DEVELOPMENT AND ANALYSIS OF A VANET NETWORK

Adrian Corral
Master of Science Thesis in Electrical Engineering

Development and Analysis of a VANET Network
Adrian Corral

Supervisors:

Ted Johansson
ISY, Linköping University

Anders Skärpe
Syntronic AB

Examiner:

Mark Vesterbacka
ISY, Linköping University

Division of Integrated Circuits and Systems
Department of Electrical Engineering
Linköping University
SE-581 83 Linköping, Sweden

Copyright 2017 Adrian Corral
# Contents

1 Introduction ........................................................................ 15
   1.1 Motivation ........................................................................... 15
   1.2 Purpose ............................................................................. 16
   1.3 Problem statements ............................................................ 18
   1.4 Limitations .......................................................................... 18
   1.5 Thesis outline ....................................................................... 18

2 Theory .................................................................................. 21
   2.1 Vehicular Ad Hoc Network (VANET) ........................................... 21
   2.2 Wireless Local Area Network (WLAN) .......................................... 22
   2.3 Ad Hoc Network .................................................................... 23
   2.4 OSI Model ........................................................................... 23
   2.5 IPv6 .................................................................................. 25
   2.6 UDP ................................................................................. 26
   2.7 Routing in VANET .................................................................. 27
      2.7.1 Topology-based protocols .................................................. 27
      2.7.2 Position-based protocols .................................................. 27
      2.7.3 Cluster-based protocols .................................................. 27
      2.7.4 GeoCast-based protocols ............................................... 28
      2.7.5 Broadcast-based protocols .............................................. 28
   2.8 Distributed Vehicular Broadcast Protocol (DV-CAST) ................. 28
   2.9 Dedicated short range communications (DSRC) ....................... 30
      2.9.1 Wireless Access in Vehicular Environments (WAVE) .......... 31
      2.9.2 European Telecommunications Standards Institute,
Intelligent Transport Systems operating in 5 GHz band (ETSI ITS G5)...............................................................................................................32

3 Method........................................................................................................35

3.1 Introduction.............................................................................................35

3.2 Tools..........................................................................................................35

3.2.1 Software...............................................................................................35

3.2.2 Hardware..............................................................................................36

3.3 Implementation........................................................................................37

3.3.1 Configuration of the device.................................................................38

3.3.2 Software Implementation.................................................................38

3.3.3 Messages types....................................................................................41

3.3.4 Broadcast Protocol.............................................................................43

3.4 Evaluation.................................................................................................51

4 Results........................................................................................................53

4.1 Real deployment results...........................................................................53

4.1.1 Packet loss, latency and jitter against distance.................................54

4.1.2 Broadcast success ratio against number of vehicles.........................56

4.1.3 Broadcast success ratio against packets per second........................57

4.1.4 Broadcast success ratio against speed............................................58

4.2 Performance of broadcast protocol.......................................................58

4.3 Comparison with theoretical studies.....................................................61

4.3.1 Traffic Scenario I...............................................................................61

4.3.2 Traffic Scenario II...............................................................................63

5 Discussion....................................................................................................67
5.1 Results........................................................................................................67
5.2 Method........................................................................................................69
5.3 The work in a wider perspective.................................................................71

6 Conclusions....................................................................................................73
6.1 Obtained results.........................................................................................73
6.2 Objectives attainment...............................................................................74
6.3 Future research and future perspectives..................................................77

Appendix A......................................................................................................79

7 Time plan.......................................................................................................79
Appendix B.......................................................................................................81

8 Interface for Road Side Units.................................................................81

Bibliography.....................................................................................................83
### List of Figures

- Figure 2.4 1: OSI model layer stack .......................................................... 24
- Figure 2.8 1: Decision Tree for DV-CAST Protocol .................................. 29
- Figure 2.9 1: WAVE protocol stack .......................................................... 31
- Figure 2.9 2: ETSI ITS G5 Protocol Stack .................................................. 32
- Figure 3.3 1: WAVE standard taking into account to develop the application .......................................................................................................................... 37
- Figure 3.3 2: Configuration of Raspberry Pi 3 network interfaces to work in ad hoc mode with IPv6 ................................................................. 38
- Figure 3.3 3: Pseudocode of the implemented software ............................ 39
- Figure 3.3 4: Resource usage of the running software ............................... 40
- Figure 3.3 5: Example of serial communication with GPS information .... 41
- Figure 3.3 6: Protocol when receiving a warning message ....................... 42
- Figure 3.3 7: Broadcast success rate comparison between DV-CAST and simple broadcast ......................................................................................... 44
- Figure 3.3 8: Distance reached comparison between DV-CAST protocol and simple broadcast ................................................................. 45
- Figure 3.3 9: DV-CAST Decision Tree ......................................................... 46
- Figure 3.3 10: Broadcast statistics of the probabilistic models ................ 47
- Figure 3.3 11: Proposed Scheme Decision Tree When Receiving an Alert Message .................................................................................................. 49
- Figure 3.3 12: Broadcast protocol when sending ....................................... 50
- Figure 4.1 1: Packet loss against distance in urban scenarios ................. 55
- Figure 4.1 2: Latency against distance in urban scenarios ....................... 55
- Figure 4.1 3: Broadcast success ratio against number of vehicles .......... 56
- Figure 4.1 4: Broadcast success ratio against packets per second .......... 57
- Figure 4.1 5: Broadcast performance against speed ................................ 58
- Figure 4.2 1: Broadcast protocol working in traffic jam scenario .......... 59
- Figure 4.2 2: Performance of Broadcast protocol .................................... 60
- Figure 4.3 1: Average packet loss probability against number of vehicles .................................................................................................................. 62
- Figure 4.3 2: Average packet loss probability against average distance .. 63
- Figure 4.3 3: Broadcasting performance against car density ................. 65
- Figure 4.3 4: Delay against car density ....................................................... 65
- Figure 6.3 1: DSRC implementation perspectives. Source: Navigant Research ........................................................................................................... 78
List of Tables

Table 4.1: Real deployment parameters...............................................................54
Table 4.2: Traffic Scenario I parameters.............................................................61
Table 4.3: Traffic Scenario II Parameters.............................................................64
# Notation

<table>
<thead>
<tr>
<th>Abbreviation/Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>Acknowledge</td>
</tr>
<tr>
<td>CCH</td>
<td>Control Channel</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communications</td>
</tr>
<tr>
<td>DV-CAST</td>
<td>Distributed Vehicular Broadcast Protocol</td>
</tr>
<tr>
<td>ETSI ITS G5</td>
<td>European Telecommunications Standards Institute, Intelligent Transport Systems operating in 5 GHz band</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>ISY</td>
<td>Institutionen för systemteknik</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport Systems</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MANET</td>
<td>Mobile Ad Hoc Network</td>
</tr>
<tr>
<td>OBU</td>
<td>On Board Units</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>Abbreviation/ Acronym</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>RSU</td>
<td>Road Side Units</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to Vehicle</td>
</tr>
<tr>
<td>VANET</td>
<td>Vehicular Ad Hoc Network</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access in Vehicular Environments</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
</tbody>
</table>
This chapter will describe the context in which the project is being done as well as justify the existence of it. Secondly, the purpose and problem statements are described. Finally, the structure of the report is defined, in order to ease the comprehension of it.

1.1 Motivation

The main motivation of this project is to study and develop technology related to autonomous driving. Autonomous vehicles are now being developed and they suppose the future in transportation. Therefore, it is interesting for technology and software companies to be participative and keep in track with the new advances in this field.

For the moment, most of the technology that is used in autonomous driving is self centred in the vehicle. That means that several radars and sensors are implemented in the vehicle in order to obtain information from the surroundings by itself and actuate in accordance to this information.

On the other hand, information can be obtained from other users and elements on the road. That is, the information can be sent and received using wireless communication. All of vehicles create a network where the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are performed. These networks are known as Vehicular Ad Hoc Networks (VANET).

VANET are meant to share the information between vehicles in order to improve the possibilities of autonomous driving. They establish a new source of information of the surroundings so the vehicles do not depend only on themselves. Furthermore, they provide a quicker medium for communicating since the messages can travel faster jumping between vehicles rather than
having to use an external antenna to transmit the information. Hence, VANET networks can be useful also in terms of security and alert transmission.

For the moment, VANET networks are mostly theoretical and the research is focused on simulations and hypothetical situations. This project will perform a further study in communication between vehicles focusing on a real deployment in order to understand the actual possibilities of these networks.

1.2 Purpose

The main objective of this project is to develop a VANET network and perform a real deployment of the network. Secondly, the network has to be analysed and it is necessary to measure the characteristics of the network. Finally, the results of the analysis have to be compared to theoretical studies and simulations of the state of the art in order to prove the correct method during the development of the project and to give validity to the work done.

By the end of the project several milestones need to be achieved. First of all, a fully working prototype will be developed, including the software implementation and the hardware configuration and firmware required for the deployment. Also, the results from the analysis collecting the measures of packet loss, latency, jitter, and scalability in changing scenarios where the speed, the distance, and the number of users in the network can be variable.

Individual objectives related to the global objective are also defined for this thesis as well as parameters that allow to determine the fulfilment of these individual objectives.

1st objective: Generality

The configured platform as well as the implemented software need to be of general purpose. That is, the software and hardware cannot be developed for only one specific situation, but they need to be dynamic and capable to perform in different scenarios. In the end, a generic platform and software need to be developed in order to be able to perform in every traffic scenario that is required.

2nd objective: Requirements accomplishment

The device has to cover correctly the basic requirements for a vehicular network. That is, it has to support the transmission of basic information as well as warnings and alerts that could disrupt the normal activity of the traffic. Basic information would include speed, direction, and location. This would allow the vehicles to be able to map their surroundings. Furthermore, the network needs to perform in highly mobile and dynamic scenarios, where devices can join or leave the network continuously.
Also, the performance needs to be good enough when it comes to execution time and communication time. The platform needs to be able to transmit and receive in time and the hardware needs to provide a channel good enough to be reliable and fast. The network needs to cover all the steps from gathering information to transmitting and processing it.

Finally the network needs to be reliable and secure. That includes not only to be able to perform in time and with effectiveness, but also to make sure that it transmits the correct information and that that fake information cannot be communicated in the network as well as it cannot be flooded with a lot of messages from one sender. The network is supposed to be an additional help to driving, providing extra information. Therefore, it is preferable to transmit no information rather than transmit the wrong information.

3\textsuperscript{rd} objective: Validity

The proposed model for hardware configuration, firmware and software needs to be validated and needs to assure that the obtained results can be trustful. Therefore the analysis of the real deployment has to offer quantitative and coherent results that need to be compared with theoretical studies and simulations.

The thesis will accomplish a variety of different tests and measurements in real scenarios with changing conditions. This will allow to compare the theoretical work of the state of the art with an actual deployment, and will help to understand possible limitations, strengths or weaknesses of the possible real deployment. Therefore this thesis seeks to provide useful information that would help to understand the real behaviour of a network of this characteristics.

4\textsuperscript{th} objective: Correct development of the network activity

The network activity has to be carried out during long periods of time without major failures that would provoke the wrong performance of the network. Therefore the network has to be formed, maintained and the information has to be communicated and processed during long periods of time to be proved functional and secure.

5\textsuperscript{th} objective: Robustness

It is necessary to generate a robust network that can support minor failures or unexpected situations. That is, if a situation out of the expected performance occurs, the network needs to adapt and continue with the usual performance whenever it is possible. It is also necessary that the network is secure and reliable in every situation.

6\textsuperscript{th} objective: Scalability

The network needs to be scalable. That means that it has to be able to support a large number of vehicles joining the network, as well as the vehicles leaving it.
Therefore, the network needs to perform correctly in every traffic scenario no matter the traffic conditions.

1.3 Problem statements

The questions this thesis will strive to answer are:

- What are the main characteristics of a vehicular network and which requirements have to be achieved?
- What are the appropriate technologies to be used to create a vehicular communication network?
- How can these techniques and technologies be implemented in a device?
- How can a real communication network be considered valid, reliable and appropriate for an actual deployment?

1.4 Limitations

Vehicular Ad Hoc Networks is a wide concept that considers from direct communication between vehicles and elements on the road to the transmission of the information to an external base station and to the internet. It also considers the processing of the global information as well as the specific processing that each vehicle needs to do. This thesis will only consider the communication and processing regarding the vehicles and the roadside elements.

Regarding this matter, both software and hardware implementation will be considered for this thesis. The choice of hardware technology is another limitation since in order to have hardware for this project it has to be commercially available and it has to fulfil cost issues. Therefore Raspberry Pi 3 has been chosen as the basic hardware to use in this project. Further upgrades to the project can consider to update or improve the hardware. On the other hand, there are no limitations in terms of software since only C language will be used as well as open source tools.

1.5 Thesis outline

Chapter 1: Introduction

The project base is briefly introduced. The purpose and objectives that are sought to achieve, problem statements and limitations are also presented in this chapter. Finally, the thesis outline to ease the lecture of the document.
Chapter 2: Theory

This chapter offers a theoretical overview of the problem. It also explains different technologies and solutions that can be used to solve the problem.

Chapter 3: Method

This chapter explains which solutions were taken and how the problems were solved. It also explains the configurations of the platform as well as the software implementation that has been done. Finally, it explains why the solutions were taken and why were they needed.

Chapter 4: Result

This chapter describes the results from the different tests carried out to measure the network characteristics. It also explains the different scenarios and conditions in which each test was performed.

Chapter 5: Discussion

This chapter discusses the results obtained from the vehicular network analysis. It also compares the results to other theoretical studies and simulations of the state of the art in order to give validity to the analysis and to help to understand the characteristics of the network.

Chapter 6: Conclusion

This chapter discusses the conclusions that can be obtained from the results. Finally, future work and improvements to the system are presented.
This chapter presents a theoretical outline of the project. In first place, a general description to vehicular networks is given. Secondly, a review on the different technologies and resources used for this application and a description on why they should be used or implemented. Finally, a deeper explanation of the behaviour of the network as well as the protocols needed for its execution.

### 2.1 Vehicular Ad Hoc Network (VANET)

Vehicular Ad Hoc Networks (VANET) is the name given to the communication networks that involve data exchange between vehicles and also roadside equipment in real time [1], [2].

Originally VANET was considered an application of Mobile Ad Hoc Networks (MANET). Later on, the concept evolved and represented a field of study by itself, due to the differences between the characteristics of both networks.

VANET provides new services based on the wireless communication in order to obtain more information about the surroundings in vehicles applications. This technology, along with the use of information and communication in rail, water and air transport and navigation systems, compose the Intelligent Transport Systems (ITS).

The main applications for VANET networks correspond to safety related applications. They can provide assistance like navigation or collision avoidance, information about the neighbour vehicles such as position, direction and speed and can be used in order to inform about alerts and warnings like accidents or obstacles on the road [3]. The main characteristics of VANET are:
• They are composed mainly by vehicles which are considered as mobile nodes. Also there can exist roadside elements that can act as a support for the network. Therefore the network is highly mobile and changing.

• The number of nodes in the network is variable. Nodes can enter or leave the network, which provokes a changing and dynamic scenario. The networks needs to adapt to these changes in the number of nodes and topology of the network.

• The network has to operate in conditions of high speed and mobility. The relative speed between the vehicles can be also higher and can affect the performance of the network.

• The nodes of the VANET are considered to have infinite energy supply. That means that the devices in charge of communication and data processing can be supplied with energy from the vehicle, so power consumption is not considered to be a major problem.

• One of the main characteristics of these networks is that they have to be very secure for the user. Therefore security is considered as a special aspect of VANET networks.

• VANET also pay special attention to reliability of the communication. Low latency as well as low packet lost is sought in the network, in order to achieve a very reliable performance.

2.2 Wireless Local Area Network (WLAN)

A Wireless Local Area Network (WLAN) is a wireless network that links two or more devices and allows the communication between them using a wireless distribution method, generally radio. Most of the WLANs are based on the standard IEEE 802.11 and are known under the Wi-Fi name.

Although VANET can use any wireless technology in order to communicate, WLAN is the most promising technology for this purpose. Wi-Fi is a well-known and fully developed technology that provides a low latency and reliable communication between the devices. The standardization for VANET considers IEEE 802.11 standards as the base for the communication protocol, specifically IEEE 802.11p [4].

Other technologies that could be considered for VANET purposes are WPAN networks, particularly the standard IEEE 802.15.4, used by protocols like Zigbee that allows the creation of dynamic mesh network. Still, for the moment most of the applications for VANET consider IEEE 802.11{a,b,g,n,} for current deployments and actual applications [5] while IEEE 802.11p is treated to be the future standard and technology to use and is being tested in multiple theoretical applications and simulations [6], [7], [8].
2.3 Ad Hoc Network

An ad hoc network does not have a central controller or access point. In the ad hoc network, all devices talk to each other directly and all the nodes are seen as equal. Therefore ad hoc networks have particular characteristics that differ them from more common networks, like networks for domestic or business purposes that rely on an access point that is in charge of managing the network. These characteristics are open communication through the network, self healing, quick distribution of information and the possibility of using routing protocols. Furthermore, no infrastructure is needed for ad hoc networks, and they support mobile nodes as well as variable number of nodes, which make this type of networks appropriate for dynamic scenarios.

The use of ad hoc networks in VANET is a must. Ad hoc technology provides the capacity to adapt to changing topologies and supports that nodes go in and out of the network without loosing the features of the network or decreasing its performance.

2.4 OSI Model

The Open System Interconnection (OSI) model characterizes the communication functions of a system into a layer architecture. It is a conceptual model that acts as reference for communication protocols. Originally the model considered a stack of seven layers to define the networking framework. Upper layers of the OSI model are focused on network services with a more software approach while lower layers of the OSI model focus to hardware oriented functions like routing or addressing. Each layer serves the layer above it and it is at the same time served by the layer below.

The first layer corresponds to the physical layer (PHY) and performs the transmission and reception of bit streams over the physical medium, as well as defines the electrical and physical specifications of the data connection. The second later is the data link layer, also described as MAC layer. It is responsible of how devices gain access to the medium as well as identifying the network layer protocols. These first two layers are defined by the standard IEEE 802. For example the standard IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi and IEEE 802.15.4 Zigbee.

Network layer provides the tools like addressing, routing and traffic control, which are essential to structuring and managing the network. An example of addressing related to the network layer are the protocols IPv4 and IPv6. This last one can also help with the routing of the network.

Transport layer is in charge of the transmission of data segments or datagrams in the network. Some tasks in charge of this layer are segmentation, acknowledgement and multiplexing. There are different protocols in the level of transport layer depending on the application. The first of these protocols is
Transmission Control Protocol (TCP). TCP provides a close communication between two members communicating by an IP network and makes sure that the data sent by a client is received correctly by a server. It is one of the main protocols of the Internet protocol suite. The second of these protocols is User Datagram Protocol (UDP). UDP provides with an open communication where several devices can communicate at the same time. The messages, referred as datagrams, are sent and received using connectionless transmission models with a minimum of protocol mechanism.

A key difference between TCP and UDP is that TCP uses a port to make a close communication between two nodes of the network, while UDP uses port numbers for addressing, then several nodes can have an open communication using the same port number. Then, TCP performs a unicast communication between two end points while UDP can perform both unicast and broadcast communication. Furthermore, TCP offers a more reliable communication due to the fact that it makes sure that the segments are well delivered and received, while in UDP error checking is not performed, which gives a quicker application since dropping packages is preferable to waiting for delayed packages in terms of time efficiency.

<table>
<thead>
<tr>
<th>Data</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network Process to Application</td>
</tr>
<tr>
<td>Data</td>
<td>Presentation</td>
</tr>
<tr>
<td></td>
<td>Data representation and Encryption</td>
</tr>
<tr>
<td>Data</td>
<td>Session</td>
</tr>
<tr>
<td></td>
<td>Interhost communication</td>
</tr>
<tr>
<td>Segments</td>
<td>Transport</td>
</tr>
<tr>
<td></td>
<td>End-to-End connections and Reliability</td>
</tr>
<tr>
<td>Packets</td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Path Determination and IP (logical addressing)</td>
</tr>
<tr>
<td>Frames</td>
<td>Data Link</td>
</tr>
<tr>
<td></td>
<td>MAC and LLC (Physical Addressing)</td>
</tr>
<tr>
<td>Bits</td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Media, Signal and Binary Transmission</td>
</tr>
</tbody>
</table>

*Figure 2.4.1: OSI model layer stack*
Finally, session, presentation and application layers are in charge of translation of the data between the networking service and the application, that is the final user for the communication. These layers include also features like high level Application Programming Interfaces (APIs) and remote file access. Application layer includes protocols like Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP).

2.5 IPv6

Internet Protocol version 6 (IPv6) is the newest version of Internet Protocol (IP) and the successor of Internet Protocol version 4 (IPv4). It is the communication protocol in charge of providing and identification and location system for the nodes on networks. That is, it allows address allocation methods and the creation of routing tables that facilitate route aggregation across the network or the internet.

Apart from address auto-configuration and route maintenance, there are many other features of this protocol like unicast, multicast, IP security (IPsec), simplification of header structure, mobile IP or IPv6 to IPv4 transition mechanisms.

IPv6 is located in the network layer of the OSI model. The addresses of IPv6 is formed by 8 groups of four hexadecimal digits. That makes a total of 128 bit address space. This address method can support $2^{40}$ subnets. On the other side, IPv4 uses a 32 bit address that can only lead to $2^{32}$ addresses. IPv4 is limited then and cannot support all the private networks that the internet required. Therefore IPv6 is meant to replace IPv4.

An example of IPv4 and IPv6 address would be:

**IPv4:** 192.255.255.1

**IPv6:** fe80::0000:0000:0000:2017:b5d3:8355:2948

The addresses are the identification that the nodes of a network need in order to receive and send messages through the network. There cannot be two nodes with the same address in the same network. There are several methods to obtain the address:

- The address can be given manually by the user that creates the network. This is not usually a valid method, due to the fact that most of the times the user that communicates in a network is different and there is no way to keep track the IP addresses that are already in use.
• The address can be obtained from tools that generate automatic addresses like avahi for Linux systems. The problem with this method is that it assigns a random address and checks if it is already in the network. Therefore it is a slow method that can lead to several problems in big networks. Also the number of addresses available for this method is limited.

• The address can be obtained from a DHCP server. The Dynamic Host Configuration Protocol (DHCP) makes sure that every node in the network has a different address assigning to each node that enters the network a IP address that is not used. This method requires a central node that acts as server while the other nodes act as clients. This is not a valid solution for dynamic and mobile networks like VANET since there cannot be a central node that manages and handles the network.

• For IPv6, the address can be obtained automatically from the MAC address of the hardware device. Each hardware device has a specific MAC address that is different from every other devices. The manufacturer makes sure that the address is unique. Therefore it can be possible to obtain an unique address also for IPv6 from the MAC address. This is the default method for most of the devices. It is also suitable for VANET networks since the vehicles can obtain an unique address without the need of external information.

2.6 UDP

User Datagram Protocol (UDP) is a transport layer protocol that allows the transmission of data, referred to as datagrams, to other host on a IP network. It is used along with the IP network layer protocol.

UDP provides with an open communication where several devices can communicate at the same time. The messages are sent and received using connectionless transmission models with a minimum of protocol mechanism.

Finally, UDP uses port numbers for addressing, then several nodes can have an open communication using the same port number. It can perform both unicast and broadcast communication. But error checking is not performed since in a broadcast communication there is no need to know who is the receiver and it cannot be expected to receive an acknowledgement from it.

UDP is the transport protocol to use in VANET. TCP cannot be used since it performs a unicast close communication between only two end devices. VANET need to use broadcast communication in order to send and collect information from every vehicle in the surroundings without knowing their addresses.
2.7 Routing in VANET

Routing is an important feature for mobile networks that are highly dynamic and changing. It is needed for route discovery in both MANET and VANET. Therefore it allows to send messages to specific nodes of the network even if they are not directly connected to the sender. This feature is usually achieved by multi-hop mechanisms. VANET adapt most of the routing protocols from MANET due to make them more suitable for increasing velocities and highly mobile nodes.

Most of the routing protocols require the use and maintenance of routing tables with the existing routes to certain nodes. There are many different protocols that can be categorised in five groups [1], [2].

2.7.1 Topology-based protocols

Topology-based protocols rely in the creation and maintenance of routes. They are classified into proactive and reactive protocols. In proactive protocols the routes are predefined so they are known before sending a message. The maintenance of the routes leads to a high network loan and bandwidth consumption.

On the other hand, in reactive protocols the route discovery takes place on demand. Then, only the route in use is maintained and traffic loan and bandwidth are saved. Two popular examples of reactive routing are Dynamic Source Routing (DSR) and Ad Hoc on Demand Distance Vector (AODV).

2.7.2 Position-based protocols

Position based protocols use geographical information to select the next hop in the network. It also used beaconing, sending small packages to advertise the nodes in the network in order to broadcast messages. The decision of forwarding the package is taken in the moment based on geographical information. Hence, the traffic loan and resources to maintain the protocol are reduced. Greedy Perimeter Stateless Routing and Distance Routing Effect Algorithm for Mobility are popular examples of position based protocols.

2.7.3 Cluster-based protocols

Cluster based protocols rely on forming small groups where a cluster head is selected. The cluster head is in charge of sending messages to other nodes. It is suitable for large networks with high scalability. The main problems are the dependence on the cluster head which makes the network more likely to errors
2.7.4 GeoCast-based protocols

GeoCast-based protocols use multicasting to deliver messages to a specific region. Multicast is a multi-hop broadcast method that does not require to know the address of the receiver. It uses flooding techniques for data transmission and reduces the collisions as packet overhead is reduced. Inter-Vehicle GeoCast and Direction-based GeoCast Routing Protocol for query dissemination in VANET are examples of GeoCast-based protocols. Also, new standards like European Telecommunications Standards Institute, Intelligent Transport Systems operating in 5 GHz band (ETSI ITS G5) can perform GeoCast-based protocols.

2.7.5 Broadcast-based protocols

This technique relies in broadcasting the messages along the network. It has been the main routing method in VANET due to the fact that in VANET the information has to be transmitted to the surroundings instead of transmitting it to a specific member of the network. Therefore, broadcasting is usually a must in VANET, and broadcast protocols have to be implemented while other routing protocols based on position or topology do not need to be implemented since in most applications there is no need to transmit to a specific node.

However, broadcast-based protocols have to deal with some problems like bandwidth consumption, high collision or high packet overhead since packages are transmitted using flooding techniques. In order to get a better performance, selective forwarding strategy is used. This is generally done by distributed and probabilistic methods. Distributed Vehicular Broadcast Protocol (DV-CAST) has proven to be one of the most well-known and efficient broadcast-based protocols [9], [10], [11].

2.8 Distributed Vehicular Broadcast Protocol (DV-CAST)

Tonguz et al. [12] presented to IEEE the demonstration of the broadcast storm problems causing packet collision and packet loss since too many vehicles broadcast at the same time in VANET. The solution to this problem was presented to IEEE in collaboration with General Motors in what it is known as Distributed Vehicular Broadcast Protocol (DV-CAST) [10], [11].

DV-CAST is a distributed and probabilistic model. Hence, it behaves differently depending on the traffic scenarios. It distinguishes between sparse and dense scenarios and reduces the broadcast overhead, packet loss and is more bandwidth efficient.
Therefore the vehicle has to first decide how to act depending on the traffic scenario. If a vehicle $V_i$ receives a broadcast message, $V_i$ firstly checks if vehicles exist behind. If so, a broadcast suppression method is taken to forward the broadcast message. On the other hand, if there is not vehicles behind, $V_i$ forwards the broadcast message via the traffic flow in the opposite direction. After $V_i$ broadcasting message, $V_i$ overhears for a period of time to ensure that the message is successfully broadcasted if the direction of $V_i$ is different from the source vehicle. $V_i$ will wait if there is no vehicles around until it receives a hello message either from a vehicle behind or a vehicle in the opposite direction, then it would act depending on which one of the situations is required.

![Decision Tree for DV-CAST Protocol](image)

Figure 2.8 1: Decision Tree for DV-CAST Protocol

Figure 2.8 1 shows the decision tree for DV-CAST protocol. MDC stands for Message Direction Connectivity, ODC for Opposite Direction Connectivity, DFlg stands for Destination Flag and ODN for Opposite Direction Neighbour. The value for MDC will be 1 if there is any vehicle behind in the same direction. ODC will be 1 if there is a vehicle in the opposite direction. Finally, DFlg will be equal to 1 if the vehicle is the intended receiver for the broadcast message and 0 otherwise.

The protocol also proposed three different schemes for the broadcast suppression protocol. The duty for the broadcast suppression protocol is to
prevent the excessive flooding in the network. The three different suppression techniques are weighted p-persistence, slotted 1-persistence and slotted p-persistence.

In weighted p-persistence, if the vehicle \( V_j \) receives a message, it rebroadcast the message with a probability \( p_{ij} \):

\[
p_{ij} = \frac{D_{ij}}{R} \quad 0 \leq p_{ij} \leq 1
\]

\[
p_{ij} = 1 \quad \text{after } t \text{ ms if no ACK}
\]

Where \( D_{ij} \) is the distance between vehicles and \( R \) the transmission range of \( V_j \).

Another way to establish \( p_{ij} \) can be based on a fixed number or depending on the number of surrounding nodes.

In the slotted 1-persistence, when the vehicle \( V_j \) receives a packet from \( V_i \), \( V_j \) waits for \( T_{sij} \) time slots. In this case has \( V_j \) probability 1 to rebroadcast the message and \( T_{sij} \) is:

\[
T_{sij} = S_{ij} \times t
\]

\[
S_{ij} = \left\lceil N_s \left( 1 - \frac{D_{ij}}{R} \right) \right\rceil \quad \text{if } D_{ij} < R
\]

\[
S_{ij} = 0 \quad \text{if } D_{ij} > R
\]

\( t \): propagation time
\( N_s \): default number of time slot

The slotted p-persistence is a combination of the two previous models where time slots are considered as well as a probability \( p_{ij} \) to forward the package.

Other probabilistic models can be implemented on top of the distributed model. That is, for the broadcast suppression, other probabilistic and flooding control techniques would be valid [13].

2.9 Dedicated short range communications (DSRC)

Dedicated Short Range Communications (DSRC) are a set of standards and protocols used in vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications in Intelligent Transport Systems. They allow a medium range wireless communication with high data transmission [14].

DSRC are allocated in 75 MHz of spectrum in the 5.9 GHz band. The key attributes of the DSRC are low latency and limited interference as well as a stronger signal. That results in better behaviour comparing to the classic WLAN networks.

Finally DSRC systems consists in Road Side Units (RSUs) and On Board Units (OBU). They are used in the majority of European Union countries, as well as the
United States. But most of these systems are not compatible at the moment [15]. Therefore it exist the need of standardization to ensure compatibility between all the systems. There is one main approach for the United States and one for the European Union. These approaches are Wireless Access in Vehicular Environments (WAVE) and European Telecommunications Standards Institute, Intelligent Transport Systems operating in 5 GHz band (ETSI ITS G5) [6], respectively.

2.9.1 Wireless Access in Vehicular Environments (WAVE)

WAVE represents the latest standardization of protocols for vehicular applications done by a work group from IEEE. WAVE architecture is lead by the specifications of IEEE 802.11p and IEEE 1609 standards [4].

WAVE pretends to modify current standards and implement new ones in order to adapt to the specific characteristics of VANET. The key attributes that WAVE pretends to cover are stronger channel and communication capacities, less latency and connection time and great reliability and security of the network.

IEEE 802.11p provides the MAC and PHY layer for WAVE technology. It is based in the original standard IEEE 802.11, specifically to IEEE 802.11a, but with some modifications in order to adapt to vehicular networks which are characterized for having to perform in highly dynamic and mobile environments [16]. IEEE 802.11p can afford transmission rates from 3 to 27 Mb/s over a bandwidth of 10 MHz. Then it works with half of the bandwidth of IEEE 802.11a. It also provides
range up to 1000 metres and can work with relative vehicle speeds of up to 30 m/s [17], much higher than the velocities that other Wi-Fi standards can support. This new standard has proven better results than the original IEEE 802.11, mainly by simulations and theoretical analysis [7], [8].

The standard IEEE 1609 is composed by a group of terms that define the architecture, communication model, management of the network, security as well as the physical access to the communications.

Specifically the standard IEEE 1609.2 focus on security. The standard IEEE 1609.3 provides the network and transport services, which would be equivalent to network layer and transport layer from the OSI model. Channel coordination and routing are managed by the standard IEEE 1609.4 as well as certain operations in the MAC sub-layer. Finally, higher layer standards like IEEE 1609.5 or IEEE 1609.6 are being now developed and will focus on network management requirements and remote management services [18].

2.9.2 European Telecommunications Standards Institute, Intelligent Transport Systems operating in 5 GHz band (ETSI ITS G5)

ETSI ITS G5 corresponds to the set of protocols and parameters as well as the access technology to be used in 5.9 GHz frequency band for European Intelligent Transport Systems [19], [20].

![Figure 2.9 2: ETSI ITS G5 Protocol Stack](image)

In many aspects is similar to the previous WAVE standard. It also uses a PHY and MAC address based on IEEE 802.11p and establish a great importance to
reliability and security of the network, as well as improving communication strength and reduced latency. Still, there are some differences when it comes to Control Channel (CCH). While in WAVE technology uses single radio devices that periodically tune to known channels to not miss important messages, ETSI ITS G5 relies in a stronger multi radio system and should always keep one radio tuned to CCH [6].

An additional feature to ETSI ITS G5 standard is the incorporation of a routing and broadcast protocol to be used in the ad hoc network based on geographical information, known as GeoNetworking protocol. This is a network layer protocol and allows the communication between individual ITS nodes as well as the distribution of messages in a geographical area [21].
3

Method

3.1 Introduction

As seen, the project seeks to have a fully working prototype to establish a real deployment of a VANET network. Then, it aims to analyse the network performance and understand the behaviour in the actual scenario.

This thesis relies on research and development. Since there are different approaches and possible solutions to solve the problem, it is needed to choose the correct method and to be sure that the proposed solution is the appropriate.

Another key factor is to have the correct documentation, papers and research to give validity to the project as well as to be able to compare the obtained results with the ones of theoretical studies.

3.2 Tools

In order to develop and implement the network, several tools have been used:

3.2.1 Software

Linux Operating System

The project has been programmed and developed in Linux. The reason to use Linux is that it provides more freedom to custom and program the network interfaces as well as the programming tools and libraries required. It is also
easier to test on and the software is compatible with Raspberry Pi 3 using Raspbian.

**C language**

The software has been developed using C language. C language is the most widespread programming language in the world, and it is understood by most of software developers. Furthermore, it allows to program all the required features of the network as well as programming UDP sockets and communication mechanisms.

### 3.2.2 Hardware

**Raspberry Pi 3**

The device in charge of managing the communication and processing the data is the Raspberry Pi 3. There are several reasons behind this choice:

- It can run Raspbian, which is a Linux-based operating system for Raspberry Pi.
- The processor of the board is good enough and fast enough to run the required software without any trouble. It can support all the processing and communication duties in a valid time.
- The Raspberry Pi 3 is a cheap board and easy to implement. It also has a lot of support since it is widely used.
- It has a Wi-Fi chip on it by default. It can also support external Wi-Fi devices that would allow more range and scope to the node.
- The hardware is easy to implement and the power consumption is low when it comes to be powered by a car.
- It supports all the software requirements of the application. It supports C programming as well as the use of external devices such as the GPS.

**GPS**

A GPS is required in a VANET application to fulfil the basic information needed in the network, such as direction, speed and position. In this project Adafruit Ultimate GPS has been used due to its compatibility with the Raspberry Pi 3 and its low price covering the required features for this application.
3.3 Implementation

The implementation has been done following several milestones in order to facilitate the development of the final prototype. This method prevents having to get the final prototype without knowing if the previous necessary features work. Therefore every phase needs to be completed before going to the next tasks.

The hardware needed, that is, the Raspberry Pi 3 as well as the GPS, is available since the beginning of the project. Hence, the implementation is done by software over the required hardware. Every feature that is needed for the prototype to work has to be either programmed or configured for the device.

First of all the WAVE standard was taking into account as the base for building the application and software. Although the proper standard was not followed, the functionality of the different layers of the communication stack was replicated in order to be able to perform in a similar way. Also, the IEEE 802.11p could not be used due to the fact that the hardware supporting the standard was not available. Instead, IEEE 802.11 bgn was used, as it is the most common
Wi-Fi standard. The upper layers of the stack were replicated following WAVE behaviour.

### 3.3.1 Configuration of the device

The first milestone that has to be achieved is to create an ad hoc network working with IPv6. That can be created using Linux interfaces or using a script that is automatically executed when the device is powered up.

Ad hoc mode can be established for any device if the hardware supports it. Most of Wi-Fi cards support this mode. It is also supported in the Raspberry Pi 3. Then it is only needed that the Linux kernel implemented in the Raspberry Pi 3 supports IPv6 due to the fact that the interface can be always modified.

Once the ad hoc network is created, the result would be to have a network without access point that allows the communication between several devices. It is required that the devices share the same network name, cell and WEP password.

#### Figure 3.3 2: Configuration of Raspberry Pi 3 network interfaces to work in ad hoc mode with IPv6

### 3.3.2 Software Implementation

The software implementation consists in the running program that will perform in the VANET network. It will handle all the communication services as well as data processing and information gathering. Therefore the software has to be optimized to be fast, efficient and to use as less resources as needed, since that will increase the performance and lifetime of the device. As said, the software implementation has been done in C code. It covers all the processing regarding the data as well as device and sockets usage and configuration. The main program also relies on the use of external libraries and files to give support to the GPS, GPIO and serial communication features.
Figure 3.3 3: Pseudocode of the implemented software
UDP Sockets

The communication relies on UDP sockets. They have to be proven to perform correctly from the first stages of the project. The devices have to act both as server and client in order to send and receive information. In order to obtain a better performance, the listening is done using threads and interruptions. In this case the program waits until an interruption comes with a new package or the waiting limit for the socket is reached. This allows the device to perform as required but with the minimum use of resources since almost 100% of the time the program does not have to perform any tasks and waits for an interruption. It has to be said that the processing speed of the device is much faster that the frequency of sending and receiving information. Hence, working with interruptions is sought in order to improve the efficiency and reduce resources usage.

Gather GPS information

GPS information needs to be gathered in every vehicle. The information required is speed, location and direction. This basic information shall be broadcasted to other members in the road. Also, the information received from other vehicles has to be recollected and processed. Standard information should be broadcasted with a frequency of more or equal than 1 Hz therefore GPS has to be updated with the same or more frequency.

The GPS information is gathered using hardware connected by serial communication to the Raspberry Pi 3. GPIO pins can be used to perform this communication. The GPS provides all the information required so it only needs to be obtained and stored. In order to complete this task, a driver can be used or the device configuration needs to be changed. The information is obtained in text mode, then future processing is also needed to obtain only the information sought.
3.3.3 Messages types

Different messages types have to be defined and configured. Every vehicle in the network has to use the messages in the same way in order to avoid error or dangerous situations. The messages carry the basic information the vehicles communicate. The format of the messages needs to be the same and understood by every member of the network.

Three different messages types have been defined in order to cover all the possible actions required in the network. Each message type has various attributes depending on their functionality. The packages are distinguish since the message type is specified in the package heading. The standard buffer of the messages is 256 bytes. Since the information is text based, there is no need for more buffer.

Standard message

The standard message is the most common of the different messages. It is communicated all the time no matter what the scenario the car is involved in. The standard message carry basic information such as latitude, longitude, direction, speed and the IP address of the sender.

The standard message does not require acknowledgement. It is simply broadcasted to the surroundings. The receivers of the standard package process and store the information in order to have more knowledge of the surroundings.

Figure 3.3.5: Example of serial communication with GPS information
The frequency for sending standard packages has to be more or equal to 1 Hz. It has been determined to use a frequency between 20 and 50 Hz since the standard packages only give basic information and do not require the quickest respond.

Warning message

Warning messages are used for sending information about actions that required to be communicated in a specific moment. These actions can be change of rail, quick deceleration or change of direction. Warning messages do not expect an acknowledgement neither. The package is sent twice just before the actions is performed.

The warning package carry basic information such as direction, position and speed as well as information about the warning. The additional information includes the direction of the message, the number of hops, the intended received, the message code to identify the warning and the proper information about the warning.

Usually warning messages only perform one hop. But it can be possible that the vehicles rebroadcast the message if it is determined. Also it can be specified the direction of the message and the intended receiver, so it is only processed by the vehicles that should be aware of the sent information.

Figure 3.3 6 Shows the behaviour of a node when receiving a warning message. The rebroadcast will only be performed if the number of hops is greater than zero. If not, the information would be processed if the vehicle is the intended destination of the message no matter if the message is rebroadcasted or not.
Alert message

Alert messages are used for sending quick information about possible accidents or dangerous reports about the traffic situation. The information carried in an alert message is similar to the warning message. Basic information such as position, direction and speed is sent as well as information about the message direction, intended destination, message code, number of hops and proper information about the alert.

The information about the intended destination, message direction and number of hops is sent in order to make sure that only the vehicles that are interested in the information would receive it, while the others do not process the information. This is done to prevent message flooding in the network and save bandwidth consumption and prevent packet loss at the same time packet delay is reduced.

The way to proceed of the vehicles when sending and receiving alert messages is determined by the broadcast protocol. Usually the message is broadcasted to all the possible members in the surroundings or even carried for hundreds of meters. This type of behaviour can be dangerous for the network since there can be a lot of vehicles broadcasting the same information at the same time. In order to prevent packet collision, packet loss and message flooding, a broadcast protocol is performed. Section 3.3.4 explains the basics of broadcast protocols as well as the proposed broadcast protocol for this project. This broadcast protocol will determine how to handle alert messages as well as process the carried information.

3.3.4 Broadcast Protocol

VANET networks rely on broadcasting or multicasting for most applications. There is no need to send a message to a specific member but to send the information to the neighbours as well as receive the information from the surroundings [9]. But this behaviour entails some problems like bandwidth consumption, high collision or high packet overhead, specially if there are many vehicles participating in the communication. These problems can decrease the network performance to the point it can not be used.

Therefore VANET networks need to implement a broadcast protocol to handle the communication. It determines the behaviour of each device when sending and receiving packages. It also includes the processing regarding the broadcast communication.

Also simple broadcasting would only have connectivity if the members of the network are directly connected. The moment there is not another vehicle to jump, the message is stopped. Hence it only considers communication using one rail while direct communication is available.
In order to improve the behaviour of the network a broadcast protocol based on distributed and probabilistic models is proposed. Most broadcast protocols are based only in probabilistic models to reduce message flooding, reduce bandwidth consumption as well as packet lost. Probabilistic models are useful when the network is full of vehicles then control over the messages has to be done. They are not a good choice in scenarios where there is spare traffic or almost no traffic. Therefore distributed models are also needed. Distributed models take into account the scenario the vehicle is involved in, that is, regular traffic, spare traffic, or dense traffic conditions. The combination of distributed and probabilistic models offer the best performance for the network.

Reference: DV-CAST protocol

The broadcast protocol presented has taken as a reference DV-CAST protocol. This protocols has been chosen since it is one of the most popular broadcast protocols and it gives a good performance [10], [11]. The research has been validated and published by IEEE and it has also been supported by General Motors.

![Broadcast success rate comparison between DV-CAST and simple broadcast](image)

Figure 3.3 7: Broadcast success rate comparison between DV-CAST and simple broadcast
Figure 3.3 7 Shows the different behaviour of DV-CAST protocol when comparing to a basic broadcast method in a VANET network. It can be seen that for spare traffic the difference in the performance is very accentuated. While DV-CAST protocol has a smoother decrease in broadcast success rate, simple broadcast method has a very pronounced fall.

Figure 3.3 8 Shows the difference in distance reached. The distance reached in simple broadcasting remains the same, that is because it depends only on the number of vehicles. The moment there is no a vehicle to communicate the message stops flowing. On the other hand, DV-CAST protocol consider traffic conditions where there can be less vehicles in the road, and the vehicles that are part of the network can carry the messages in both directions until they find another vehicle to communicate.

It is a distributed and probabilistic model, hence it considers three different scenarios: regular traffic, sparse traffic and dense traffic. The determination of the traffic scenario is made locally by each vehicle when an alert message is received. The probabilistic model is applied if the number of vehicles in the network is high and the message flooding has to be reduced. DV-CAST protocol
can reach a 70% reduction in broadcast redundancy and packet lost ratio in a well connected vehicular network.

Regular and dense traffic scenarios are treated equally in DV-CAST protocol. A vehicle is considered to be in regular or dense scenario if it has at least another vehicle behind, in the same rail. This vehicle is able to continue the transmission of the package, therefore a broadcast suppression technique is applied, based on a probabilistic model.

Spare scenario is considered when there are no vehicles in the same direction of the sender. The protocol then relies in the opposite direction vehicles to carry the message. If there is a vehicle in the opposite direction, the message is sent so the vehicle in the opposite direction carry the message until it finds a new vehicle in the intended direction, or until the package timer expires. If there are no vehicles neither in the opposite direction, the sender waits until a vehicle appears in the same rail following the intended direction or in the opposite direction. If no vehicle appears, the message is dropped after the package timer expires. On the other hand, if a vehicle appears, the sender rebroadcast the alert message and the DV-CAST protocol continues.

Figure 3.3 9 Shows the basic decision tree of the DV-CAST protocol as explained before. MDC stands for Message Direction Connectivity, ODC for Opposite Direction Connectivity and DFlg for Destination Flag. Destination Flag is set to 1 if the vehicle is in the correct lane and direction and is set to 0 if it is in the opposite direction.
When applying broadcast suppression a probabilistic technique is established. As it was seen in Section 2.8 there are three probabilistic models that can be applied. The models are weighted p-persistence, slotted 1-persistence and p-persistence.

![Figure 3.3 10: Broadcast statistics of the probabilistic models](image)

Figure 3.3 10 Shows the different statistics of the three models. It can be appreciated that weighted p-persistence and slotted 1-persistence have a similar behaviour. 1-persistence would be a model that broadcast 100% of the packages so the packet loss ratio as well as the bandwidth consumption would be very high, then it is not an appropriate model. Slotted 0.5-persistence would have a reduced packet loss ratio and bandwidth consumption, but the delay would be significantly higher and the penetration rate much lower comparing to the other models. Hence, the better solution would be weighted p-persistence or slotted 1-persistence, since they provide low packet loss ratio, low delay and very high
penetration rate. Furthermore, weighted p-persistence has been chosen as the model to follow since it has one of the best performances and also would help to reduce significantly the bandwidth consumption.

**Proposed protocol**

The proposed protocol is based in DV-CAST protocol but with some incorporations. This is because although DV-CAST protocol has promising results it can be optimized. Therefore the proposed protocol is similar to DV-CAST protocol with just some additions.

Firstly, DV-CAST protocol only considers broadcast messages that go from the sender to vehicles behind it. But broadcasting by definition would reach every car in the surroundings. Hence the first measure to implement is to define who is the intended destination of the message. Then the new messages will also carry information about if the message should go ahead or behind the first sender. The receiver will determine in first place if he is the intended destination of the message. If it is not, then it will drop the message, saving processing time and bandwidth in the network.

In second place, a number of hops is implemented to the messages. Currently DV-CAST only considers a package to be stopped if the package timer expires when the vehicle is in a spare traffic scenario. In dense scenarios this behaviour could lead to a problem since when many cars are in the network the message would not be dropped, eventually causing the network to be flooded and even collapse. Therefore a number of hops for every packet is implemented. If the receiver gets a package with number of hops equal to 0, then we would not rebroadcast the information any more.

Furthermore, an acknowledgement systems is implemented (ACK). If a vehicle who has already rebroadcast an alert message receives a new one with less number of hops, that means it is the ACK from a vehicle ahead in the intended direction of the message. Therefore the vehicle in the intended direction has been awarded of the message. The sender can stop rebroadcasting since it is sure that the forwarding vehicles have received the message correctly.

Last of all, an alert list is implemented for the proposed protocol. That is when an alert is received it is updated in the vehicle's alert list. When the package timer expires or the ACK is received the alert is removed from the list. With this method the vehicles are allowed to record different alerts from different sources of vehicles. Original DV-CAST only considers one unique alert from one source that propagates through the network. That is not valid for a real deployment therefore implementation of an alert list is mandatory.

Every alert message needs to have information about the source and location of the alert, information about the alert itself, information about the intended direction of the message as well as information of the sender like sender IP, sender speed and location. It also needs to have a code to identify the alert so it can be updated in the alert list or removed if the ACK or the timer expires.
Figure 3.3 11 Shows the decision tree for the proposed protocol. It can be seen that the core of the protocol is the same as it is in DV-CAST protocol. Some additional features has been added in order to make the protocol more suitable for a real deployment.

The proposed protocol also considers the broadcast suppression protocol or the rebroadcast that has to been performed depending on the traffic scenario. Once an alert has been received either the broadcast suppression or rebroadcast protocol is activated.

The vehicle works with an alert list, hence several alerts can be handled and considered at the same time. The alert list will be gone through and the action dictated by every member of the list will be performed. It has to be considered that usually most of the elements in the list will they are cleared after the ACK is received or the package time expires.
In case of having to execute the rebroadcast, the vehicle will simply wait for a hello message from a neighbour node. When the hello message is received the sender will broadcast all the alerts on the list waiting for a hello message.

In case of needing broadcast suppression for the message, the vehicle will broadcast the message with probability \( p \). After \( \mu \) ms if no ACK has been received the vehicle will start to broadcast with probability 1.

The probability of the broadcast suppression is determined by a weighted \( p \)-persistence model.

\[
p_{ij} = \frac{D_{ij}}{R} \quad 0 \leq p_{ij} \leq 1
\]

\[
p_{ij} = 1 \quad \text{after} \ t \ \text{ms if no ACK}
\]

Once an alert has been received and stores on the list, the broadcast protocol for sending messages is activated until there is no tasks to perform regarding the alerts. Figure 3.3 12 Shows the behaviour of the protocol when sending messages. The list is gone through and for every activated alert the protocol activates the broadcast suppression method, continues waiting for a hello or does nothing.

\[\text{Figure 3.3 12: Broadcast protocol when sending}\]
3.4 Evaluation

Once the network is fully programmed and configured it has to be tested in different scenarios. The analysis will determine if the network is suitable for a real deployment and know its strengths and weaknesses.

Firstly, the variables to measure are latency, jitter and packet lost ratio. These variables can determine the success rate of the network as well as time needed to transmit the information.

Furthermore, these variables need to be measured in different conditions. That is, different speeds, distances and number of nodes would be considered for the test.

The objective of the evaluation is also to give validity to the network and to the software created. This can be done comparing the results of the analysis with theoretical results and simulations of previous studies and papers. Therefore, with the evaluation and analysis of the real deployment it will be possible to determine if the network is appropriate for a real scenario and how to improve the network performance.

Hence, the evaluation has to be done using real hardware running the proposed software that has been programmed. The hardware has to be installed in a vehicle in order to perform the test.

The number of different scenarios includes changing different parameters of the network. The different parameters are:

- **Nodes density (nodes/km):** typically considering between 0 and 50 nodes/km in straight lane or between 0 and 100 nodes/km² in urban scenarios.

- **Scenario length and area:** it considers the total surface where the tests are being done. Typical values considered are lengths from 0 to 1.5 km and areas up to 3 km².

- **Transmission range:** the distance between the vehicles in the moment of the communication. The standard values would be from 0 to 200m.

- **Velocity:** it considers the speed of the vehicles. Typical values go up to 30 m/s while 8 m/s would be an standard value for urban scenarios.

- **Data payload size:** it considers the size of the packages transmitted, that is the number of bytes per packet. The usual value is 512 but 256 bytes per package can be considered too. It is not considered to be a large size package since the amount of information per package is not big.

- **Transmission and reception power:** it cannot be changed since it depends on the hardware. But it has to be considered since updated in the
hardware can lead to improvements in the available power and the performance of the network.

- **Frequency for sending packages**: it considers the number of packages per seconds that are being sent. A standard value considered in simulations would be around 1Hz, while most reasonable values can be around 5 to 50Hz.

- **Time since emission**: the amount of time that has passed since the simulation started can be considered for special scenarios such as rebroadcast of warnings or alerts.

Furthermore, the variables considered to be measured are:

- **Latency**: the amount of time since the sender broadcast a package until the receiver processes it.

- **Jitter**: the standard deviation in the latency since it is interesting to measure how regular is the time in the communication between vehicles.

- **Packet loss rate**: it measures the number of packages that are sent but not received.

- **Transmission range**: the distance that determines the maximum scope of the communication.

- **Network performance**: it measures the reliability in the reception of packages as well as the ability of the network to avoid collapse in special scenarios such as the rebroadcast of an alert from many vehicles.

The measurement of this variables would determine the reliability and security of the network. Also upgrades to the hardware need to be considered since they can improve the global performance of the network.
In this chapter the results of the prototype performing in different tested scenarios will be presented. As said, the results will show different parameters such as latency, packet loss or delivery ratio while changing some variables like distance between vehicles, vehicles density or speed. The idea behind the testing is to check the prototype and analyse how the network performs when having a real deployment.

In section 4.1 the results of the real deployment will be shown. In order to get this results the prototype is installed in the vehicles, which are cars or bicycles for urban scenarios. The packages sent correspond with standard messages with information about position, speed and direction of the vehicle.

In section 4.2 the results of a real deployment testing the performance of the broadcast protocol will be shown. Also these results will be compared with the simulation results of DV-CAST, published in a paper of the state of the art.

Finally, in section 4.3 the results of two different traffic scenarios will be shown. In this case the values of two papers of the state-of-the-art will be presented, and they will be compared with the results of the proposed prototype performing in the same conditions.

### 4.1 Real deployment results

First of all, the developed network has been tested in different scenarios, that is, changing different variables and measuring the parameters of interest for the network. In order to obtain the results, the real deployment was kept working for at least fifteen minutes. Also a minimum of five different deployments were done every time a value wanted to be measured, then the mean value of the results was obtained. The parameters for the real deployment are shown in Table 4.1.
Most of the test has been done in urban scenarios which are characterised for having lower speeds and more vehicles in the transmission range. The average distance between vehicles would be lower in average also. This test have been carried out without the help of any additional antenna. The transmission power is 0.25 W, which means that the results can be improved by using more suitable and more powerful hardware. In the same way, using IEEE 802.11p working in 5.9 GHz would improve the obtained results.

4.1.1 Packet loss, latency and jitter against distance

The first measurements are carried out in order to test how the distance influences in the packet loss ratio, latency and jitter as shown in Figure 4.1.1 and Figure 4.1.2. In this test a raspberry Pi 3 with the running software was installed.
in two cars. The messages carried standard information such as position, speed and direction. The rest of the parameters are kept constant. Therefore the test conditions are the following:

- Distance between vehicles: \( \beta \) = variable
- Packets per seconds: \( \lambda \) = 50 packet/s
- Average speed: \( s \) = 6 m/s
- Number of vehicles: \( n \) = 2

![Packet loss against distance in urban scenarios](image1)

*Figure 4.1 1: Packet loss against distance in urban scenarios*

![Latency against distance in urban scenarios](image2)

*Figure 4.1 2: Latency against distance in urban scenarios*
4.1.2 Broadcast success ratio against number of vehicles

Secondly, the broadcast success ratio is measured against the number of vehicles in the transmission range as shown in Figure 4.1 3. This test was done using different CPUs and raspberry Pi 3 carried out in bicycles in an urban scenario. Due to the lack of physical devices for a further deployment, the maximum number of devices considered is 8 senders at the same time. Once more, the test is carried out for urban scenarios where the parameters are the following:

- Distance between vehicles: $\beta = 10-20$ metres
- Packets per seconds: $\lambda = 50$ packet/s
- Average speed: $s = 6$ m/s
- Number of vehicles: $n =$ variable

![Figure 4.1 3: Broadcast success ratio against number of vehicles](image-url)
4.1.3 Broadcast success ratio against packets per second

In third place, the broadcast success ratio is measured against the number of packets per seconds, that is, the frequency to send packages by each vehicle. The results are shown in Figure 4.1.4. The more packages per second will make it easier to miss some packages, but it has not as much influence as increasing the number of vehicles, since the main problem to miss messages is that they arrive at the same time, when the channel is busy. On the other hand, increasing the frequency of sending messages can increase slightly the packet loss ratio, but it will also increase significantly the number of packages received. This test was performed installing the hardware in five bicycles in an urban scenario.

- Distance between vehicles: $\beta = 10$-20 metres
- Packets per seconds: $\lambda = 5 - 100$ packet/s
- Average speed: $s = 6$ m/s
- Number of vehicles: $n = 5$

![Figure 4.1.4: Broadcast success ratio against packets per second](image)
4.1.4 Broadcast success ratio against speed

Last of all the broadcast success ratio is measured against the speed of the vehicle as shown in Figure 4.1 5. Increasing the speed involves increasing the distance between vehicles in order to maintain self driving as this test was performed installing the prototype in two vehicles and driving in urban and highway scenarios. Therefore there are two reasons that provoke that the broadcast performance decreases

- Distance between vehicles: $\beta = 10\text{-}70$ metres
- Packets per seconds: $\lambda = 50$ packet/s
- Average speed: $s = 0\text{-}20$ m/s
- Number of vehicles: $n = 2$

![Figure 4.1 5: Broadcast performance against speed](image)

4.2 Performance of broadcast protocol

As said, the broadcast protocol implemented is a distributed and probabilistic protocol based on DV-CAST protocol. In order to measure performance of the
Development and Analysis of a VANET Network

proposed protocol, it is tested in a traffic jam scenario. The characteristics of the scenario are:

- Distance between vehicles: $\beta = 10\text{-}70$ metres
- Packets per seconds: $\lambda = 100$ packet/s
- Average speed: $s = 0\text{-}10$ m/s
- Number of vehicles: $n = 10\text{-}30$ nodes/km

The protocol reacts to an alert message, such as one provoked by an accident. The probabilistic suppression technique applied is weighted $p$-Persistence with and acknowledgement method.

Figure 4.2 1: Broadcast protocol working in traffic jam scenario
In the first stage, the car that detects the accident sends an alert message with probability \( p \), according to the probabilistic protocol. When the cars in the first level receive the alert, they broadcast the information. This message is also received by the original car, which now knows that the cars in the first level have received the message correctly, therefore it acts as an acknowledgement and the first car would stop broadcasting. When the cars in the second level receive the alert message they also broadcast the information. This new message would act as an acknowledgement for cars in the first level. Hence these cars would stop broadcasting. This behaviour continues until the maximum number of hops is reached or there are no cars in the lane so the a car in the opposite lane has to be used to transmit the information. The probabilistic protocol is used to transmit the information with a high number of packets per second, so it makes sure that the information reaches the next vehicle as fast as possible, but sending less messages when the number of surrounding vehicles increases. Also the vehicles stop broadcasting when receiving an acknowledgement in order to decrease the number of packets in the network so the risk of flooding decreases. The performance of the broadcast protocol of the prototype developed in this project in a traffic jam scenario is compared to the performance of the model proposed in the paper, as seen in Figure 4.2 2.

Figure 4.2 2: Performance of Broadcast protocol
4.3 Comparison with theoretical studies

As said, another main objective of this project is to compare the results obtained with results published in papers of the state-of-the-art. In order to fulfill this objective, the real deployment will be done in the same conditions as presented in the paper. Then, the results obtained in this project will be shown in the same graphs as the simulations results published in the papers to compare them. It is important that the articles are valid and reliable so they give validity to the project.

4.3.1 Traffic Scenario I

The simulation results published in the first traffic scenario include packet loss probability when changing the number of vehicles and the distance between them [22]. The reference paper was presented by IEEE members at the IEEE Transactions on Communications in 2015. The changing variables are distance (β), the number of vehicles (n) and the number of packets per second (λ).

<table>
<thead>
<tr>
<th>Scenario Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet payload</td>
</tr>
<tr>
<td>Distance between vehicles</td>
</tr>
<tr>
<td>Number of vehicles</td>
</tr>
<tr>
<td>Packets per second</td>
</tr>
<tr>
<td>Length</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Power</td>
</tr>
<tr>
<td>Carrier frequency</td>
</tr>
<tr>
<td>Transmission rate</td>
</tr>
</tbody>
</table>

Table 4.2: Traffic Scenario I parameters
Firstly, the average packet loss probability against the number of vehicles is shown in two different scenarios with a number of packets per second of 50 and 100. Both scenarios are tested with an average distance between vehicles of 10 metres. The results can be compared with the theoretical results from the paper as it can be seen in Figure 4.3 1.

Secondly the average packet loss probability is measured against the average distance between vehicles as shown in Figure 4.3 2. Once more, two different urban scenarios are considered with 25 vehicles and 100 packets/s and 10 vehicles and 50 packets/s.

\[ \text{Figure 4.3 1: Average packet loss probability against number of vehicles} \]
Traffic Scenario II

The second scenario considers the broadcast performance of the network, latency and the throughput in an urban scenario [23]. This paper was presented by IEEE members at the IEEE Transactions on Vehicular Technology in 2015.
<table>
<thead>
<tr>
<th>Scenario Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet payload</td>
</tr>
<tr>
<td>Distance between vehicles</td>
</tr>
<tr>
<td>Traffic Density</td>
</tr>
<tr>
<td>Packet frequency</td>
</tr>
<tr>
<td>Area</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier frequency</td>
</tr>
<tr>
<td>Transmission rate</td>
</tr>
</tbody>
</table>

Table 4.3: Traffic Scenario II Parameters

The paper collects results that measure broadcast performance as well as latency against car density. The results published are based on simulations and theoretical results in an urban scenario. In order to make a valid comparison between the real deployment and the simulation results, the same parameters have to be considered. The number of cars considered is Poisson distributed with the following mean.

Following the same distribution the broadcast performance ratio against the car density can be obtained for an urban scenario in particular road segments considered for the test.

\[ N(x_1, x_2, t) = \int_{x_1}^{x_2} n(s, t) \, ds \]

\( n(x, t) \): car density at location \( x \) at time \( t \)

\( x_1, x_2 \): points of the road segment

(4)
Development and Analysis of a VANET Network

Simulation results model 1: Wss=32
Simulation results model 2: Wss=4
Real deployment

**Figure 4.3 3: Broadcasting performance against car density**

Simulation results model 1: Wss=32
Simulation results model 2: Wss=4
Real deployment

**Figure 4.3 4: Delay against car density**
In this case the results of the simulations are exposed depending on the value of the contention window size, which is usually a value between 0-31 for Wi-Fi and changes depending on the traffic load of the channel.

The comparison in the values of broadcast performance against car density can be seen in Figure 4.3 3 while the comparison in latency is seen in Figure 4.3 4. The results show that the values remain in the same margins as expected.
This chapter analyses the results obtained from the different tests and discusses the comparison between the results obtained and the results from papers of the state-of-the-art. Also it evaluates the theory and method used in the deployment and the gathering of results.

5.1 Results

The main purpose of the measured results is to have an idea of how the network behaves in real conditions. It can be used as a starting point in order to know what are the strength and weaknesses of the network.

The latency of the communication in urban scenarios is around 5-7 milliseconds while the processing time when sending and receiving is in the order of microseconds. This time gives a reaction distance of 7.7 cm when the vehicle moves at 40 km/h and of 23.3 cm when it moves at 120 km/h. Therefore the latency plays in favour of the network reliability, giving enough reaction time to avoid accidents or problems. It has to be considered that at 40 km/h the security distance recommended is 16 metres and at 120 km/h is 144 metres. Therefore the reaction distance provided when using VANET represents 0.48% of the recommended distance at 40 km/h and 0.16% at 120 km/h. Theoretical results of WAVE protocol using the new standard operating in 5.9 GHz frequency band show latency values between 3.3 and 16 milliseconds. This values are still more than enough in terms of safety and reliability. It can be concluded that latency plays in favour of this networks.

When it comes to packet loss ratio or broadcasting performance, it has much more impact. Most of the simulations focus then on packet loss ratio since the lack of information suppose the main problem to these networks together with corrupt information.
Firstly, it is analysed how the distance impact in the packet loss ratio. It has been seen that with a transmission power of 0.25W operating in 2.4 GHz the communication performs in values lower than 10% up to 60 metres while from there the packet loss ratio is incremented but the communication is still possible. The new hardware of the state of the art operating in 5.9 GHz confirms to reach more than 200 metres. Hence distance is not a major problem for vehicular networks.

Secondly, the impact of the number of vehicles has to be measured. Results has shown that the packet loss probability drops exponentially with the number of vehicles reaching around 15% packet loss when the number of vehicles is 8. The comparison between the results from the real deployment and the different simulations have shown that the real results are slightly worse in most of the cases, except when the sending frequency is low, which is expected since the simulation is based on the WAVE protocol and operates with much better hardware. Still, the results are in the same magnitude levels and the waveform is similar, so the general behaviour when increasing the number of vehicles is known. The best results obtained from the simulation show values around 5% when the number of vehicles is 15 and 30% packet loss when the number of vehicles is 50. In highway scenarios the number of vehicles is usually reduced except when in jam conditions while in urban scenarios the number of vehicles in the surroundings is much higher. The processing time is not a key problem so the maintenance of the information of the surroundings is not a problem. Also it has to be said that in urban scenarios there is no need of much information per second so receiving a small part of the messages would be valid. The main problem in terms of security and reliability relies in alert scenarios for example after an accident. In that case, if the number of vehicles is high, probabilistic protocols and acknowledgement have to be used in order to improve the performance of the communication and prevent flooding.

In third place, the impact of the number of packets per second is analysed, that is, the frequency with which the vehicles send the messages. The results from the real deployment show that when increasing the number of packets per second the packet loss ratio increases, up to almost 10% when 100 packets/s are being sent. It has to be said that the increase of packet loss ratio occurs mainly from 50 to 100 packets/s. Still, the increase in the packet loss ratio is very low. Increasing the frequency of sending packages would almost not decrease the performance of the network and much more information per second would be received. It is a good way of compensating the packet loss increase when the number of vehicles in communication range go up. For example, with 15 vehicles in the surroundings and 20 packets/s a vehicle would receive 16 messages per second per vehicle in average but when increasing to 50 packets/s it would receive an average of 40 without decreasing the global network performance. It has to be considered than more than 100 packets per second would not provide any more useful information and would increase the risk of flooding the network.

In fourth place, the speed impact has been measured between two vehicles driving at the same speed. It has been seen that the broadcast performance decreases quickly but it is maintained in suitable values. It has to be considered
that when increasing the speed also the safe distance has to be increased, then there are two parameters that affect this value.

The broadcast protocol has proven to work as expected following the scheme of the DV-CAST decision tree but with the incorporation of an acknowledgement method in order to reduce the message flooding. It can be concluded that the broadcast protocol is needed in order to have the quickest response without the risk of collapsing the network. As it has been seen, if no probabilistic method is applied, the increase in the number of packets can lead not only to a network flood but also to a slower response due to the increase in the packet loss ratio.

It can be considered that the main problem for the communication performance is the number of vehicles. It increases the packet loss and the risk of network flooding. In order to reduce the impact of the number of vehicles in the network different resources can be used. First of all distributed and probabilistic protocols has been implemented in order to reduce the number of packets in the network that carry the same information. Also, acknowledgement methods can be implemented in order to reduce the number of vehicles sending once it is known that the message is received.

On the other side, the main strength of the network is the low latency which has an average value of 5-7 milliseconds. It gives plenty of reaction time due to the fact that is direct communication between vehicles. Also, the distance reached in the communication is consider to be a strength. Basic hardware can reach 100 metres in the communication while more specific hardware can reach more than 200 metres without decreasing the performance.

5.2 Method

The method relies on the implementation and programming of the prototype. When implementing the prototype, the Raspberry Pi 3 was used as the primary hardware because it is cheap, commercially available and easy to configure and program. Furthermore, it allows to work on the standard IEEE 802.15.11 b/g/n by default with a suitable power transmission. This was considered to be the most accessible way to perform a real deployment with several devices working at the same time. Although it was a good option in terms of implementation and number of available devices, it is not considered as the best option as a product for the future. The state of the art technology relies on the use of hardware that supports IEEE 802.11p where the DSRC standards can be applied. Still, the hardware is not commercially available and the standards are not finished, so in order to achieve a complete real deployment using more accessible hardware was in the end considered as the best option. The GPS was considered to be also a good election due to its prize and facilities to work together with the Raspberry Pi 3.
When it comes to the software implementation, it has all been programmed in C language. C language is the most popular choice when it comes to embedded systems and communication, so it was considered to be the best choice.

The software implementation has been done following the OSI model as a reference trying to replicate the WAVE communication stack. Although the different layers have been taken into consideration and the functions of each layer have been implemented, it had not followed the IEEE 1609 standard. Following the complete standard would have taken a lot of human and time resources that were not available. Furthermore, final security was not considered for the prototype. However, the software implementation covers all the basic features expected from a vehicular network. It is able to send information regarding, speed, location and direction and send different message types depending on the situation. Also, a broadcast protocol such as DV-CAST has been implemented following the decision tree and algorithms of well known papers. The final implementation of the prototype is able to send, receive and analyse the basic information expected from a vehicular network as well as to apply distributed and probabilistic models to situation regarding alerts that require a quick response and more reliability.

Finally, when it comes to testing, it has been done in real deployments as expected and compared to papers of the state of the art. This was done in order to test the validity of the network as well as the reliability and security. The results are located in the same magnitude values as the simulation results published in the papers. The results are slightly worse in performance, as expected since simulation do not replicate perfectly the reality and the hardware used in the real deployment was not the best in terms of performance as it was explained. Most of the test have been done in urban scenarios in order to compare with the papers. This was considered to be the best option in order check the validity. Also, the lack of resources in terms of hardware and vehicles made it difficult to test many different scenarios. So although the test are considered to have been done correctly and to be adequate for the deployment, it is considered that more test in new scenarios could have given a wider perspective of the communication in the network. Furthermore, the results have given a valid idea of how this kind of vehicular network behaves.

The choice to program and develop the full system first and then perform the deployment was made. This was done because testing a partial system makes no sense in order to obtain valid results, although the behaviour of every segment of the software was previously tested and confirmed. Furthermore, the results depend in great terms on the hardware, which was not possible to change. This makes it possible to test improvements in the software as well as implementing the software in hardware with better performance in order to obtain better results.
5.3 The work in a wider perspective

Ethical and social aspects related to this project are related to those same aspects in autonomous driving. The main social impact is to improve the security of the vehicles. In the end autonomous driving will finish with the necessity of a driver and the human factor in order to reduce the number of problems and accidents to the minimum, as well as improving the efficiency of the driving. The vehicular networks will be one more of the different technologies to make the objective possible. In particular, the communication between vehicles have to pay extra attention to security and reliability, since the information comes from external other vehicles and not from the vehicle itself. Then, the information can be corrupted or the communication can decrease its performance due to external agents.

When it comes to ethical aspects, they are also a key factor in autonomous driving. Autonomous driving relies on the fact that the vehicles are going to take decisions instead of humans. Therefore, the decisions made by the vehicles would affect not only the people in the vehicle but also people in other vehicles. Ethical aspects have to be considered in order to decide which aspects will be determining in order to make the decision when there are human lives to consider. There has been a lot of debate considering if the vehicle should consider the passengers security above any other or if it should consider all the people involved in a possible accident and make the decision in order to save the most.
This chapter concludes the project with some general thoughts about the performance of the prototype, its behaviour, results of the real deployment and the comparison with simulation results obtained from papers of the state of the art.

In general terms, it is believed that the project has given a further view on the present and future of vehicular networks. It has given a practical view of how the technology should work and finally some results have been obtained and comparisons have been done.

6.1 Obtained results

The obtained results will be exposed from a global point of view, trying to justify the importance that every milestone have taken in the whole project.

Firstly, it has to be named one of the duties in which the most time have been invested during the project, which is the software programming and the development of the prototype. On the one side, the device has been configured in order to behave as intended and to have the needed features to communicate in a vehicular network. That is, configure the network interfaces of the device and the network communication mode as well as configuring the GPS and serial communication with de GPS to gather the data. Furthermore, the running software has been programmed and implemented. The software includes all the features and characteristics that define a vehicular network like gathering the GPS data, send the information regarding location, direction and speed to other vehicles, implement alert messages and a broadcast protocol to prevent network flooding and collapse.

Secondly, the evaluation and validation of the software has been done in order to see if indeed the behaviour obtained is the expected from the network. In
order to perform the evaluation and validation the different sections of the software have been tested individually and then the whole set of software has been evaluated together. The evaluation had to be done both with debugging methods and checking the network with several devices at the same time. Since the communication depends not only in one device, but at least two, testing and validation has to be done trying different scenarios where the devices have real communication with each other.

In third place, measurements of different parameters has been done in order to know how the network behaves in a real scenario. That is, latency, jitter and packet lost has been measured in different scenarios changing variables such as distance between vehicles, speed, number of vehicles or number of packets per second. Also the processing time of the running software has been measured. At this point several conclusions can be made. It has been seen that the parameter with the most influence in the packet loss or communication performance is the number of vehicles. The drop in the communication performance can be compensated by increasing the number of packets per second, since the percentage of packet loss would slightly increase but the absolute value of information received would be much higher. The distance depends in great terms of the hardware and power transmission. With very basic hardware the distance reached can be easily 100 metres while with specific hardware 200 metres can be reached without any decrease in the performance. Finally, latency and jitter are the key parameters that make the direct communication a viable technology. The average latency in the communication would be between 5 and 7 milliseconds, which gives a lot of reaction time for the software to actuate. The main problems have also been detected, that is, having a great number of vehicles in the network that not only decrease the communication performance but also increase the risk of network flooding. Several responses can be taken to prevent this problem, like applying distributed and probabilistic protocols as well as acknowledgement methods if needed in order to decrease the number of vehicles sending information or the number of packets in the network.

Finally, the results from the real deployment were compared to the result of different papers of the state of the art. The comparison has been done in order to give validity to the results. The comparison was done following the same scenario conditions in order to be able to compare the results. It has been shown that the results obtained in the real deployment are slightly worse in terms of packet loss and similar in terms of latency. This results were expected since the papers consider results from simulations and with use of the latest hardware and communication standard. Still, the results obtained are in the same magnitude order and are correlated with the paper simulations. Therefore it was concluded that the developed prototype is valid as a first approach for a real deployment and knowing it strengths and weaknesses.

6.2 Objectives attainment

This section focuses on commenting each one of the individual objectives proposed in 1.2 Purpose, exposing if it is considered to be fulfilled or not.
1st objective: Generality

Some of the test have showed that the real deployment is suitable for different conditions with parameters like the number of vehicles, distance between vehicles or number of packets per second. Therefore it has been proven that the software and prototype developed is suitable for several scenarios, not only for some specific ones. Also the device is dynamic and capable to perform if the external conditions change. Then, the objective is considered to be fulfilled.

2nd objective: Requirements accomplishment

First of all, the hardware used has been chosen according to the requirements of the vehicular networks. That is, the hardware chosen supports wireless ad hoc communication using the most spread standard, that is IEEE 802.11 bgn. Also, it uses additional hardware that provides the GPS information. This hardware along with the implemented software cover all the basic requirements of a vehicular network such as sending information regarding location, direction and speed as well as being able to inform about warning and alerts. Furthermore, the device implement a broadcast protocol that include distributed and probabilistic method to improve the network performance.

When it comes to the performance of the network in terms of execution time and communication reliability, it has been seen that latency and broadcast performance values are suitable for this type of application although a great number of vehicles can decrease the performance. However it has been proved that additional resources can be use to prevent this problem.

Finally, the network is reliable and secure as long as it behaves in the standard margins of distance, number of vehicles, speed and number of packets per second. It has to be said that the security of the network has only been considered in a very early stage therefore the prototype cannot be considered to be secure against risk like corrupted packets with wrong information or external senders that flood the network. Future work would need to focus in the improving of security.

Still, the objective is considered to be accomplished since the prototype developed covers the requirements of a vehicular network and can perform in a real deployment.

3rd objective: Validity

In order to give validity to the network, the software and hardware have been tested. First of all, it has been tested that the network activity occurs without any problems. Secondly the results obtained from the measurements have been compared with theoretical studies and simulations in order to be proven trustful. That is, a quantitative analysis has been done and it has been proven that the results obtained are in the same magnitude scale as the ones from the
simulations. Furthermore, the results are coherent and they scale as expected comparing to the simulation results. Hence, the objective is considered to be fulfilled.

4th objective: Correct development of the network activity

In order to prove the correct development of the network activity it has to be tested the correct formation of the network, its maintenance and its performance for long period of time.

It is not an easy task to be able to test the correct development of the network in every possible scenario. Also the vehicular networks are designed to perform during several hours when the vehicle is active and the vehicle is supposed to communicate with many others during that time. In order to validate the correct development of the network activity it has been tested that the network behaves correctly in every phase of its behaviour.

The network is able to be formed and connect devices when they are powered up and it is able to accept new devices as well as to be able to continue its correct performance when some devices leave the network. Hence the key phases of connecting or leaving the network do not suppose a problem in any condition.

Also, the network has proven to perform for long periods of time maintaining good performance. This has been checked for periods of some hours working in the expected way. The main feature that has not been tested is meeting many different vehicles during the working time of the device. Still, the objective is considered to be fulfilled since the network has performed correctly in every phase and every scenario that has been tested.

5th objective: Robustness

In order to check robustness failure conditions are generated or environments where the network does not behave as usual are sought. Some examples of failure can be the lost of communication with some devices or the appearance of interferences.

It has been checked that the network responses correctly to interferences. Since the communication takes place in the outside, it performs better due to the lack of obstacles. Also, the disappearance of nodes does not affect the other devices in the network, which continue their performance. The parameters most likely to affect the robustness of the network are having a great number of vehicles at the same time or increasing the distance between them. Still, standard values give high values of broadcast performance. Therefore, the objective is considered to be fulfilled.

6th objective: Scalability

Scalability measures the capacity of the network to perform correctly when there is a large number of vehicles joining the network, both simultaneously or
Development and Analysis of a VANET Network

in different time periods. It has been seen that the performance decreases with the number of vehicles and it is difficult to maintain a good performance with more 30 or 40 vehicles at the same time. Also, it could not be tested the network for long periods where a lot of devices join and leave the network. Therefore the objective was not able to be fully checked and it is considered not to be fulfilled.

6.3 Future research and future perspectives

As it was said at the beginning of the chapter, it is considered that the project has given a first approach to the technology regarding vehicular networks and it has been possible to know the strong and weak points taking into account the results from the analysis of the real deployment. While the results obtained are promising, there is plenty of room for improvements in both the hardware and software implemented.

Firstly, the standard used for the communication protocol is not the latest of the state-of-the-art since the hardware working with IEEE 802.11p is not commercially available and the standards are not finished. Still, the next step would be to research in this new technology in order to implement it. The behaviour of the upper layers can be maintained as described, only having to adapt them to the new standard. Furthermore, due to hardware availability, the network has been tested in scenarios with a small number of vehicles. Future research would need to implement the chosen solution in several devices and test it in bigger scenarios.

Secondly, this project has not considered the security implementation required for a vehicular network. Security is a key aspect of IoT technology and also of vehicular networks. Future research would need to focus in implementing security to make the network protected against corrupted packets as well as flooding. The standard regarding security is not finished for the WAVE protocol, but when finished, the logic step is to take the standard as a base for building the security of the network, making it reliable in every possible situation.

Still, the future perspective for this technology show that it is going to be widely implemented and it will work hand by hand with other technologies in autonomous driving, acting as an additional source of information. Once the standardization is finished, it will be much easier to the manufactures to follow the same path and be compatible.
The latest predictions establish a future scenario where DSRC and 5G technology will be implemented in every vehicle. But for the moment it can only act as an additional source of information since it cannot be expected that every vehicle has the technology.
# Appendix A

## Time plan

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/19/16</td>
<td>12/23/16</td>
<td>Research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Test UDP Sockets over Ad Hoc Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication with other CPU and RPi3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPS data and sending GPS information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prototype: Broadcast and gather information from others</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define characteristics, type and frequency of messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Broadcast Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prototype: Send, receive and analyze useful information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Writing Report: Chapters 1, 2, 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Half time Check</td>
</tr>
<tr>
<td>03/20/17</td>
<td>03/24/17</td>
<td>Fix errors and perform updates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prototype: New features, error corrections and updates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Test Scalability, Reliability in real deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comparison with papers and other research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fix errors according to results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implement security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final Prototype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Writing Report: Chapters 4, 5, 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Final Presentation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/16/17</td>
<td>01/16/17</td>
<td>Week 1</td>
</tr>
<tr>
<td>01/19/17</td>
<td>01/19/17</td>
<td>Week 2</td>
</tr>
<tr>
<td>01/26/17</td>
<td>01/26/17</td>
<td>Week 3</td>
</tr>
<tr>
<td>02/02/17</td>
<td>02/02/17</td>
<td>Week 4</td>
</tr>
<tr>
<td>02/09/17</td>
<td>02/09/17</td>
<td>Week 5</td>
</tr>
<tr>
<td>02/16/17</td>
<td>02/16/17</td>
<td>Week 6</td>
</tr>
<tr>
<td>02/23/17</td>
<td>02/23/17</td>
<td>Week 7</td>
</tr>
<tr>
<td>03/01/17</td>
<td>03/01/17</td>
<td>Week 8</td>
</tr>
<tr>
<td>03/08/17</td>
<td>03/08/17</td>
<td>Week 9</td>
</tr>
<tr>
<td>03/15/17</td>
<td>03/15/17</td>
<td>Week 10</td>
</tr>
<tr>
<td>04/02/17</td>
<td>04/02/17</td>
<td>Week 11</td>
</tr>
<tr>
<td>04/09/17</td>
<td>04/09/17</td>
<td>Week 12</td>
</tr>
<tr>
<td>04/16/17</td>
<td>04/16/17</td>
<td>Week 13</td>
</tr>
<tr>
<td>04/23/17</td>
<td>04/23/17</td>
<td>Week 14</td>
</tr>
<tr>
<td>05/01/17</td>
<td>05/01/17</td>
<td>Week 15</td>
</tr>
<tr>
<td>05/08/17</td>
<td>05/08/17</td>
<td>Week 16</td>
</tr>
<tr>
<td>05/15/17</td>
<td>05/15/17</td>
<td>Week 17</td>
</tr>
<tr>
<td>05/22/17</td>
<td>05/22/17</td>
<td>Week 18</td>
</tr>
<tr>
<td>06/01/17</td>
<td>06/01/17</td>
<td>Week 19</td>
</tr>
<tr>
<td>06/18/17</td>
<td>06/18/17</td>
<td>Week 20</td>
</tr>
<tr>
<td>07/05/17</td>
<td>07/05/17</td>
<td>Week 21</td>
</tr>
</tbody>
</table>
One of the possible applications of VANET networks is to use road side infrastructure to gather information and be able to monitor the surroundings in different spots of the road. In order to prove the functionality of road side units, it has been developed an application that gathers the data from surrounding vehicles and shows their position in an graphical interface. As it has been seen, DSRC rely on Road Side Units (RSUs) and On Board Units (OBU). In this case, it is shown as a possible application for RSU in an urban scenario where the first level infrastructure can be used as receiving point. The interface is programmed in JAVA.
Bibliography


