik und Informationstechnik* 132.7 (2015-11-01), pp. 409–416. issn: 1613-7620. doi: 10.1007/s00502-015-0343-0. url: https://doi.org/10.1007/s00502-015-0343-0 (visited on 2023-10-16) (cit. on pp. 19, 20).

[32] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*. 2019-04. url: https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf (visited on 2023-11-27) (cit. on p. 20).

[33] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*. 2019-04. url: https://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.03.01_60/en_30263703v010301p.pdf (visited on 2023-11-27) (cit. on p. 20).

[34] A. K. Malhi, S. Batra, and H. S. Pannu. "Security of vehicular ad-hoc networks: A comprehensive survey". In: *Computers & Security* 89 (2020-02), p. 101664. issn: 01674048. doi: 10.1016/j.cose.2019.101664. url: https://linkinghub.elsevier.com/retrieve/pii/S0167404818312872 (visited on 2023-11-28) (cit. on pp. 22, 23).

[35] H. Hasrouny et al. "VANet security challenges and solutions: A survey". In: *Vehicular Communications* 7 (2017-01-01), pp. 7–20. issn: 2214-2096. doi: 10.1016/j.vehcom.2017.01.002. url: https://www.sciencedirect.com/science/article/pii/S2214209616301231 (visited on 2023-12-15) (cit. on p. 23).

[36] ETSI. *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*. 2010-09. url: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf (visited on 2023-11-28) (cit. on p. 24).

[37] ETSI. *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*. 2018-04. url: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf (visited on 2023-12-05) (cit. on p. 25).

[38] ETSI. *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2*. 2021-07. url: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf (visited on 2023-11-28) (cit. on p. 25).

[39] M. J. N. Mahi et al. "A Review on VANET Research: Perspective of Recent Emerging Technologies". In: *IEEE Access* 10 (2022). Conference Name: IEEE Access, pp. 65760–65783. issn: 2169-3536. doi: 10.1109/ACCESS.2022.3183605. url: https://ieeexplore.ieee.org/abstract/document/9797696 (visited on 2023-12-19) (cit. on p. 26).

[40] M. Lu et al. "Pan-European deployment of C-ITS: the way forward". In: (2019) (cit. on pp. 26, 27).

A

Appendix 1 Lorem Ipsum

I

Bundles of services

Service bundle	C-ITS Services	Rationale
Bundle 1 Day 1, V2V, ITS-G5	• Emergency brake light • Emergency vehicle approaching • Slow or stationary vehicle(s) • Traffic jam ahead warning • Hazardous location notification	• Day 1 safety-based V2V services based on ITS-G5 communication, likely to be deployed to vehicles supported by US legislation
Bundle 2 Day 1, V2I, mainly applicable to motorways	• In-vehicle signage • In-vehicle speed limits • Probe vehicle data • Shockwave damping • Road works warning • Weather conditions	• Day 1 V2I, services that deliver most benefit to motorways. Some services listed here may also be applicable to other road types
Bundle 3 Day 1, V2I, mainly applicable to urban areas	• Green Light Optimal Speed Advisory (GLOSA) / Time To Green (TTG) • Signal violation/Intersection safety • Traffic signal priority request by designated vehicles	• Day 1 V2I, services expected to only be applicable in urban areas. Therefore, these services are in a separate bundle to those in Bundle 2
Bundle 4 Day 1.5, V2I, Parking Information	• Off street parking information • On street parking management and information • Park & Ride information • Information on AFV fuelling & charging stations	• C-ITS services intended to provide information regarding parking (and refuelling) to drivers
Bundle 5 Day 1.5, V2I, Traffic and other information	• Traffic information and smart routing	• C-ITS services intended to provide traffic information to drivers
Bundle 6 Day 1.5, Freight specific services	• Loading zone management • Zone access control management	• Zone management services
Bundle 7 Day 1.5, V2X (mainly applicable to urban areas), likely to be ITS-G5	• Vulnerable road user protection (pedestrians and cyclists)	• V2X service expected to be post day 1. Communication method is likely to be ITS-G5. Main benefits are likely to be seen in urban areas.
Bundle 8 Day 1.5, V2V, likely to be ITS-G5	• Cooperative collision risk warning • Motorcycle approaching indication	• Post day 1 V2V services that are likely to be based on ITSG5. As for Day 1 services, V2V and V2I services are in separate service bundles.
Bundle 9 Day 1.5, V2I	• Wrong way driving	• Post day 1 V2I service. As for Day 1 services, V2V and V2I services are in separate service bundles.

Table 1: C-ITS service bundles for scenario building[16]