# 5LIC0 Networked embedded systems - Report 2 Related Work and Design

Keyshav Suresh Mor (k.s.mor@student.tue.nl) - 1237978
Sjoerd Westendorp (s.westendorp.1@student.tue.nl) - 0864518
Dennis van den Brandt (d.p.j.v.d.brandt@student.tue.nl) - 0742705

October 5, 2018

***Abstract*—This report will focus on the implementation possibilities of a new system for the automotive industry. A quick response spare-part service concept is introduced, where cars which have stalled at the side of the road would be able to get spare parts, so they be repaired fairly quickly if possible. In order for this system to work, a fast and reliable communication network between the two cars needs to be setup. This report will therefore focus on the current protocol used for vehicle to vehicle communication, look into literature on this subject and formulate a plan in order to test how the quick-response spare part system can be implemented for vehicles of today and the future.**

## I. Scenario

Cars have become more advanced and contain more and more parts. While they are also getting more reliable, there are still a lot of systems which can fail. Most of the times these failures are easy to fix. For example a flat tire, a broken fuse or a cooling system leak. Although these systems are easy to fix when they fail, it is hard to have spare parts for all of these systems in your car at all times. However, what if there was a system where these parts can be delivered to the driver when his cars breaks down.

Instead of carrying spare parts for every possible situation in the trunk, it would be a smart if these parts where divided over multiple cars. If each car would contain one or more of these spare parts, then these drivers could assist a car which has broken down at the side of the road.

Therefore the goal of this project is to investigate a wireless system in which cars can communicate these faults. That way a driver having the spare parts which are needed by the broken down car can be signaled to pull over and help.

Two prominent communication technologies for vehicle for infrastructure(V2X) and vehicle to vehicle(V2V) communication exist, one of which is WiFi-p and the other is C-V2X. Our focus would be on WAVE or WiFI-p as it is popularly known. The goal of this report is to determine if it is possible to use this protocol for the broken car scenario.

The broken down car would initiate a WAVE Basic Service Set transmitting a Wildcard Beacon, which other cars can connect to immediately upon receiving the beacon. If a connection has been established, the broken down car must broadcast the part it needs. The cars which have these parts should signal the driver or the computer that is driving. This system must be able to communicate very fast, since if a car breaks down at the side of a highway, the time needed by a car passing the stalled car with a speed of 130 kilometers an hour is rather short. The maximum latency allowed for communication by the WAVE standard is 20 milliseconds.

## II. WiFi Standard

The generic Wi-Fi standard 802.11 laid the foundation of the V2X ( Vehicle-to-Infrastructure) communication protocols, particularly the 802.11p WAVE standard [2].

The 802.11 standard is designed for wireless communications. It operates in 900 MHz, 2.4, 3.6, 5 and 60 GHz frequency bands.

The range of communication varies from 20 metres in Indoor settings up to 5000 metres in outdoor settings. The data transfer rates may vary from 1 Mbit/sec to 3466.8 Mbit/sec.

The modulation techniques used are usually Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM).

The DSSS and OFDM allows the 802.11a and 802.11p amendments of 802.11 standard to have high data carrying capacity with low inter channel interference despite the fact that the channels are tightly packed across the frequency spectrum, closely overlapping with each other.

### A. WiFi Protocol Stack

The 802.11 standard introduced many amendments like the 802.11a/b/g/n to improve the basic 802.11 standard. These form the PHY layer of the Wifi Stack. On the top of this comes the 802.11 standard MAC frame which is common to all the 802.11 amendments. [2]

### B. Basic Network Operations

An Infrastructure Basic Service Set (IBSS/BSS) is formed when 802.11 stations share the same access point (AP). Each station listens to beacon signal from the AP before joining the IBSS or BSS after authentication and authorization.

802.11 has a Distribution Service (DS) which allows multiple interconnected BSS's form an Extended Service Set (ESS).

Each BSS has a Service Set ID (SSID) to identify itself in public or private locations. It is 0 to 32 bytes long. It is different from the BSSID which is a 48-bit long field like a MAC Address which is common to all stations in a service set. This is the MAC Address of the Access Point (AP).

The IEEE 802.11 standard data frame format is common to all 802.11 amendments, see figure 1. The frames include up to 4 address fields to carry Source Address (SA), Destination Address (DA), Transmitting Station Address (TA) and Receiving Station Address (RA).

There is a QoS control field which decides the Quality of Service being provided. The data frame field is of variable length.

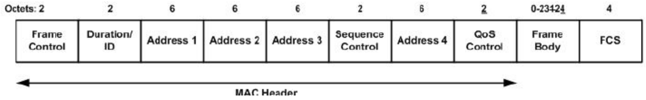
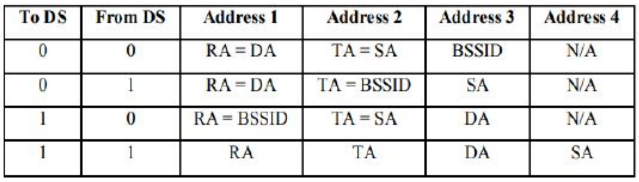


Fig. 1. 802.11 Data Frame Format



| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | RA = DA | TA = SA | BSSID | N/A |
| 0 | 1 | RA = DA | TA = BSSID | SA | N/A |
| 1 | 0 | RA = BSSID | TA = SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |

Fig. 2. 802.11 MAC Address Frame Format

### C. Need for a Special Vehicular Amendment

Authentication and Authorization to join a BSS takes a lot of time in the regular Wi-Fi amendments. This violates the latency requirements of V2X communication which could cause vehicle safety hazards.

It is impossible to implement a common BSSID for a WiFi network, in case of moving vehicles, without modifying the protocol.

The range and security of the network is critical in case of vehicular networks. The security, management and networking aspects had to be added in the form of the IEEE 1609 standard.

As the 2.4 GHz and 5 GHz frequency bands are free and unlicensed, there is a lot of interference from the adjacent channels which could cause security issues and data corruption and collision.

As the 802.11p standard is only a minor modification of the 802.11a standard, there was no need for a new wireless networking protocol and it allowed use of existing hardware, which helped the automotive industry to keep their costs low while implementing the standard in vehicles.

## III. The WiFi-p or WAVE Amendment

The 802.11p or the WAVE standard is a amendment to the the generic 802.11 standard which stands for Wireless Access in Vehicular Environments. [2]

### A. MAC Layer Amendment

Safety of vehicles is the focus of the WAVE standard. Such safety applications are dependent on low latency communication with least possible channel interference and noise. Thus, to ensure this, all 802.11p radios in a vicinity need to configured to the same channel and should be configured for the same BSSID.

A station in WAVE mode can send and receive data frames with a Wildcard BSSID with To DS and From DS fields in MAC Data Frame set to 0. Wildcard BSSID contains all 1s in its frame.

WBSS is WAVE Basic Service Set established when radio in WAVE Mode sends out beacon signal containing all necessary information for a station to join the WBSS.

A station in a WBSS is in WAVE mode and can still transmit frames with the wildcard BSSID in order to reach all neighboring stations in cases of safety concerns.

Similarly, a station already in a WBSS and having configured its BSSID filter accordingly, can still receive frames from others outside the WBSS with the wildcard BSSID.

A station ceases to be a member when it stops sending and receiving frames that use the BSSID of the WBSS. A station in WAVE mode and a part of the WBSS can still receive frame from others outside the WBSS with the same wildcard BSSID.

A station is WAVE mode is allowed to transmit and receive messages with the Wildcard BSSID without priority, meaning that two vehicle can communication with each other without additional overhead.

A station cannot be a member of multiple WBSS and it should not join an IBSS. It should also never use the usual MAC authentication and authorization process. This must be handled higher up the protocol stack. A WBSS ceases to exist when it has no members.

802.11p radios that are part of a WBSS, can use Distribution Service with ”To DS” and ”From DS” bits in MAC Address frame set to 1, if and only if the BSSID of the target Infrastructure Basic Service Set (IBSS) is known.

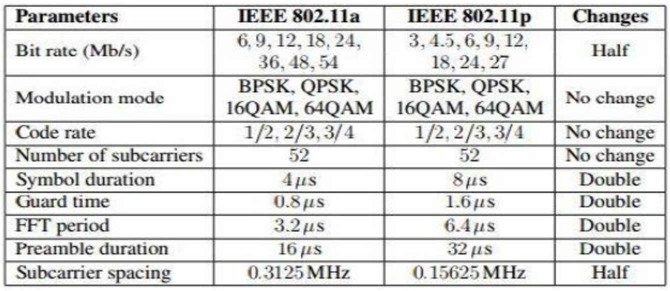
### B. PHY Layer Amendments

A Dedicated Short Range Communication (DSRC) frequency spectrum was allocated for WAVE in the United States with 75 MHz band in the 5.9 GHz frequency range.

Channels are 10 MHz wide. Channel 178 is the control channel, Channel 172 and 184 are Safety Channels and other channels are all service channels. In total there are 7 channels with a spacing of 0.66 MHz.

The 802.11p standard has half the bit-rate and half subcarrier spacing of 802.11a but double guard time and symbol duration than that of 802.11a. This increases reliability.

In Europe and Japan, the 5.9 GHz band is allocated with a bandwidth of 80 MHz and 20 MHz respectively.



| Parameters | IEEE 802.11a | IEEE 802.11p | Changes |
|---|---|---|---|
| Bit rate (Mb/s) | 6, 9, 12, 18, 24, 36, 48, 54 | 3, 4.5, 6, 9, 12, 18, 24, 27 | Half |
| Modulation mode | BPSK, QPSK, 16QAM, 64QAM | BPSK, QPSK, 16QAM, 64QAM | No change |
| Code rate | 1/2, 2/3, 3/4 | 1/2, 2/3, 3/4 | No change |
| Number of subcarriers | 52 | 52 | No change |
| Symbol duration | 4 $\mu s$ | 8 $\mu s$ | Double |
| Guard time | 0.8 $\mu s$ | 1.6 $\mu s$ | Double |
| FFT period | 3.2 $\mu s$ | 6.4 $\mu s$ | Double |
| Preamble duration | 16 $\mu s$ | 32 $\mu s$ | Double |
| Subcarrier spacing | 0.3125 MHz | 0.15625 MHz | Half |

Fig. 3. Summary of the differences between 802.11a and 802.11p on the PHY layer.

### C. IEEE 1609 Standard

The IEEE 1609 standard defines the services provided through the 802.11p standard [2]. The 1609.3 standard covers the WAVE Connection setup and management. The 1609.2 standard defines the security of the WAVE standard. The 1609.4 standard defines the multi-channel operation. The 1609.1 standard defines the resource management among various channels and over different datagram protocols which are possible to be implemented over the WAVE stack.

### D. Medium Access in WAVE

The 802.11p standard implements a Distributed Control Function (DCF). The DCF follows a principle of Collision Sense Multiple Access  Collision Avoidance (CSMA-CA) where the channel is only accessed if the physical layer senses no ongoing activity.

The medium is indicated busy if the received power level is higher than a particular threshold. It should be indicated busy even in absence of transmission if received power is higher than a higher threshold.

The concept of Inter Frame Spacing is used which indicates how long the medium should be idle before a new transmission begins. Important messages have a shorter IFS (SIFS) and periodic messages have a distributed IFS (DIFS). Whenever the station senses that the medium is busy, the station selects a random number of back off slots, which decrement after the medium is sensed idle. The countdown stops whenever the medium is busy. As the slot count reduces to zero, the frame is transmitted.

### E. Enhanced Distributed Channel Access

To prioritize the important safety and time critical messages over regular periodic service messages, 802.11p standard implements the Enhanced Distributed Channel Access (EDCA). This helps create a Quality of Service(QoS) support with 4 defined Access Categories.

Each frame is assigned one category depending on the application generating the message, the importance and the urgency of the message. The Arbitration Inter Frame Space Number (AIFSN) replaces the DIFS.

Frames with Access Category Index (ACI) 3 have a smaller AIFSN and thus lower barrier to access the medium than the frames with ACI 0,1 and 2.

ACI 2 and 3 are reserved for critical safety messages. ACI 0 is for regular access and ACI 1 is foreseen for non-prior background messages.

### F. WAVE Architecture

The WAVE Architecture takes over from the C2C, CALM and COMeSafety Architecture with a separate channels for critical safety and important messages and other service channels for infotainments and traffic efficiency messages.

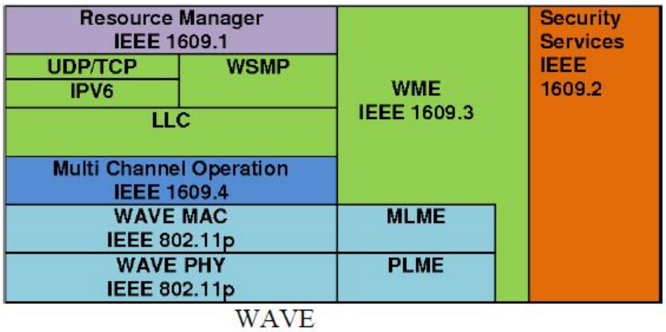


Fig. 4. WAVE Architecture

## IV. Existing Work

The existing work in the WAVE standard is largely experimental which studies various applications in automotive sectors across different regions.

Various experiments have been carried out in USA, Japan and Europe to provide proof of concepts which can be commercialized in the future [3].

Some of these notable programmes are IntelliDrive, Vehicle Safety Communication (VSC), California Partners for Advanced Transit and Highways (PATH), Smartway, Advanced Safety Vehicle (ASV) etc. [4]

It must be understood that most of these programs have focused on safety and critical applications which is the main purpose of introducing Wireless communication in vehicles. Infotainment applications and other services like Internet are possible but they are complex and are driven by commercial goals.

CVIS ( Cooperative Vehicle Infrastructure Systems) is one such program which involves communication between Vehicles and Infrastructure which can be studied further and might help us realize our application better as it focuses upon Infotainment applications.[4]

PRECIOCA (Privacy enabled capability in cooperative systems and safety applications) is another such program which experiments and tests infotainment applications through V2X communication.[4]

It must be understood that the application we imagine is an infotainment service application and while it does provide some safety, it essentially focuses upon quick repair response for a broken down vehicle.

Thus we believe that while our application is unique, some similar experiments for different applications must have been conducted and study of these can help us in development of our project.

## V. Plan

Although originally the intent was to implement the network for existing hardware. It was found that most hardware does not support WiFi-p. Existing hardware typically only support specific WiFi standards. On top of that WiFi-p frequencies require a license to use. The more niche WiFi-p is therefore typically not supported. As such it was decided to instead test the network using a simulation. This still allows the usefulness of WiFi-p in the scenario to be shown.

### A. Simulator

The network will be simulated using NS-3 [1]. NS-3 is a discrete-event network simulator for networked systems. This simulator is particularly relevant since it has explicit support for WiFi-p. NS-3 has a special model called `wave`, which involves the MAC and PHY layers. The `wave` model puts its focus on the MAC layer.

In the simulator the PHY layer is the same as regular WiFi. This is because in the WiFi-p standard the PHY layer is still 802.11a OFDM with minor changes in channel spacing and channel width. However the documentation of the simulator indicates that WiFi-p allows for more powerful signals. As such the simulator will by default underestimate the transmission range. This must be taken into account while creating the simulation of the scenario.

NS-3 comes with several WiFi-p example networks. The intend is to use these example networks to create the network as described earlier.

### B. Intended System Behaviour

The intended behaviour of the system is as follows:

- A car breaks down and stop at the side of the road.
- This car enables a WAVE beacon with a wildcard BSSID and creates a WBSS.
- Cars passing by join the WBSS.
- Communication establishes and message exchanged if a passing car has the item the broken car needs.
- If it has an item the broken car needs, then the passing car stops near the broken car.
- Else it will just drive by.
- Once the broken car has its spare parts, the beacon is disabled again.

### C. Abstractions

The passing cars can be abstracted as nodes moving along a linear path. The broken car is next to this path and is a node that does not move. Cars that have move past the broken car are not relevant and can be ignored. As such the network used for the simulator is just a few nodes in size: One for the broken car, and a few for the passing cars.

Note that the movement of a car that already has decided to stop or not is not relevant. At that point the communication with that car has already succeeded. That car therefore no longer need to be simulated. The same is true for any car that has driven out of range regardless of whether they successfully communicated or not.

### D. System requirement

The most important aspect of the system is the latency of the communication. In particular, how much time is there between a passing car getting into range of the beacon of a broken car, and the decision whether a car is going to stop or not. Lets call this period the `Decision Latency`. If the `Decision Latency` is too long, the passing cars will not have the time to stop near the broken car or may have gone out of the communication range.

### E. Summary

The NS-3 simulator will be used to simulate the communication several cars driving past a broken car. The goal is the minimize the `Decision Latency` of this process.

## References

[1] NS-3 Simulator. URL: https://www.nsnam.org/

[2] Daniel Jiang, Luca Delgrossi. ”Towards an International Standard for Wireless Access in Vehicular Environments”, *Mercedes-Benz Research & Development North America, Inc.*

[3] Sherali Zeadally, Ray Hunt, etc.. ”Vehicular ad hoc networks (VANETS): status, results, and challenges.”

[4] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. ”Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions”.