Universidade de Aveiro Departamento de Eletrónica,
Telecomunicações e Informática
2018

João Miguel
Pereira de Almeida

Comunicações Confiáveis Sem-Fios para Redes Veiculares

Dependable Wireless Communications for Vehicular Networks

MAP tele DOCTORAL PROGRAMME
IN TELECOMMUNICATIONS

Universidade de Aveiro Departamento de Eletrónica,
2018 Telecomunicações e Informática

João Miguel
Pereira de Almeida

Comunicações Confiáveis Sem-Fios para Redes Veiculares

Dependable Wireless Communications for Vehicular Networks

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Telecomunicações, realizada sob a orientação científica do Doutor Arnaldo Silva Rodrigues de Oliveira, Professor Auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e do Doutor Joaquim José de Castro Ferreira, Professor Adjunto da Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro.

Apoio financeiro da FCT através da bolsa de doutoramento ref. SFRH/BD/52591/2014.

Dedico este trabalho à minha família pelo incansável apoio ao longo do meu percurso académico.

o júri / the jury

presidente / president	Prof. Doutor Vasile Staicu Professor Catedrático, Universidade de Aveiro
vogais / examiners committee	Prof. Doutor Paulo Jorge de Campos Bartolomeu Doutorado (nível 2), Universidade de Aveiro
	Prof. Doutor Aníbal João de Sousa Ferreira Professor Associado, Universidade do Porto
	Prof. Doutor Julián Proenza Arenas Professor Associado, Universitat de les Illes Balears
	Prof. Doutor Marina Aguado Castrillo Professora Associada, Universidad del País Vasco
	Prof. Doutor Joaquim José de Castro Ferreira Professor Adjunto, Universidade de Aveiro

agradecimentos / **acknowledgements**

Agradeço toda a ajuda dos meus orientadores, colegas, família e amigos, tanto no apoio ao trabalho desenvolvido no âmbito deste doutoramento, como a nível mais pessoal. Um obrigado especial ao Instituto de Telecomunicações e à Universidade de Aveiro pelo facto de me terem acolhido ao longo destes últimos quatro anos. Por último, um agradecimento à Fundação para a Ciência de Tecnologia e ao Programa Doutoral MAP-Tele por me terem dado a possibilidade de realizar este doutoramento.

Palavras Chave

dependabilidade, tolerância a faltas, sistemas de tempo-real, redes veiculares sem-fios, comunicações dedicadas de curto alcance, sistemas inteligentes de transporte, segurança rodoviária.

Resumo

As comunicações veiculares são uma área de investigação bastante promissora, com inúmeros potenciais serviços que podem melhorar a experiência vivida no tráfego. A segurança rodoviária é o objectivo mais importante por detrás do desenvolvimento das redes veiculares sem-fios, visto que muitos dos atuais acidentes e vítimas mortais poderiam ser evitados caso os veículos tivessem a capacidade de trocar informação entre eles, com a infraestrutura rodoviária e outros utilizadores da estrada.

Um futuro com sistemas de transporte rodoviário seguros, eficientes e confortáveis é algo ambicionado pelas diferentes partes envolvidas - utilizadores, fabricantes, operadores da infraestrutura e autoridades públicas. As aplicações de Sistemas Inteligentes de Transporte (ITS) cooperativas vão contribuir para alcançar este propósito, em conjunto com outros avanços tecnológicos, nomeadamente a condução autónoma ou uma melhor infraestrutura rodoviária baseada em sensorização avançada e no paradigma da Internet das Coisas (IoT).

Apesar destes benefícios significativos, o desenho de sistemas de comunicações veiculares coloca desafios difíceis, em grande parte devido aos ambientes extremamente dinâmicos em que estes operam. De modo a atingir os requisitos de segurança crítica envolvidos neste tipo de cenários, é necessário um cuidadoso planeamento por forma a que o sistema apresente um comportamento confiável. Conceitos de dependabilidade e de sistemas de tempo-real constituem ferramentas essenciais para lidar com esta desafiante tarefa de dotar as redes veiculares de determinismo e tolerância a faltas.

Esta tese pretende endereçar alguns destes problemas através da proposta de arquitecturas e da implementação de mecanismos que melhorem os níveis da dependabilidade das comunicações veiculares de tempo-real. As estratégias desenvolvidas tentam sempre preservar a necessária flexibilidade do sistema, uma propriedade fundamental em cenários tão imprevisíveis, onde eventos inesperados podem ocorrer e forçar o sistema a adaptar-se rapidamente às novas circunstâncias.

Resumo (cont.)

A contribuição principal desta tese foca-se no desenho de uma arquitectura tolerante a faltas para redes veiculares com suporte da infraestrutura de beira de estrada. Esta arquitectura engloba um conjunto de mecanismos que permite detecção de erros e comportamento tolerante a faltas, tanto nos nós móveis como nos nós estáticos da rede. A infraestrutura de beira de estrada desempenha um papel fundamental neste contexto, pois fornece o suporte que permite coordenar todas as comunicações que ocorrem no meio sem-fios. Para além disso, é também responsável pelos mecanismos de controlo de admissão e pela troca de informação com a rede de transporte. Os métodos propostos baseiam-se num protocolo determinístico de controlo de acesso ao meio (MAC) que fornece garantias de tempo-real no accesso ao canal sem-fios, assegurando que as comunicações ocorrem antes de um determinado limite temporal. No entanto, as soluções apresentadas são genéricas e podem ser facilmente adaptadas a outros protocolos e tecnologias sem-fios.

Neste trabalho são introduzidas técnicas de mitigação de interferência, mecanismos para assegurar comportamento falha-silêncio e esquemas de redundância, de modo a que os sistemas de comunicações veiculares apresentem elevados níveis de dependabilidade. Além disso, todos estes métodos são incorporados no desenho dos componentes da rede veicular, guarantindo que as restrições de tempo-real continuam a ser cumpridas.

Em suma, as redes veiculares sem-fios têm o potential para melhorar drasticamente a segurança rodoviária. Contudo, estes sistemas precisam de apresentar um comportamento confiável, de forma a prevenir a ocorrência de eventos catastróficos em todos os cenários de tráfego possíveis.

Keywords

dependability, fault-tolerance, real-time systems, wireless vehicular networks, dedicated short range communications, intelligent transportation systems, road traffic safety.

Abstract

Vehicular communications are a promising field of research, with numerous potential services that can enhance traffic experience. Road safety is the most important objective behind the development of wireless vehicular networks, since many of the current accidents and fatalities could be avoided if vehicles had the ability to share information among them, with the road-side infrastructure and other road users.

A future with safe, efficient and comfortable road transportation systems is envisaged by the different traffic stakeholders - users, manufacturers, road operators and public authorities. Cooperative Intelligent Transportation Systems (ITS) applications will contribute to achieve this goal, as well as other technological progress, such as automated driving or improved road infrastructure based on advanced sensoring and the Internet of Things (IoT) paradigm.

Despite these significant benefits, the design of vehicular communications systems poses difficult challenges, mainly due to the very dynamic environments in which they operate. In order to attain the safety-critical requirements involved in this type of scenarios, careful planning is necessary, so that a trustworthy behaviour of the system can be achieved. Dependability and real-time systems concepts provide essential tools to handle this challenging task of enabling determinism and fault-tolerance in vehicular networks.

This thesis aims to address some of these issues by proposing architectures and implementing mechanisms that improve the dependability levels of real-time vehicular communications. The developed strategies always try to preserve the required system's flexibity, a fundamental property in such unpredictable scenarios, where unexpected events may occur and force the system to quickly adapt to the new circumnstances.

Abstract (cont.)

The core contribution of this thesis focuses on the design of a fault-tolerant architecture for infrastructure-based vehicular networks. It encompasses a set of mechanisms that allow error detection and fault-tolerant behaviour both in the mobile and static nodes of the network. Road-side infrastructure plays a key role in this context, since it provides the support for coordinating all communications taking place in the wireless medium. Furthermore, it is also responsible for admission control policies and exchanging information with the backbone network. The proposed methods rely on a deterministic medium access control (MAC) protocol that provides real-time guarantees in wireless channel access, ensuring that communications take place before a given deadline. However, the presented solutions are generic and can be easily adapted to other protocols and wireless technologies.

Interference mitigation techniques, mechanisms to enforce fail-silent behaviour and redundancy schemes are introduced in this work, so that vehicular communications systems may present higher dependability levels. In addition to this, all of these methods are included in the design of vehicular network components, guaranteeing that the real-time constraints are still fulfilled.

In conclusion, wireless vehicular networks hold the potential to drastically improve road safety. However, these systems should present dependable behaviour in order to reliably prevent the occurrence of catastrophic events under all possible traffic scenarios.

Contents

List of Figures

List of Tables

Glossary

3G Third Generation. xi, 16, 18

4G Fourth Generation. xi, 16, 18

5G Fifth Generation. xi, 2, 3, 13, 14, 50

5GAA 5G Automotive Association. xi, 14

ABS Anti-lock Braking System. xi, 1

ACI Adjacent Channel Interference. xi, 5, 34

AD/DA Analog-to-Digital/Digital-to-Analog. xi, 18

BLE Bluetooth Low Energy. xi, 13

BPSK Binary Phase Shift Keying. xi, 15

BSS Basic Service Set. xi, 3, 15

CACC Cooperative Adaptive Cruise Control. xi, 2, 29

CAM Cooperative Awareness Message. xi, 16, 37

CCH Control Channel. xi, 15

CCI Cross Channel Interference. xi, 4, 34

CEPT European Conference of Postal and Telecommunications Administrations. xi, 15

C-ITS Cooperative ITS. xi, 1, 3

COTS Commercial-Off-the-Shelf. xi, 18

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance. xi, 3, 15, 36, 38

CTMC Continuous-Time Markov Chain. xi, 49

D2D Device-to-Device. xi, 14

DCCS Distributed Computer Control System. xi, 2, 4, 19

DENM Decentralized Environmental Notification Message. xi, 16, 37

DSRC Dedicated Short Range Communications. i, v, xi, 13, 14, 16, 18, 33–35

EC Elementary Cycle. v, xi, 38–40, 43

eCall Emergency Call. xi, 18

EFC Electronic Fee Collection. xi, 2

ETSI European Telecommunications Standards Institute. v, xi, 3, 14–16, 34, 36, 40, 47

FCC Federal Communications Commission. xi, 15, 34

FDMA Frequency Division Multiple Access. xi, 37

FIR Finite Impulse Response. xi, 5, 36

FP Free Period. xi, 38–40

FPGA Field Programmable Gate Array. xi, 5, 18, 19

FTT Flexible Time Triggered. ii, xi, xii

GF Group Formation. xi, 29

GPS Global Positioning System. xi, 16, 18, 19, 37, 40

GSM Global System for Mobile Communications. xi, 13

I/Q In-phase and Quadrature. xi, 18

IEEE Institute of Electrical and Electronics Engineers. v, xi, 3, 14–16, 18, 34, 36, 38, 47

IFS Inter-Frame Space. xi, 6, 39, 44

IoT Internet of Things. xi, 2

IoV Internet of Vehicles. xi, 2

IP Internet Protocol. xi, 3, 15

ITS Intelligent Transportation Systems. v, xi, 1, 3, 13–16, 18–20, 29, 33, 34, 36, 40, 43, 47

IW Infrastructure Window. xi, 38–40

LMAC Lower MAC. xi, 18

LTE Long Term Evolution. xi, 13

LTE-V LTE-Vehicular. xi, 13, 14

MAC Medium Access Control. ii, xi, xii, 3, 6, 14, 15, 18, 34, 36–38, 46, 48

mmWave Millimeter Wave. xi, 14

OBD On-Board Diagnostics. xi, 16, 18

OBU On-Board Unit. ii, v, xi, xii, 4–6, 16, 18, 29, 33, 38–41, 43, 45, 48, 49

OFDM Orthogonal Frequency-Division Multiplexing. xi, 15, 18

PC Personal Computer. xi, 18

PER Packet Error Rate. xi, 34

PHY Physical. xi, 14, 18

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analyses. v, xi, 21, 24, 48

PSD Power Spectral Density. xi, 34, 36

QAM Quadrature Amplitude Modulation. xi, 15

QPSK Quadrature Phase Shift Keying. xi, 15

RF Radio Frequency. xi, 18, 28

RSSI Received Signal Strength Indicator. xi, 29

RSU Road-Side Unit. ii, v, xi, 4–6, 16, 28, 29, 33, 37–46, 48, 49

SBC Single Board Computer. xi, 16, 18

SCH Service Channel. xi, 15

SINR Signal-to-Interference-plus-Noise Ratio. xi, 34

SOW Synchronous OBU Window. xi, 38–40

TDMA Time Division Multiple Access. xi, 5, 6, 37–39

UAV Unmanned Aerial Vehicle. xi, 49

UMAC Upper MAC. xi, 18

USB Universal Serial Bus. xi, 16, 18

V2I Vehicle-to-Infrastructure. xi, 13

V2V Vehicle-to-Vehicle. xi, 13, 14

VANET Vehicular Ad-hoc NETwork. xi, 2–4

V-FTT Vehicular-FTT. ii, v, xi, 38–40, 44, 46

VLC Visible Light Communications. xi, 13

VTL Virtual Traffic Light. xi, 29

WAVE Wireless Access in Vehicular Environments. v, xi, 3, 14–16, 18, 34, 36, 47

WHO World Health Organization. xi, 1

CHAPTER 1

Introduction

This chapter presents the scope and motivation for the realization of this work, as well as a brief description of the thesis contribution. At the end of the chapter, the document organization for the rest of the dissertation is also presented.

1.1 Scope and Motivation

There are over 1.2 million fatalities each year from road traffic accidents, being one of the major causes of death worldwide [1]. According to the World Health Organization (WHO)'s data, a traffic crash is the most likely cause of death for a young person aged 15-29 years. Intelligent Transportation Systems (ITS) have been developed in the last few decades with the main goal of modifying this scenario, so that the number of accidents, injuries and fatalities can be drastically reduced. In conjunction with other factors, such as the improvements on road infrastructure, technological innovation in vehicle's system design has contributed to a steady decrease in the number of victims in the recent years [2]. Notable examples of such introduced functionalities are the Anti-lock Braking System (ABS) and the airbag. However, the objective already established in some developed countries is even more ambitious. The envisioned strategy, known as "Vision Zero" [3], aims to completely eliminate the fatalities and serious injuries caused by road crashes. The initiative started in Sweden and has already influenced the road safety agendas and action plans of other nations and cities.

In this context, Cooperative ITS (C-ITS) can play a decisive role since they allow road users to collaboratively interact, thus avoiding dangerous traffic situations. From a safety perspective, C-ITS have the ability to improve traffic awareness of pedestrians, cyclists, drivers and vehicles themselves (in case of autonomous driving), by extending theirs fields of view and producing warning alerts in the presence of hazardous conditions. Besides safety applications, C-ITS may contribute to achieve sustainability goals, e.g. decrease CO2 emissions, road congestions and energy consumption. Infotainment applications based on C-ITS can also be developed, in order to improve passenger's comfort and to provide a better riding and driving experience.

These collaborative systems will need a way to communicate and currently, Vehicular Adhoc NETworks (VANETs) constitute the main enabling technology behind these applications. Vehicular communications are indeed able to support the development of these services, since they allow vehicles to communicate among each other, to exchange information with the road-side infrastructure and eventually with pedestrians, cyclists and other objects located close to the roads. This is the essential concept behind Internet of Vehicles (IoV) [4], which constitutes a subgroup of the future Internet of Things (IoT). In the IoV framework, at least a significant percentage of vehicles will be equipped with these communications capabilities, and will be able for instance to disseminate an accident detection, avoiding further chain collisions. Another advantage is that vehicles will be connected with other networks, for example with the sensors network of the driver's home, allowing him/her to remotely control the heat or air conditioning systems, the garage door, the lightning and surveillance systems [5]. There is a myriad of possible services, including Electronic Fee Collection (EFC) systems for automatic payment of tolling plazas, parking lots or gas stations, Cooperative Adaptive Cruise Control (CACC) or platooning applications through which vehicles are able to travel very close to each other, thus optimizing traffic efficiency and reducing air drag so a significant amount of fuel can be saved.

During a transitory market penetration period, vehicular communication systems will be regarded as an auxiliary technology that could aid drivers to take more informed decisions and provide warnings regarding dangerous situations. However, after this initial phase, and with the advent of autonomous vehicles, road traffic systems will necessarily rely on the information provided by this and other technologies (such as cameras and radars). At that stage of development, the human judgement, which is very prone to error, will likely be replaced by computer-driven decisions. In this scenario, dependability will be an essential aspect in road traffic safety systems, since their operation will strongly depend on the correct service provided by vehicular communication devices. Based on these arguments, vehicular networks must be analysed as Distributed Computer Control Systems (DCCSs), in which nodes interact together to achieve the common goal of guaranteeing traffic safety.

In the last few decades, DCCSs have been widely used in many application fields, such as robotics, industrial process control, avionics and automotive systems. A large number of these applications pose strict timing requirements, which if not fulfilled may cause important economic and environmental losses or even put human life in danger [6]. These systems must exhibit a high probability to provide continuous correct service. Beyond that, many of them comprise real-time activities that must be performed within stringent time bounds. Therefore, in safety-critical DCCSs with real-time constraints, such dependability attributes are of uttermost importance, since its distributed nature requires a timely and reliable exchange of data among the several nodes, in order to achieve the envisaged control over the operating environment.

These concerns are already being taken into consideration in the development of the next generation of mobile networks, known as 5G. In fact, 5G holds the promise to enable new wireless applications, including the operation of dependable and real-time safety-critical systems. The target requirements of small latency (round trip times lower than 1 ms) and high reliability and availability levels ($> 99.999\%$) envisioned by the 5G community [7], will provide the basis for the Tactile Internet (real-time cyber-physical control) and will enable the operation of mission-critical systems (e.g. remote surgery), advanced industrial automation, smart grid management, etc. [8]. C-ITSs and in particular vehicular networks are also among those promising 5G-enabled applications, however a lot of research is still needed to achieve the required strict latency and dependability values.

1.2 The Problem

Safety-critical vehicular applications are inherently hard real-time systems for which the failure of meeting a deadline can lead to severe damage and pose significant threat to human life [9]. The first few steps in attempting to provide the necessary quality of service were given by acknowledging that vehicular communications require specifically designed communication systems in order to cope with high network dynamics and short connection times [10]. Some standards attempting to solve these issues were developed, namely the IEEE WAVE and ETSI ITS-G5 protocol stacks, both based on the same IEEE 802.11 physical layer [11] but containing specific features tailored to vehicular environments, such as: reduced bandwidth channels, increased maximum power and segregated frequency bands. For instance, double timing parameters are utilized, in order to achieve less interference due to the multi-path propagation and the Doppler shift effect. Another example is the introduction of non-Internet Protocol (IP) messages that operate outside the context of a Basic Service Set (BSS), enabling faster packet transmission by avoiding the registration and authentication procedures, commonly present in typical wireless local area networks. In exchange of this lower overhead however, security issues become more critical.

Despite the use of dedicated spectrum and specifically designed protocols, the current standards governing VANETs still fall short of providing dependable communications, as desirable if this technology is to be used in support of safety applications. In fact, the design of dependable VANETs requires innovative solutions in order to overcome the inherent problems of wireless environments, such as unpredictable channel conditions, dynamic network topologies, spectrum interference and so forth. For instance, notwithstanding the designation of a specific channel for safety purposes, there are still concerns about data traffic congestion in the wireless medium [12] [13]. This is one of the most serious problems in VANETs [14], since it affects the timeliness and dependability of the exchanged messages. These congestion control issues arise in the Medium Access Control (MAC) layer defined in IEEE 802.11 standard, which adopts a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. In a wireless medium ruled by this CSMA/CA technique, packet collisions may occur indefinitely, due to the non-determinism of the back-off mechanism. Therefore, native IEEE 802.11 alone does not support real-time communications. However, this property is crucial for safety applications, where warning messages have to be always delivered within a bounded delay, i.e. before a predefined deadline.

Moreover, system components and vehicular network nodes may be affected by different failure events, specially due to the stressful conditions in which they operate, i.e. it is not a static and quiet environment. As a result, several types of faults must be considered in vehicular scenarios. For example, the wireless channel is regularly affected by transient faults in the communication link due to cross channel interference or the constantly changing atmospheric and road traffic conditions. These effects are much larger than the ones observed for instance in wired or indoor wireless environments. Furthermore, channel permanent faults could also occur, due to unregulated interference, which can typically be considered as malicious faults, since the spectrum band assigned for wireless vehicular communications is reserved by law. Not only the wireless channel, which is a single point of failure in vehicular systems, but also the nodes of the network should be regarded as a possible source of problems. For instance, hardware and software faults can affect the operation of either the Road-Side Units (RSUs) that constitute the network infrastructure or the On-Board Units (OBUs) placed inside each vehicle. In safety-critical scenarios, such faults (either malicious or resulting from malfunctions) may compromise the operation of the entire system, causing a catastrophic event with irreversible damage.

For the given reasons, a careful design work must be performed in the deployment of vehicular communications systems, by taking into consideration the general dependability aspects of safety-critical applications, as well as the specific issues that arise in the vehicular context. As it is the case for many others DCCSs, due to the non-deterministic behaviour of the environment where VANETs operate, the use of the best design's practices does not fully guarantee the absence of faults. Thus, fault-tolerance methods need to be included in the system operation to avoid that possible faults can cause its failure. By combining these kind of mechanisms with system's real-time requirements, dependable vehicular communications systems can be developed for operating in safety-critical scenarios.

1.3 The Thesis

The thesis supported by the research work performed in the scope of this PhD argues that: *In order to prevent error propagation in vehicular communications systems and to tolerate faults in the most critical elements of the network, fault-tolerance concepts and techniques can be successfully applied. This can be achieved without compromising the required system's flexibility and the real-time operation of wireless vehicular networks.*

1.4 Original Contributions

This dissertation is based on work presented in five papers published in several journals and conferences in the research field of this thesis and containing original contributions to the state-of-the-art.

Paper A - Mitigating Adjacent Channel Interference in Vehicular Communication Systems (by J. Almeida, M. Alam, J. Ferreira and A. S. R. Oliveira, in *Digital Communications and Networks*) presents a digital filter to mitigate the effects of Cross Channel

Interference (CCI) in the receiver nodes of wireless vehicular networks. The proposed Finite Impulse Response (FIR) filter relies on modern digital signal processing techniques, such as polyphase decomposition and multi-rate systems, in order to achieve a strong attenuation of the interfering signals, while keeping a low-delay message decoding at the reception chain. The design of the two-stage low-pass filter took place based on actual measurements of the Adjacent Channel Interference (ACI) effect captured in a laboratory environment.

The filter was tested and evaluated in MATLAB® and the obtained results prove the effectiveness of the proposed scheme in mitigating interference from adjacent channel transmissions. Moreover, the multi-rate approach followed during the design phase, allows an efficient implementation of the filter in an Field Programmable Gate Array (FPGA).

Paper B - Fail Silence Mechanism for Dependable Vehicular Communications (by J. Almeida, J. Ferreira and A. S. R. Oliveira, in *International Journal of High Performance Computing and Networking*) introduces a fault-tolerant architecture to improve the dependability attributes of infrastructure-based vehicular networks. In the proposed scheme, the RSUs behave as the master nodes of the network, being responsible for all the transmission scheduling and admission control policies. A real-time communications protocol based on Time Division Multiple Access (TDMA) is utilized, with the goal of guarantee deterministic behaviour of the OBU nodes. In this way, messages are transmitted at predefined time slots, avoiding packet collisions in the wireless medium. In addition to this real-time protocol, several mechanisms are employed in order to achieve higher reliability and availability levels in the network operation. This group of mechanisms constitute the fault-tolerant architecture mentioned above.

In particular, this paper focuses on the design of a fail silence mechanism for the RSU devices. The main goal of this mechanism is to guarantee fail-silent behaviour to the master nodes of the network. By ensuring that RSUs only transmit correct information or no information at all, it is possible to apply replication strategies to these nodes, which are responsible for crucial tasks in the network operation.

Paper C - An RSU Replication Scheme for Dependable Wireless Vehicular Networks (by J. Almeida, J. Ferreira and A. S. R. Oliveira, in *EDCC 2016 - 12th European Dependable Computing Conference*) proposes an active replication scheme for the RSU nodes, in order to overcome a possible failure in the device's operation. Given the presence of the fail silence mechanism previously described, an RSU node may only exhibit the fail silence failure mode. As a result, the design of a replication scheme for these units becomes simplified, since the failure detector only needs to monitor the primary node's operation and identify when it stops sending messages. This task is relatively easy to implement, given the fact that RSUs periodically transmit messages at predefined instants, according to the real-time protocol.

After the fail-silent failure has been detected by the backup RSU, this redundant unit immediately replaces the operation of the faulty node. This recovery procedure is executed within a short time period, in order to fulfil the real-time requirements of the network protocol. The omitted message is transmitted only with a small delay by the backup node, causing no interference in the communications schedule.

Paper D - Timing Analysis of an Active Replication Scheme for the Road Side Units of Vehicular Networks (by J. Almeida, M. Alam, J. Ferreira and A. S. R. Oliveira, in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*) performs a detailed timing analysis of the active replication scheme previously mentioned. The impact of a primary RSU failure in the real-time communications protocol is carefully examined. The recovery procedure of a faulty RSU is studied under different circumstances, both for single and multiple RSUs scenarios. The critical parameter under analysis is the Inter-Frame Space (IFS) between consecutive transmissions, whose value is small enough in the real-time protocol, in order to create a TDMA-based contention-free period.

The results obtained in this study show that even in the presence of a primary RSU failure, this IFS value can be kept sufficiently small, thus guaranteeing the deterministic operation of the MAC protocol. However, in case of simultaneous failures of multiple primary RSUs, that condition does not hold any longer. As a result, several possible strategies are discussed in order to overcome this issue.

Paper E - A Medium Guardian for Enhanced Dependability in Safety-Critical Wireless Systems (by J. Almeida, J. Ferreira and A. S. R. Oliveira, in *IEEE Transactions on Intelligent Transportation Systems*) presents a novel technique to guarantee fail-silent behaviour in wireless communications systems. The proposed mechanism, named medium guardian, is inspired in the bus guardian concept originally developed for fieldbus technologies. The main objective of the medium guardian is to ensure that messages sent by a wireless node, are valid both in value and time domains. In certain scenarios, the frequency domain could also be verified. This way, it is possible to assure that packets exchanged in the wireless medium are correct and faults in a node do not interfere with the remaining communications taking place in the channel.

In this paper, the medium guardian concept is generically described and the use case scenario of wireless vehicular communications is utilized to demonstrate the pertinence and effectiveness of this method. A medium guardian architecture is designed and a practical implementation is developed to monitor the operation of a OBU node in the real-time framework described above. The introduction of medium guardians in the mobile nodes (OBUs) of the vehicular network is also part of the proposed fault-tolerant architecture. The guardian constitutes a less expensive solution than the replication scheme employed in the RSU nodes, however it provides a smaller fault coverage. This option can be justified by the crucial role played by the RSUs in network coordination and admission control mechanisms.

1.5 Document Organization

The rest of the dissertation is organized as follows:

- **Chapter 2 - Dependability Concepts and Wireless Vehicular Communications -** This chapter provides the background concepts for the realization of this PhD thesis. The basic topics of dependability and vehicular networks are summarized in this part of the dissertation, in order to introduce the research work described in the remaining chapters.

- **Chapter 3 - A Survey on Fault-Tolerance Techniques for Vehicular Networks -** A survey on fault detection and fault tolerance mechanisms for wireless vehicular communications is presented in this chapter. The publications listed and analysed in this survey are the result of a systematic review process of the literature.
- **Chapter 4 - Fault-Tolerant Architecture for Dependable Vehicular Communications -** This chapter presents in a structured manner the main contributions reported in the appended papers. A fault tolerant architecture for infrastructure based vehicular networks is described, including the distinct mechanisms that were proposed during the course of this thesis, in order to enhance dependability in safety-critical vehicular communications.
- **Chapter 5 - Conclusions and Future Work -** The main conclusions of this thesis are summarized in this final chapter. Additionally, some possible future research work in the field is also presented.

CHAPTER 2

Dependability Concepts and Wireless Vehicular Communications

This chapter presents an overview of some basic dependability concepts, as well as the background in the area of wireless vehicular communications.

2.1 Dependability and Real-Time Communications

Dependability aspects are of uttermost importance in the operation of distributed real-time systems. Such systems must present trustworthy behaviour without compromising the necessary operational flexibility. This way, it is possible to guarantee the provision of safety-critical services. In the following, these concepts will be discussed in greater detail.

2.1.1 Distributed Systems

A distributed system can be defined as a system composed by several processing units that communicate through a network in order to execute a set of activities in a distributed manner. As opposed to centralized systems, where all the computing is performed in a single central entity, in distributed systems a set of interconnected nodes cooperate and exchange information in order to achieve a common goal. Some typical examples of distributed systems are peer-to-peer networks, automated industrial lines and aircraft control systems[15].

The communications network is one of the most important elements of a distributed system. It enables nodes, which can be deployed in geographically separate locations, to synchronize and exchange information and thus cooperate. Such important component must be designed with utmost care. If the network is overloaded (i.e. system resources demand exceeds the maximum available) or isn't able to fulfil the specific requirements of each communication stream (e.g. packet delay, drop rate), the system may experience a performance degradation and in the worst case, a partial or global system failure (i.e. a part or the whole system may be unable to communicate effectively and thus, unable to operate properly) [15] [16].

2.1.2 Real-Time Systems

In some occasions, distributed systems may present timeliness requirements that are dictated by the environment in which they operate. Since the environment has inherent temporal dynamics, in order to properly interact with it, these systems not only have to produce logically correct solutions but also need to apply them within specified time intervals. Systems where the correctness of the system behaviour depends on both the logical computations and the time instant when they are produced and applied, are called real-time systems [17]. These systems can be found for instance, in industrial automation, flight control systems, automotive or military applications.

Real-time systems are usually composed by computational tasks which implement specific functionalities and have stringent timing constraints that must be met in order to achieve proper behaviour. A typical constraint on a task is the deadline, i.e the instant before which a task should complete its execution without impairing the system. Depending on the effects of a missed deadline, tasks can be categorized as [17]:

- **Non real-time:** task has no time constraints and always contributes to the system whenever it finishes its execution;
- **Soft:** task's output still has some utility to the system after missing its deadline, however, the system's performance is degraded;
- **Firm:** task's output has no utility to the system after a deadline miss, however it does not cause catastrophic consequences on the system behaviour;
- **Hard:** task only contributes to the system if it finishes within its deadline. A deadline miss may cause catastrophic consequences, e.g. overall system failure with human and/or material losses.

Real-time systems can be categorized as soft or hard according to the supported task types and the consequences raised by deadline misses [17], [6]:

- **Soft Real-Time Systems:** Systems that only integrate soft and/or firm tasks are categorized as soft real-time. In these systems, deadline misses may induce overall performance degradation without catastrophic consequences. A typical example for this type of system is video and sound streaming in which a deadline miss typically results in minor image/sound glitches.
- **Hard Real-Time Systems:** Systems that contain at least one hard task are categorized as hard real-time. In these systems, a deadline miss may result in a system failure with catastrophic effects, e.g. material and/or human losses. A typical example for this type of system is a nuclear power plant control in which a deadline miss could result in the failure of the nuclear reactor.

As stated earlier, proper temporal behaviour is required for the correct operation of real-time distributed systems. The temporal behaviour of the whole system depends on several elements such as the node's software, e.g. running tasks, behaviour and the capacity of the underlying communication system to provide timely delivery of messages. Communication systems capable of delivering messages within specific temporal constraints are known as real-time communication systems [6].

2.1.3 Dependability

Dependability is a generic concept that describes the level of trust one can have in the operation of a system. According to Laprie *et al.* [19] [18], dependability can be divided in 3 different classes of notions - attributes, threats and means - as presented in figure 2.1.

The attributes of dependability denote different properties that can be expected from a dependable system, whose importance can vary between distinct applications:

- **Availability** is defined as the readiness to provide a correct service.
- **Reliability** is the probability of a system to present continuous correct service.
- **Safety** is defined as the absence of tragic consequences on the operating environment.
- **Integrity** is the absence of improper system alterations.
- **Maintainability** is defined as the capacity of the system to undergo modifications and repairs.

The impairments or threats are the undesired circumstances that can prevent a system from being dependable. There are typically three main terms associated with the threats to dependability: faults, errors and failures. A fault is a defect in the design or in the operation of the system that can lead to an error. An error is an incorrect value of the total system state that may cause a failure. Finally, a failure is an event that occurs when the delivered service of the system presents some deviation relatively to the correct behaviour.

During the design of safety-critical systems, several means or techniques can be used to attain the various attributes of dependability. The purpose of these techniques is to reduce the impact of faults in the overall system's operation:

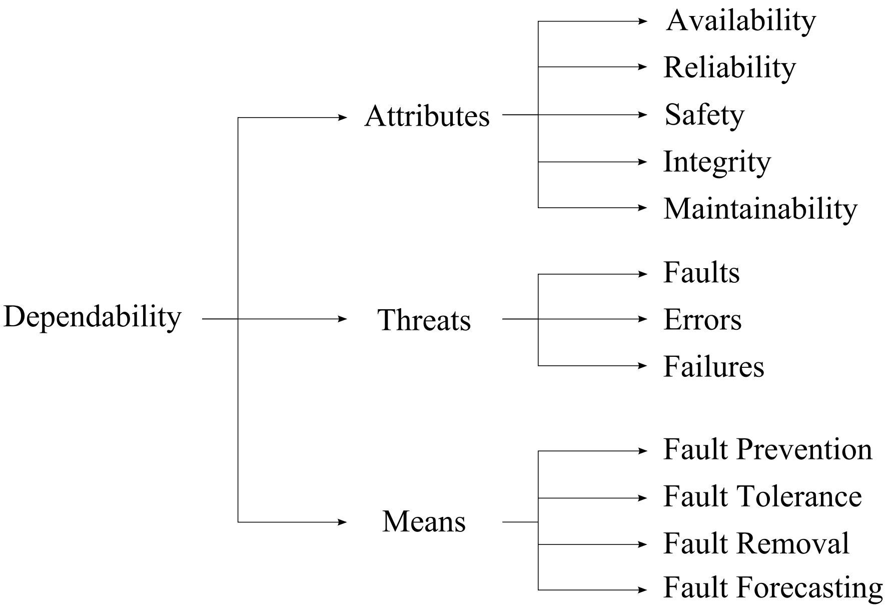


Figure 2.1: The dependability tree, according to Avizienis *et al.* [18].

- **Fault prevention** deals with preventing faults from occurring or being introduced in the system.
- **Fault tolerance** comprises methods to avoid system failures and the provision of service complying with its specifications even under the presence of faults.
- **Fault removal** techniques aim to reduce the number and severity of faults.
- **Fault forecasting** methods try to detect the present number of faults in the system, as well as their future occurrence and consequences.

2.1.4 Fault Tolerance

The different techniques are indeed complementary, since in order to achieve the target dependability levels, distinct mechanisms need to be applied. For instance, the use of the best design's practices typically does not guarantee the full absence of faults, thus fault-tolerance techniques are normaly required. In most cases, efforts to completely prevent (fault prevention) or remove faults (fault removal) are imperfect, too restrictive for system's flexibility or prohibitively expensive. Nevertheless, these mechanisms must be properly implemented, so that only residual design faults need to be dealt by fault tolerance mechanisms.

The main goal of fault tolerance is to avoid failures even under the presence of faults. Fault-tolerance techniques are commonly classified into two main categories: error detection and system recovery [18]. Both groups of techniques are necessary to tolerate faults arising during system's operation. Error detection deals with the correct identification of an error in the system, while recovery methods aim to modify the state of a system presenting errors and faults, to a scenario with no detected errors and without faults that can be activated again.

Fault tolerance in safety-critical communications needs to take into consideration the hard real-time guarantees and the required system's flexibility in such dynamic environments. For that reason, in this scenario certain fault-tolerance techniques are more suitable than others. For example, concurrent error detection methods and system recovery strategies based on error compensation mechanisms, can usually provide appropriate solutions under these circumstances.

In communications networks, it is important to handle faults both in the network nodes and in the communications channel. Fault tolerant communications aim to guarantee that two or more network nodes can exchange information in spite of faults that may affect the communications link or some of the participating nodes. Several fault tolerance techniques can be found in the literature and are widely disseminated in the system's design and network architecture. Notable examples are voting schemes, N-version programming, hardware replication, etc. All of these mechanisms have in common the fact that they are based on some type of redundancy.

2.1.5 Types of Redundancy

Redundancy consists in utilizing more resources than the ones required in the case of a fault free scenario. A system presenting fault tolerance capabilities typically involves redundancy and diversity techniques. This way, it is possible to avoid the presence of single points of failure in the system and to prevent common-mode failures. Redundancy corresponds to an increment in resource utilization (mainly replication), in order to provide resilience against faults arising in the system. Traditionally, redundancy techniques can be classified in three main groups:

- **Temporal redundancy** is characterized by the attempt to deliver the same information at multiple moments in time. Retransmission based protocols, such as TCP, are clear examples of this strategy.
- **Information redundancy** corresponds to the use of additional data, so that information can still be retrieved in case of partial data loss. For instance, error correction codes require the transmission of redundant data in order to recover the contents of the exchanged message.
- **Spatial redundancy** refers to the possibility of providing the same information from different sources. Hardware replication constitutes a traditional example of spatial redundancy, where several replicas are able to deliver the same service.

Redundancy may also be categorized in terms of protocol stack layer in which it is applied. For instance, redundant channel links can be classified as physical layer redundancy. As a result, the distinct strategies may be categorized based on the OSI levels. Cross-layer solutions are also possible, covering faults in a set of different layers of the protocol stack. For example, entire node replication, from the RF antenna up to the application level, constitutes one of these cases.

2.2 Wireless Vehicular Communications

As already mentioned in chapter 1, vehicular communications are an important field of research in the area of Intelligent Transportation Systems. Future ITS will need wireless communications among vehicles and between vehicles and the road side infrastructure. Vehicular communication systems can be more effective in preventing road accidents than the case where vehicles work individually to achieve the same goal. This is due to the cooperative techniques that can be exploited when vehicles and the roadside stations possess information about others parties' situation (e.g. location, speed and heading). As an example of this class of safety applications, chain collisions could be avoided if the information about the first crash is disseminated by all the other nodes in the vicinity of the accident.

Several technologies have been proposed to support the exchange of information between different nodes of a vehicular network. Some examples are GSM and ZigBee [20], Bluetooth Low Energy (BLE) [21] and Visible Light Communications (VLC) [22]. Currently however, the most commonly accepted technology by the different stakeholders worldwide (standardization institutes, car manufacturers, motorway operators, etc.) is based on Dedicated Short Range Communications (DSRC). DSRC have been designed to support a variety of safety applications and infotainment services based on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. This technology has been developed for more than a decade, with field trials being carried out in different scenarios [23] [24]. At this moment, DSRC based systems are mature and ready for initial market penetration with clear safety benefits. More recently, other alternatives, such as LTE-Vehicular (LTE-V) or Fifth Generation (5G), have received special attention from the scientific community, industry and standardization bodies [25]. Originally, LTE standard was designed for cellular networks, thus not taking into consideration Device-to-Device (D2D) link requirements. However this concept was recently introduced in the new releases (LTE-V), making it possible to support side-link or V2V communications [26] [27]. Despite the current recognition of DSRC as the most promising candidate for initial vehicular network deployment, 5G is regarded as the future vehicular communications technology, namely by the 5G Automotive Association (5GAA), a cross-industry organization from automotive, technology and telecommunications industries, including for instance AUDI, BMW, Ericsson, Huawei, Intel and Nokia [28]. According to the latest perspectives, Millimeter Waves (mmWaves) will constitute the basis of 5G technology and will enable the exchange of massive automotive sensory information, including e.g. fine-grade object detection, real-time road video and high resolution maps [29].

Given the current importance of DSRC systems, the contributions made during the execution of this PhD thesis were developed with a particular focus on this technology, albeit the fact that these can be applied or easily adapted to any other wireless technology. For that reason, DSRC standards are described in more detail next.

2.2.1 DSRC Standards for Vehicular Networks

There are two main reference protocol stacks for vehicular networks based on DSRC systems, one developed by the Institute of Electrical and Electronics Engineers (IEEE) and the other one from European Telecommunications Standards Institute (ETSI). The IEEE protocol stack was initially introduced in America and later ETSI proposed a similar framework in Europe. Both of them are illustrated in figure 2.2.

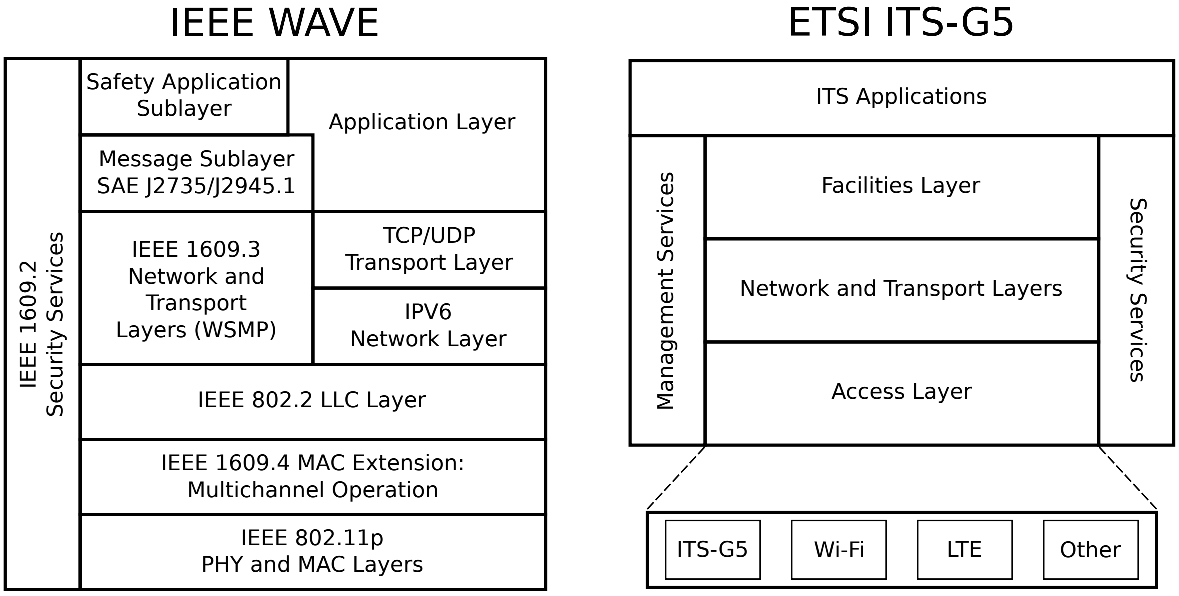

IEEE WAVE
IEEE 1609.2 Security Services
Safety Application Sublayer
Application Layer
Message Sublayer SAE J2735/J2945.1
IEEE 1609.3 Network and Transport Layers (WSMP)
TCP/UDP Transport Layer
IPV6 Network Layer
IEEE 802.2 LLC Layer
IEEE 1609.4 MAC Extension: Multichannel Operation
IEEE 802.11p PHY and MAC Layers
ETSI ITS-G5
ITS Applications
Management Services
Facilities Layer
Network and Transport Layers
Access Layer
Security Services
ITS-G5
Wi-Fi
LTE
Other

Figure 2.2: IEEE WAVE and ETSI ITS-G5 protocol stacks.

The protocol stack in America is denominated as IEEE Wireless Access in Vehicular Environments (WAVE), while the one in Europe is referred as ETSI ITS-G5. Both of them rely on IEEE 802.11p, from the IEEE 802.11 family of Wi-Fi standards, for the implementation of their Physical (PHY) and MAC layers [11]. The physical layer is almost identical to IEEE 802.11a, using also OFDM with BPSK, QPSK, 16-QAM and 64-QAM modulations, but with double timing parameters to achieve less interference due to the multi-path propagation and the Doppler shift effect. With double timing parameters, the channel bandwidth is 10 MHz instead of 20 MHz, and the data rate is half, i.e., 3...27 Mbit/s instead of 6...54 Mbit/s.

The MAC layer adopts a CSMA/CA, as IEEE 802.11a, but it is adjusted for the vehicular communication environments, which differ significantly from the sparse and low-velocity characteristics of a traditional Wi-Fi deployment. In vehicular environments, nodes present high mobility, some areas are often densely populated and frequently there is non-line-of-sight. As a consequence, some tweaks were introduced in the standard to allow low overhead operations, in order to guarantee fast and reliable exchange of safety messages. For example, non-IP messages that operate outside the context of a BSS were defined, enabling quick transmission of packets by avoiding the registration and authentication procedures, commonly present in typical wireless local area networks.

The Federal Communications Commission (FCC) in the United States and the European Conference of Postal and Telecommunications Administrations (CEPT) allocated a dedicated spectrum band at 5.9 GHz (figure 2.3). In America, a bandwidth of 75 MHz was reserved, while in Europe only 50 MHz were assigned. This spectrum was divided into smaller 10 MHz wide channels and in the American case, a 5 MHz guard band at the low end was also included. As a result, there are 7 different channels for IEEE WAVE operation and 5 for the case of ETSI ITS-G5.

In Europe, 30 MHz (3 channels) are reserved for road safety in the ETSI ITS-G5A band and 20 MHz are assigned for general purpose ITS services in the ETSI ITS-G5B band. As a general rule, a Control Channel (CCH) (the number 178 in the United States and the

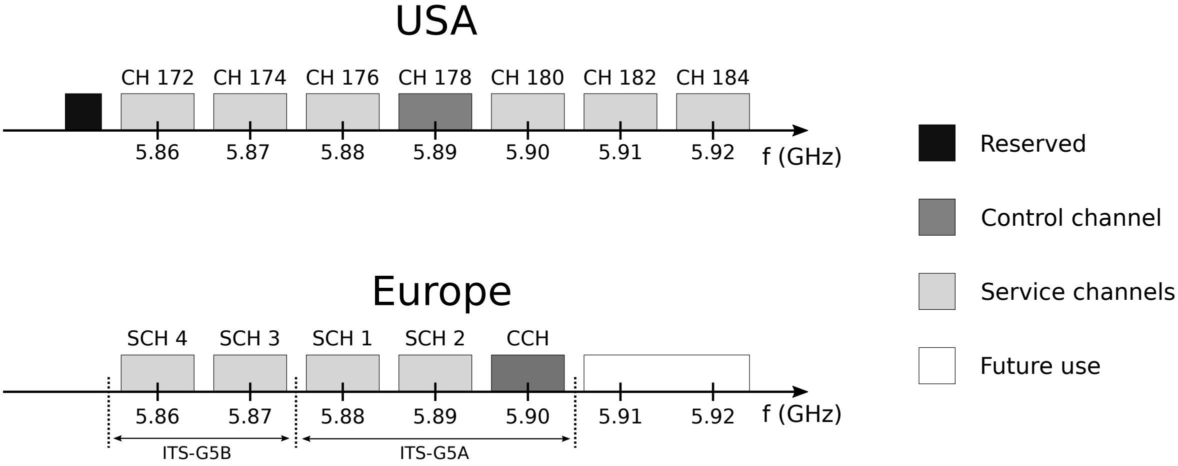


Figure 2.3: Spectrum allocation for vehicular communications in the United States and Europe.

180 in Europe) is exclusively used for cooperative road safety and control information. The remaining channels are designated as Service Channels (SCHs). In the United States, concerns about the reduced capacity for road safety messages led to the decision to allocate SCH 172 specifically for applications regarding public safety of life and property.

The ETSI-G5 standard defines two basic types of messages that support the operation of safety applications. The Cooperative Awareness Messages (CAMs) are periodic beacons that are transmitted with a frequency rate between 1 to 10 Hz and that comprise essential data about current vehicle's state, e.g. location, speed and orientation. On the other hand, the Decentralized Environmental Notification Messages (DENMs) are event-triggered packets that contain information regarding a road hazard or an abnormal traffic condition.

2.2.2 IT2S Platform

A custom IEEE WAVE / ETSI ITS-G5 station was developed at Instituto de Telecomunicações - Aveiro site [30], prior to this PhD work. Due to the high flexibility, reconfigurability and low-level control of both software and hardware components, this platform was utilized to implement, test and validate the experimental work of this thesis.

The general architecture of this station, named IT2S platform, is composed by the main blocks and interconnections presented in figure 2.4. There are three key physical components, namely the IT2S board, the Single Board Computer (SBC) and the Smartphone, which are responsible for executing specific tasks and for implementing different layers of the protocol stack. The communication between the Smartphone, the SBC and the IT2S board is ensured through USB links. Furthermore, there are external interfaces to systems outside the IT2S platform, such as the On-Board Diagnostics (OBD)-II system available in all recent vehicles. The remaining external connections include the GPS and the DSRC 5.9 GHz antennas in the IT2S board, the Ethernet ports in the SBC and the 3G/4G interfaces in the Smartphone.

The IT2S platform can operate either as an RSU or as an OBU. When the platform is working as an RSU, there is no need for a graphical user interface, and therefore the Smartphone is not included in the overall system's architecture. Moreover, if there are several RSUs placed along the road, the network operator will probably desire to remotely access those units or to make them working cooperatively. As a result, a back-hauling network will be required to exchange information among RSUs or between an RSU and a gateway node. In the case of IT2S platform, the Ethernet interface available in the SBC can be used for this purpose.

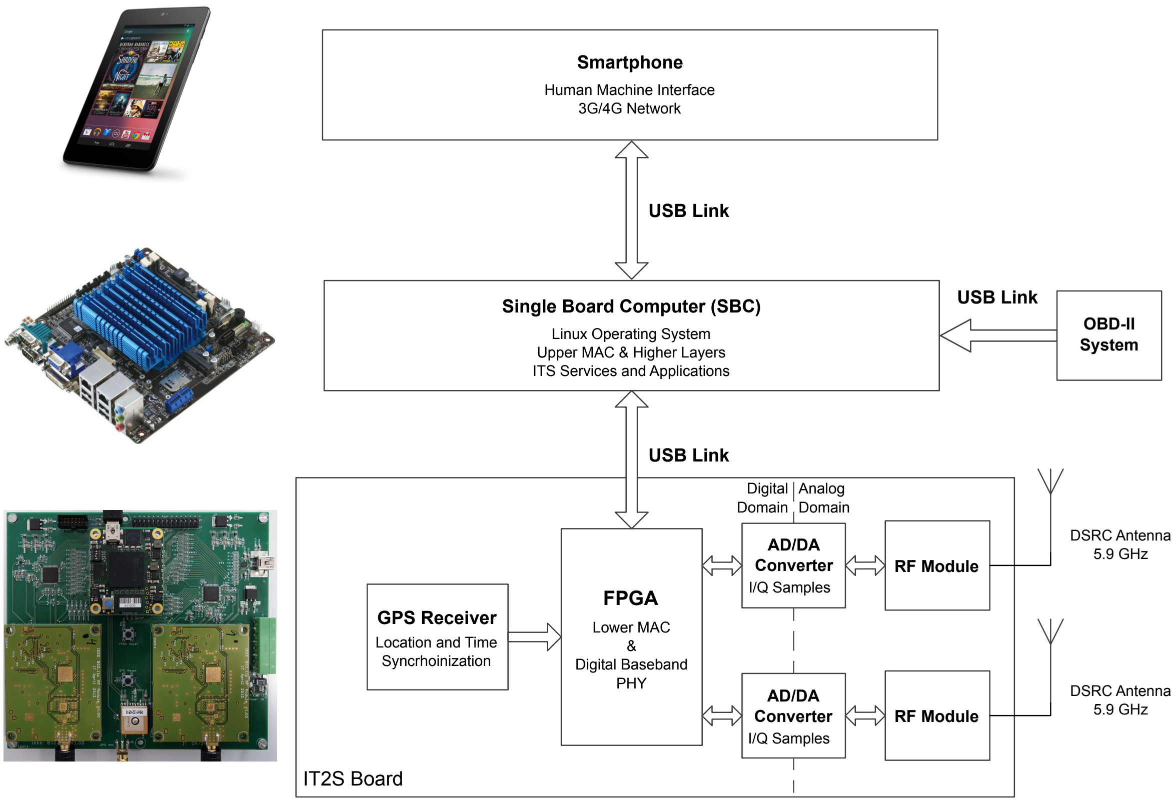


Figure 2.4: IT2S Platform architecture.

Smartphone

The Smartphone is responsible for implementing the graphical user interface with the vehicle's driver and passengers. For instance, it should be able to display warnings in case of road accidents or traffic congestions. Another important advantage of the Smartphone is its capability to provide connectivity between the IT2S platform and a Third Generation (3G) or Fourth Generation (4G) network. This feature allows the remote diagnostics and access to the information available in the platform, as well as a possible upgrade of the software and the reconfiguration of the bitstream in the FPGA. Finally, it could also enable the implementation of the Emergency Call (eCall) service, which basically consists in an automatic call to the 112 emergency number in the event of a serious road accident.

Single Board Computer

As already mentioned, the main function of the SBC is to execute the higher layers of the WAVE / ITS-G5 protocol stack, namely from the high level functionalities of the MAC layer, called Upper MAC (UMAC), to the Application layer. The SBC is a Commercial-Off-the-Shelf (COTS) embedded PC (e.g. Aaeon EMB-CV1) that runs a Linux-based operating system, providing a high degree of flexibility and more control over the system's operation. When operating as an OBU, the SBC can also interact with the OBD-II system available in all recent vehicles. This way, it can access detailed information about vehicle's status and performance.

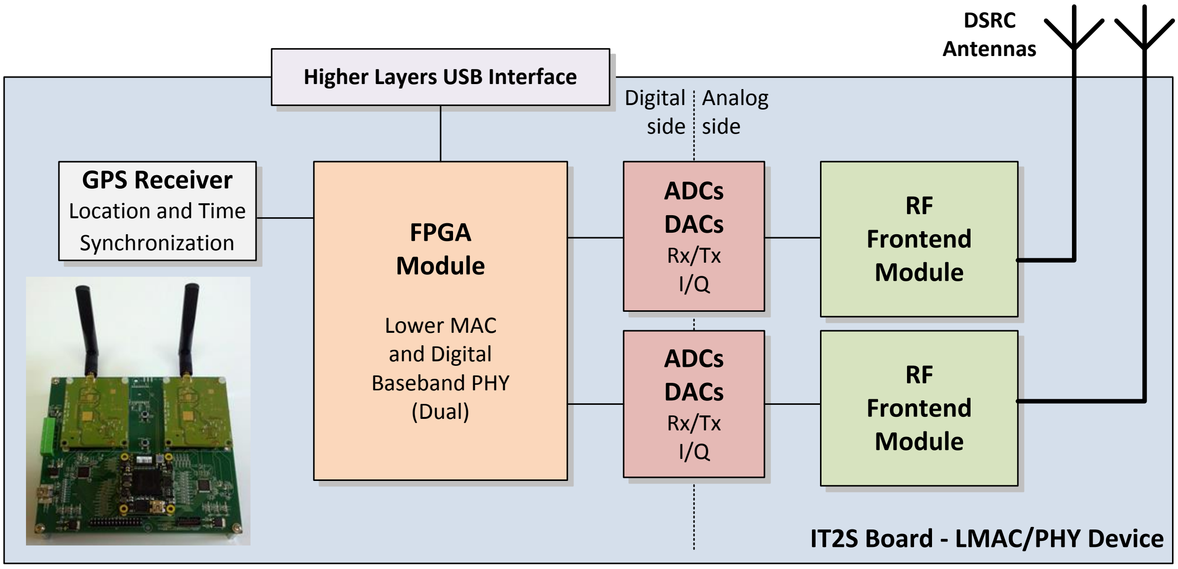


Figure 2.5: IT2S Board Architecture.

IT2S Board

The IT2S board (figure 2.5) is the core module of this platform, since it is not based on a commercial solution, but in a device completely developed from scratch at Instituto de Telecomunicações (Aveiro site). It implements the recent IEEE 802.11p standard, focused on the MAC and Physical layers of the protocol stack. However, since the implementation of the MAC layer resides in a hardware/software partition co-design, only the low level functionalities are executed in the IT2S board by the FPGA. This sub-layer that comprises the time-critical and deterministic operations of the MAC scheme, is designated as Lower MAC (LMAC).

The physical layer is completely implemented in the IT2S board, being divided in two main parts: the Analog and the Digital PHY. The Analog PHY is responsible for the signal processing operations in the analog domain, such as the up and down conversion from baseband to RF and vice-versa, respectively. On the other hand, the Digital PHY deals with signals in the digital domain, implementing the OFDM transmission and reception chains, converting bytes from a MAC frame into baseband In-phase and Quadrature (I/Q) samples and the reverse operation.

In order to cope with the simultaneous multi-channel operation requirement, the board includes two complete sets of hardware units (2 DSRC antennas and RF modules, 2 Analog-to-Digital/Digital-to-Analog (AD/DA) processors and 2 digital PHY and LMAC modules inside the FPGA) for the implementation of the IEEE 802.11p standard in both radios. The IT2S board also incorporates a GPS receiver for location and synchronization purposes. The interconnection with the SBC is established through an USB link and it is based on a time multiplexing scheme, allowing the co-existence of several independent channels for accessing each radio unit separately, retrieving information from the Global Positioning System (GPS) device, performing updates on the FPGA bitstream, etc.

2.3 Dependable Vehicular Communications

As stated earlier, traffic fatalities are one of the major causes of death in the world and vehicular communications have emerged as a promising technology to improve the safety of drivers, passengers, and pedestrians on the road. However, there are still some problems to solve before the full potential of this technology can be exploited. As recognized by the scientific community in vehicular networks [31], the development of safety-critical vehicular communications should have a strong contribution from the research fields of computer science, namely fault tolerance and reliable consensus. First of all, vehicular communication systems should take advantage of previous research work done in traditional DCCS, given the fact that they are inherently distributed, i.e. the different nodes are physically apart and cooperate to achieve the common goal of improving traffic safety. The design of vehicular networks, pose even more challenges than traditional distributed systems, because vehicular environments present high mobility and unpredictable link conditions, characteristics that do not arise in static or low-mobility networks. As a result, innovative strategies are needed to overcome these new issues and fulfil the associated requirements.

The design of ITS in general and specifically vehicular communication systems should take into account the fact that strong real-time constraints are present in this type of scenarios, and therefore vehicular networks supporting safety-critical applications should be analysed as hard real-time distributed systems. For instance, in case of accident, the vehicles approaching the location of the hazard should receive a warning message with sufficient time in advance, in order for them to take appropriate measures, avoiding a possible chain collision. If these hard deadlines cannot be met, catastrophic consequences may occur, possibly causing human, economic and environmental losses. Beyond that, this type of safety-critical systems must exhibit a high probability to provide continuous correct service, in order to guarantee that real-time activities are performed within stringent bounds. This usually implies that several dependability aspects are taken into consideration during the design of the system.

In conclusion, dependability attributes are of uttermost importance in the vehicular environment, since a failure in system's operation can lead to severe consequences. As a result, one should prevent failures to occur, and for that purpose, fault-tolerant techniques must be included in the design of vehicular communication systems. More generally, there are numerous situations where the various attributes of dependability can be effectively utilized in the ITS domain.

CHAPTER 3

A Survey on Fault-Tolerance Techniques for Vehicular Networks

This chapter presents a systematic survey of fault tolerance techniques in the area of wireless vehicular communications.

3.1 Introduction

The following systematic review process provides a literature survey of publications in journals and conferences proceedings, available through a set of different search databases (IEEE Xplore, Web of Science, Scopus and ScienceDirect). A systematic method, based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Statement was conducted in order to identify the relevant papers for this survey. Subsequently, the selected articles were analysed and categorised according to the type of redundancy used to achieve fault tolerance, corresponding to three main groups (temporal, spatial and information redundancy).

3.2 Method

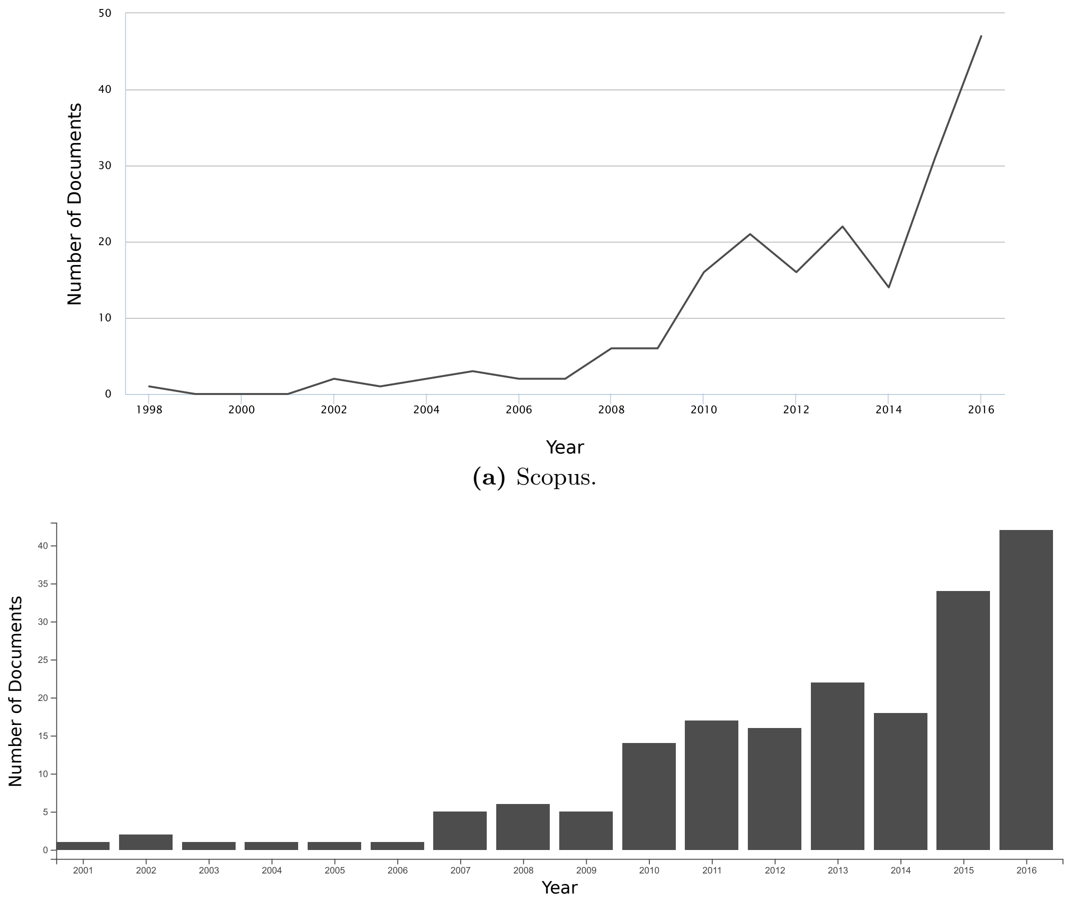
3.2.1 Search Approach and Groups of Keywords

The search method for this survey was based on a systematic review process according to the PRISMA Statement [32]. Four different databases were employed in this search (IEEE Xplore, Web of Science, Scopus and Science Direct), while others, such as Google Scholar, TRID or Academic Search Complete, were also explored but due to several distinct restrictions (e.g. the impossibility to search only on the article's metadata), were not included in the search tools for this review. The approach followed in the paper identification process, required that at least one term from each of two groups of keywords was present in the article's metadata. These two groups of keywords were the following:

- "fault tolerance", "fault tolerant", "fault detection", "dependability", "dependable", "safety critical"
- vehicular network, vehicular communication, "connected vehicles", "VANET", "cooperative vehicles", "cooperating vehicles", "intervehicle communications", "vehicle to vehicle"

The terms "reliability", "reliable" and "real-time" were also considered for the first group of keywords, however since these terms are typically employed in a broader sense, it was decided to limit the search to the keywords shown above. By employing these search terms, a total number of 816 papers were identified (403 from the IEEE Xplore database, 194 from Web of Science, 209 from Scopus and 10 from ScienceDirect).

Both Scopus and Web of Science search tools provide charts with the results distribution along the years. These graphs can be observed in figure 3.1, where the year of 2017 was not included since not all the publications from this year were already accounted for. From the analysis of both charts, it is possible to derive a clear growth in the number of articles published with the search terms. This trend demonstrates the raising importance given by the scientific community to the topic of fault tolerance and dependability in the field of vehicular networks.



(a) Scopus.

(b) Web Of Science.

Figure 3.1: Results distribution along the years.

3.2.2 Selection Process and Inclusion/Exclusion Criteria

After this initial step, the duplicated entries were removed, as well as standards and other invalid results, such as programs, forewords or table of contents from conference proceedings. A total of 469 papers remained for analysis. Then, the titles and abstracts of the remaining articles were screened to exclude research work outside the scope of this survey, focusing for instance in satellite communications or intra-vehicle networks such as CAN or FlexRay. 135 records were still left for the final selection process, in which not only the metadata (title and abstract) but also the body of the paper was analyzed. A set of several criteria was used to ensure the eligibility of the articles to include in this survey:

- be published in English in a peer reviewed journal or conference proceedings;
- be focused on safety applications using wireless vehicular communications;
- including fault tolerance techniques to improve the dependability attributes of vehicular networks.

Complementarily, the following exclusion criteria were utilized in this selection process:

- only the most recent paper from a set of similar articles by the same author was kept (for instance, a paper published in a conference and later extended to a journal or magazine);
- papers not specifically focusing on safety-critical applications (with strict real-time constraints) were excluded;
- articles focusing on security issues of vehicular networks were not selected for the review;
- papers targeting railway, aviation systems, unmanned autonomous vehicle (AUxV), military vehicular clouds (MVC) or wireless sensor networks (WSN) were also considered out of scope of this analysis;
- research works referring to fault-tolerance techniques designed to alternative technologies for vehicular applications, such as visible light communications (VLC), were not included;
- articles not specifically focusing on vehicular networks were discarded, like the ones with a broader scope (e.g. MANETs).

Following these criteria, 18 papers were selected. An additional record was added after screening the reference lists of this final selection, summing up a total number of 19 articles to be subject of analysis in this survey. The complete paper selection process can be visualized in figure 3.2.

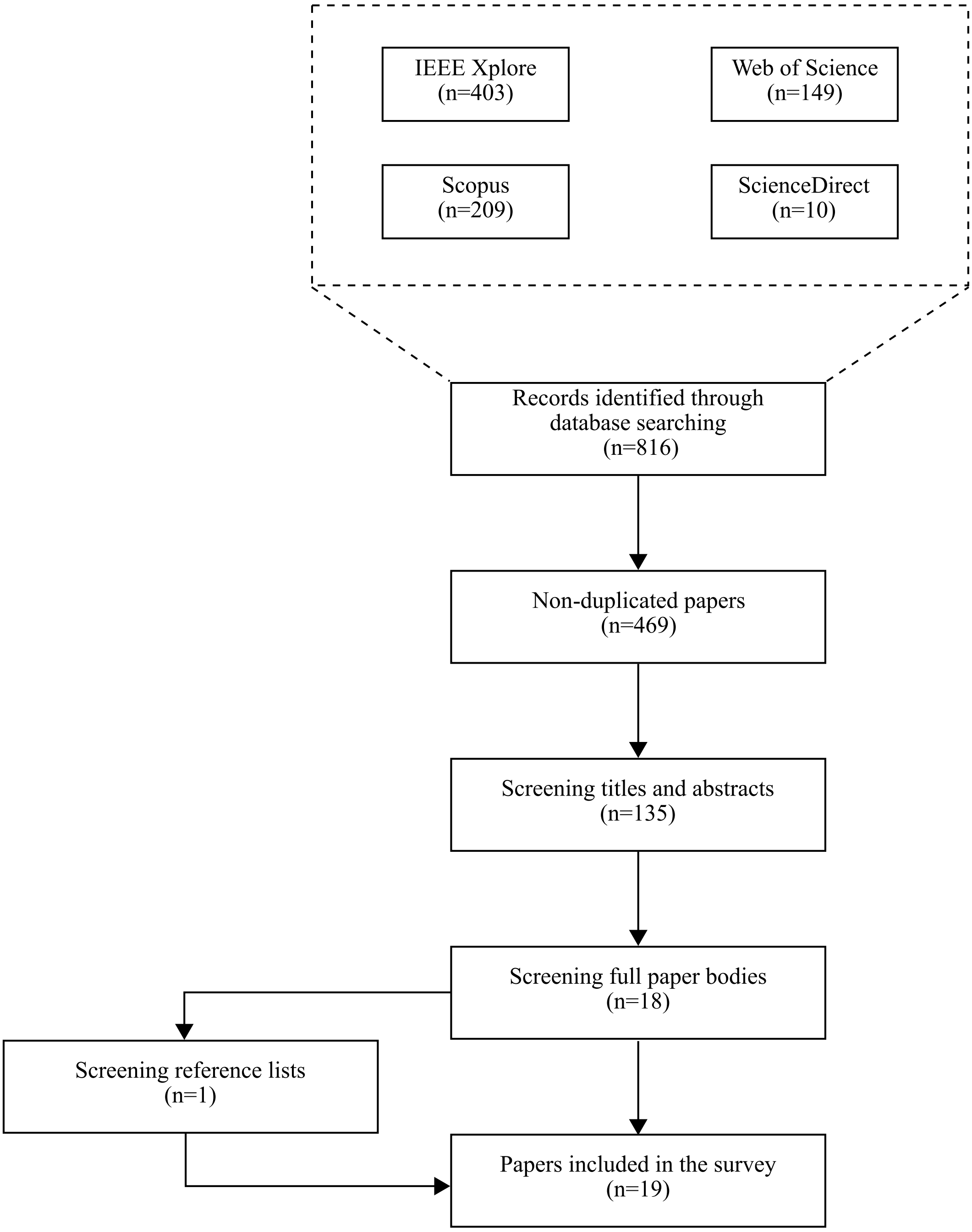

IEEE Xplore (n=403)
Web of Science (n=149)
Scopus (n=209)
ScienceDirect (n=10)
Records identified through database searching (n=816)
Non-duplicated papers (n=469)
Screening titles and abstracts (n=135)
Screening full paper bodies (n=18)
Screening reference lists (n=1)
Papers included in the survey (n=19)

Figure 3.2: Systematic paper review process according to PRISMA Statement [32].

3.3 Taxonomy

The selected publications encompass fault tolerance techniques that can be categorized according to the type of communications redundancy used (temporal, spatial and information). This classification can be visualized in table 3.1. This section summarizes the contributions of each one of the selected publications.

Temporal	Spatial	Information
jonsson2013 [33]	matthiesen2008 [34]	kumar2015 [35]
bohm2016 [36]	cambruzzi2010 [37]	eze2015 [38]
savic2017 [39]	abrougui2012 [40]	
	chang2012 [41]	
	lann2012 [42]	
	sanderson2012 [43]	
	aljeri2013 [44]	
	casimiro2013 [45]	
	worrall2014 [46]	
	ploeg2015 [47]	
	fathollahnejad2015 [48]	
	bhoi2016 [49]	
	elhadef2016 [50]	
	medani2017 [51]	

Table 3.1: Results classification according to the type of redundancy used.

3.3.1 Temporal Redundancy

Regarding temporal redundancy methods, solutions found in the literature are based on packet retransmission schemes. For instance, the work of Jonsson *et al.* [33] focuses on increasing MAC protocol reliability for platooning applications. Time is divided into periodic transmission cycles, called superframes, each one including both Contention-Based Phases (CBPs) and Contention-Free Phases (CFPs). Applications with hard real-time constraints utilize the CFPs to transmit information. These CFPs rely on a polling-based mechanism administered by a master vehicle that applies a Time Division Multiple Access (TDMA) scheme for nodes' transmissions. Each transmission corresponds to a specific time slot, which are ordered according to the Earliest Deadline First (EDF) policy and a real-time ARQ (Automatic Repeat Request) scheme. This ARQ scheme allows the retransmission of packets not well received and that can still be transmitted before their deadline expires. The performance evaluation of the protocol demonstrates a reduction in message error rate by several orders of magnitude when compared to the case without retransmissions.

Following a similar approach, Böhm and Kunert [36] propose a retransmission scheme based on the data age of previously received messages. The framework targets intra-platooning communications but also communication between different platoons (inter-platooning). A dedicated service channel is used for intra-platooning communications, while vehicles in distinct platoons exchange information through the control channel. The platoon leader or master is responsible for periodically disseminating beacon messages to all the other vehicles in the platoon. Then during a collection phase, vehicles transmit status updates, which may or may not be well received by the master. In case of unsuccessfully decoded packets, the leader vehicle initiates a retransmission phase by sending individual polling messages to the other nodes, that immediately attempt to retransmit the failed messages. After that, a control phase begins which is used by the master to coordinate the other platoon members based on the retrieved status information. During this window, control packets are transmitted individually to each regular vehicle. At the end, another retransmission phase begins based on acknowledgments returned by the receiving nodes. Moreover, retransmission opportunities are assigned to the nodes, according to the data age of the messages received by the leader vehicle, which keeps a table with the reception time of the latest status update and acknowledgment frames. From this record, higher transmission priorities are allocated to vehicles with older successfully transmitted messages. The protocol evaluation demonstrated the feasibility of the proposed scheme and the ability to maintain a stable data age value for the platoons.

The work of Savic *et al.* [39] targets a distinct application, in this case the collision avoidance problem of fully autonomous cars at road intersections. An algorithm for distributed intersection crossing is proposed, being able to cope with an unknown and large number of communications failures. A priority for intersection crossing is assigned to each one of the vehicles based on current position estimates and the cars' dynamics. Three types of packets are exchanged: periodic heart-beat messages and 'ENTER' and 'EXIT' messages immediately before and after crossing the intersection, respectively. In case of receive-omission failures, the 'ENTER' or 'EXIT' packets are retransmitted and the model assumes that at least one heart-beat message is received before the intersection crossing algorithm starts and that vehicles eventually succeed to receive the 'ENTER' and 'EXIT' messages. The numerical results show only a slight increase of the intersection crossing delay under the presence of communications failures.

3.3.2 Spatial Redundancy

In [34], Matthiesen *et al.* investigate the utilization of replicated application services in dynamic clusters of vehicles. The goal is to increase the reliability and availability of safety-critical applications in ad-hoc vehicular networks. The example of a distributed shared memory, which support the operation of a stateful road-traffic information service, is presented in this work. Several metrics are analysed and evaluated for different cluster dimensions, such as data consistency, response time and application availability. A Replication Manager is employed in order to achieve stable clusters, by selecting replicas with good communication metrics that minimize service response time and reconfiguration overhead in case of faulty behaviour. These faults can be due for instance to excessive delay or high packet loss, which may affect timeliness and correctness of the service, thus leading to inconsistent application states.

The work of Cambruzzi *et al.* [37] proposes a failure detection scheme based on a protocol that detects both link and system failures. It employs a heartbeat mechanism in which, all road-side units and vehicles transmit a beacon message periodically to their single-hop neighbours. When a beacon packet reaches its destination, the receiving node adds or updates its neighbours' list with the received information together with a timestamp of the packet. If no message is received from that neighbour during a predefined time interval, the node is considered to be faulty and is inserted into a list of suspects. The algorithm uses adaptive timeouts in order to cope with the dynamic conditions of vehicular networks. By exchanging information with other neighbours, it is possible to verify if the suspect node is indeed faulty. In this model, only two types of faults are assumed. Those caused by a system crash and the ones caused by a vehicle exiting the road. Malicious or Byzantine faults are not considered in this study.

Based on a similar failure detection mechanism, Abrougui *et al.* [40] introduce a fault-tolerance location-based service discovery protocol for vehicular networks. This protocol handles the discovery procedure of different types of both safety and infotainment services and it was designed to perform well even under the presence of service provider failures, communication link failures and road-side units failures. The proposal relies on a cluster-based infrastructure, where road-side units are clustered around service providers, the congested areas of the vehicular network and the intermittent areas to improve the connectivity of the network. The proposed fault-tolerance mechanisms were introduced at the network level, in order to cope with several types of failures in the connection between the service provider and the service requester. Essentially, in case of link or system failure, an algorithm is employed to designate alternative nodes that will supply or forward the information missed in the faulty nodes/links. Simulation results showed an improvement in the success rate of discovery queries of approximately 50% and 30%, in case of roadside router and link failure scenarios, respectively, when compared with a simplified version of the protocol without fault tolerance techniques.

Chang and Wang [41] also propose a fault-tolerant protocol but for reliable broadcast of alert messages in vehicular ad-hoc networks. The goal of this protocol is to reduce the total number of messages needed to disseminate the alert message along the road. The proposed method designates the two farthest vehicles in the radio range of the source vehicle to act as candidate relay nodes of the message to be broadcast. This selection is performed by the source vehicle and it is based on the GPS coordinates provided by all vehicles in the transmission range. If the farthest vehicle from the source node does not transmit the safety message within a maximum time interval, the sub-farthest will assume that there was a system failure and will disseminate the intended message.

The work of Gérard Le Lann [42] deals with omission failures originated by transient fault in the transmitter, receiver or in the communications channel. High reliability and strict timeliness properties are achieved through group dissemination protocols, so that every message can be delivered to a given set of vehicles within a worst-case deadline. The proposed fault-tolerant strategy relies on the spatial redundancy provided by the multiple copies of information kept in the different vehicles. This approach would typically lead to high overhead, however the notion of proxy sets is introduced in order to limit the scope size of the global dissemination protocol. A proxy set is a group of contiguous vehicles such that at least one member of the group receives the message that should have also been received by the intended destination node, being this member aware of the response that the destination node would return.

Sanderson and Pitt [43] propose an adaptation of the *Paxos* algorithm [52] to implement consensus formation in self-organizing vehicular networks. The proposed algorithm (*IPcon*) handles institutionalised consensus in spite of faults occurring in the dynamic clusters of vehicles. The protocol tolerates faults caused by nodes that fail by permanently stopping or later restarting, delayed, lost or duplicated messages, however malicious vehicles and corrupted packets are not considered. The evaluation of the algorithm demonstrates the resilience against role failures (nodes may play 4 different roles in the *IPcon* protocol) and cluster fragmentation and aggregation.

A fault detection protocol is introduced in [44] by Aljeri *et al.*, in order to mitigate communications problems in vehicular networks. Fault diagnosis is performed by comparing the output messages from a group of vehicles. This way, it is possible to identify faulty vehicular nodes. The process is initiated by an RSU, which attributes the same task to a group of vehicles. Then, the results are computed by each node and the answers are transmitted back to the initiator. If the results are identical, it is assumed that there are no faults in the network. On the other hand, if different results are yielded, faulty road components can be detected. Additionally, a more efficient implementation of the protocol is proposed that relies on regional RSUs, which decreases the total number of packets transmitted and the diagnosis latency of this method.

In [45], Casimiro *et al.* develop a kernel-based architecture (KARYON) for safety-critical coordination in vehicular systems. Besides dealing with sensor faults and real-time properties of the wireless communications (e.g. self-stabilizing protocol), the proposed architecture also introduces extra components to the standard MAC layer. According to the followed subsystem isolation, the authors assume in the fault model that communication components can experience crash or timing faults, however data can not be corrupted, i.e. faults may occur in the time domain, but not in the value one. In addition to the standard MAC layer, two extra elements are introduced: the Mediator Layer (MLA) and the Channel Control Layer. For example, the MLA is responsible for node failure detection and membership, as well as for controlling temporary network partitions. On the other hand, the Channel Control Layer supervises the channel state and enhances the network resilience by taking advantage of the diversity of radio channels available for vehicular communications purposes.

The work of Worrall *et al.* [46] deals not only with complete loss of radio communications, but also with partial degradation of the wireless link. In some cases, the communications performance is affected in an intermittent way or behaves poorly after a certain distance, due e.g. to damages in the external cables, antennas or connector. The proposed method utilizes data gathered during normal operation so that the antenna behaviour can be modelled and used in future fault detection. This model is derived by analysing and learning the properties of wireless communications in a fleet of vehicles, taking into account parameters such as relative orientation, bearing and range between vehicles. The detailed knowledge about the communications performance is then utilized to detect partial antennas faults or permanent link failures, which are identified by observing when the RF communications deviates from the expected operation. Additional computational resources are required in order to allow online execution of the mathematical model and appropriate comparison with the run-time results of the antenna performance.

Platooning applications constitute a particular use case scenario of vehicular communications. Ploeg *et al.* [47] address the problem of faulty links in a platoon of vehicles. A safe distance between the members of the platoon is continuously computed by taking into consideration the availability of sensor data and the communications link performance. This safe distance is employed by the CACC system according to a graceful degradation scheme that adjusts the settings of CACC to keep as much functionality as possible, even under the presence of faults, but always guaranteeing string stability in the platoon. Moreover, two different network topologies can be applied, depending on the time delay of the communications link. If this delay exceeds a predefined treshold value, the platoon service switches from an one-vehicle look-ahead topology to a two-vehicle look-ahead configuration. This fault-tolerance strategy can only be applied if the delay time is not excessively large, otherwise wireless communications should not be employed in order to preserve string stability.

In [48], Fathollahnejad *et al.* propose a synchronous Group Formation (GF) algorithm to enhance self-organizing vehicular applications under the presence of an unbounded number of asymmetric communication failures. The main goal of the GF algorithm is to achieve agreement, or at least to reduce the probability of unsafe disagreement, on the membership of a cooperative ITS application, e.g. Virtual Traffic Lights (VTLs). A decision mechanism is employed by each member node (vehicle) to identify the other nodes in the group at each moment in time. The mechanism relies on the utilization of an extra component, designated as *oracle*. These *oracles* are local devices present in each node, being responsible for detecting the remaining participants in the group. The obtained simulation results show that when the local *oracles* provide a correct estimate of the group formation, only safe disagreement scenarios may occur. However, when the *oracles* underestimate the total number of nodes, unsafe disagreement situations may happen and the likelihood of such scenarios increases with the probability of receive omissions in the communications channel.

Bhoi and Khilar [49] introduce a fault-tolerant routing protocol for vehicular ad-hoc communications in urban environments. A fault detection technique is used by the vehicle itself to detect if its own operation is fault free or not. If a faulty behaviour is identified, the OBU does not participate any longer in the routing process. The fault detection mechanism targets soft faults, i.e. erroneous behaviour in the OBU devices causing the generation of incorrect data for a long period of time. This may be caused by high noise affecting the node's operation, making it still able to compute, send and receive information. However, beaconing data transmitted by the vehicle can not be considered valid, being this information (position, speed, etc.) indispensable for hop selection in the routing algorithm. For that reason, these nodes are automatically excluded from the routing process by self detecting these soft faults, through the analysis of the Received Signal Strength Indicator (RSSI) values from the received messages and the location coordinates provided by the neighbouring nodes. The proposed protocol provides good results in terms of end-to-end delay, path length and false alarm rate.

The work of Mourad Elhadef [50] suggests the utilization of a primary-backup approach for the design of a fault-tolerant intersection control algorithm. The VTL system is based on a centralized solution, with an RSU controller responsible for coordinating all traffic crossing the intersection. The controller manages the vehicles approaching the site, by granting or denying access to the intersection, in order to guarantee safety, liveliness and fairness, while at same time maximizing road traffic throughput. Both the primary and the backup controllers are constantly synchronizing with each other, so that the backup unit can always be kept updated with all the necessary traffic information. Only permanent crash failures are considered in the fault model. Whenever the main controller stops sending and receiving messages (a *keep alive* timer is used to detected if the primary node is down), the backup unit takes control of the intersection.

In [51], Medani *et al.* develop a time synchronization strategy for the nodes of vehicular networks. Clock synchronization is essential to support the correct operation of safety-critical applications in road traffic environments (e.g. for event causality, medium access control or security purposes). The proposed method, named Offset Table Robust Broadcasting, attains high accuracy and presents fault-tolerant capabilities, so that every node is aware of neighbouring clock times and is able to synchronize its communications with other nodes. The clock offsets among several nodes are computed using a round-trip time mechanism and acknowledgement messages are exchanged to ensure that the offset table delivery reaches all nodes.

3.3.3 Information Redundancy

Finally, with respect to information redundancy mechanisms, the identified solutions are based on network coding techniques. For instance, the work of Kumar and Dave [35] introduces a decentralized method that provides reliable and scalable vehicular communications, independently of the traffic density level. The solution employs network coding and random walks in order to deal with the constantly changing topologies, varying vehicle density and unreliable channel conditions of vehicular networks. Raptor codes, which are characterized by its low complexity and thus fast decoding, are used to encode and disseminate information in a completely distributed manner, providing better fault tolerance. In this scheme, a vehicle transmits its data to a random set of neighbouring vehicles and then each vehicle only encodes the information its has received. Posteriorly, a receiving vehicle can efficiently decode the transmitted data by collecting a sufficient amount of data blocks from the network nodes it interacts with while moving. Random walks are utilized to disseminate the data, avoiding the need for supporting a generic layer of routing protocols. The performance evaluation of the proposed scheme is evaluated through simulation and the results are compared against the simple broadcast framework (store and forward strategy) and other related works in the literature. Data overhead and average end-to-end delay are kept low for different traffic densities and data sending rates, while network reachability and packet delivery ratio are improved in comparison with the other analysed solutions.

Eze *et al.* [38] also propose an innovative communications scheme based on the network coding concept, named Coding Aided Retransmission-based Error Recovery (CARER). The goal is to improve broadcast reliability and timely delivery of messages with less number of retransmissions. In this scheme, each node performs an exclusive OR (XOR) operation on a set of both received and generated packets and then send these encoded messages to all the vehicles in a one-hop distance. The advantage of this technique over simply broadcasting the raw packets is that it allows nodes to recover lost frames with low communications overhead. Additionally, the protocol uses a location-aware algorithm that selects an appropriate vehicle for rebroadcasting the encoded packet towards the desired propagation direction. The traditional Request-to-Broadcast/Clear-to-Broadcast (RTB/CTB) handshake is used to overcome the hidden node problem and reduce collisions in the wireless medium. An analytical model was developed and simulation tests were performed to evaluate the performance of the protocol. The results show an increased packet recovery probability and a lower packet collision probability when compared to the simple repetition based error recovery scheme with no network coding mechanism involved.

3.4 Conclusion

In summary, there are not many research works in the area of fault-tolerant vehicular communications. However, an increasing interest can be observed in the recent years, with more protocols, mechanisms and architectures being proposed in order to enhance the dependability attributes of wireless vehicular networks. The analysed publications show that the development of safety-critical applications in such dynamic environments require a careful planning that preserves system's flexibility and real-time guarantees while providing fault-tolerance capabilities. As a conclusion, there is still a lack of strategies available to completely fulfil the operation of dependable vehicular networks. This is the main motivation for the realization of this thesis, being the most important contributions summarized in the next chapter.

CHAPTER 4

Fault-Tolerant Architecture for Dependable Vehicular Communications

This chapter presents the main contributions of this PhD thesis, focusing on the design, implementation and validation of mechanisms to increase the dependability of wireless vehicular networks.

4.1 Introduction

Methods to enhance the dependability attributes of vehicular communications are of uttermost importance in this type of environments, given the safety-critical characteristics of road traffic systems. In this chapter, several strategies are presented in order to provide a more dependable framework for the development of cooperative ITS applications. It starts with a method to mitigate the interference problems in vehicular communications systems (Paper A) and continues with a set of techniques to increase fault-tolerance in real-time vehicular networks, namely a fail-silence enforcement mechanism (Paper B), an RSU replication scheme (Paper C and Paper D) and a medium guardian for the OBU nodes (Paper E). The next sections provide a summary and an integrated view of the research work of this thesis. These contributions can be analysed in greater detail by consulting the appended papers at the end of the current document.

4.2 Interference Problems in Vehicular Communications Systems

DSRC technology operating in the 5.8 GHz frequency band is utilized by up to 50% cars and more than 85% of trucks in Europe, in order to traverse toll plazas and free flow sections in a time efficient way. These DSRC systems are different from the ones employed in vehicular networks, whose operation takes place in the 5.9 GHz band, as explained in chapter 2.

Tolling systems based on this technology have contributed to enhance road transportation by supporting a safer and seamless way to drive on the traffic network. Furthermore, DSRC tolling also play a key role in the business model of many motorway operators in Europe.

It is expected that in the near future, vehicular communications systems will support tolling services and the operation in the 5.8 GHz will no longer be necessary. However, during a transition period, both technologies will coexist and with the dissemination of vehicular networks, there is a risk of interference between the 5.8 GHz and the 5.9 GHz frequency bands. This issue was clearly identified in the ETSI ITS-G5 standardisation process, during which potential technical compatibility issues have been highlighted between DSRC tolling systems and ITS-G5 used by cooperative vehicles [53].

This problem only arises in Europe where the radio bands utilized for these two purposes are very close to each other (figure 4.1). However, in the rest of the world, other potential sources of radio interference may also impact the performance of vehicular communications systems. For instance, in the United States the FCC proposed sharing the IEEE WAVE spectrum band with unlicensed devices, such as Wi-Fi [54] [55]. Several protocols have been suggested to allow the coexistence of both technologies in the same frequency band. Most of them are based on detect-and-avoid mechanisms that sense the wireless channel before transmitting. For instance, if ITS-G5 communications are present, the Wi-Fi may use extended back-off periods in the MAC layer. Another possibility is to vacate the communications channel for a long period of time if the Wi-Fi device detects an ITS-G5 transmission.

Cross Channel Interference is another source of problems that may arise when other vehicular communications modules are transmitting in neighbouring radio channels. For example, if a node is broadcasting a message in channel 178 and another one starts transmitting in channel 180, some Power Spectral Density (PSD) of the signal will interfere with the receivers of the packet sent in channel 178. Besides decreasing the Signal-to-Interference-plus-Noise Ratio (SINR), thus increasing the probability of higher Packet Error Rate (PER) values, there is another undesired effect that translates into larger delays to access the wireless channel, since the transmitters may perceive the medium as busy due to the interference from nearby channels. This Adjacent Channel Interference problem is well-know in the wireless domain and has already been studied for the vehicular case [56]. Some strategies to minimize the negative impact of the ACI effect in the communications quality are based on the reduction of the transmission power when messages are being exchanged in adjacent channels or changing to another frequency whenever possible.

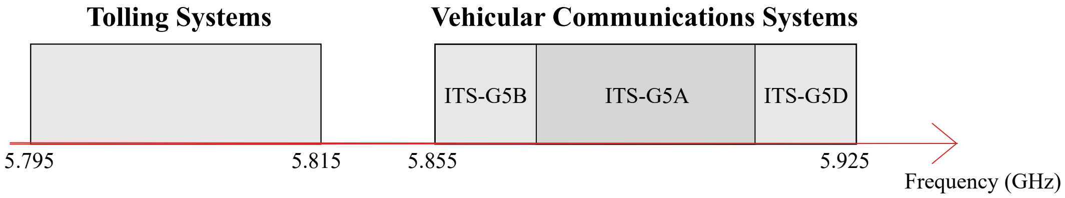


Figure 4.1: DSRC spectrum in Europe for vehicular communications and tolling systems.

4.2.1 Mitigating Communications Channel Interference

In order to handle this interference problem, a digital FIR filter has been developed in the scope of this thesis (Paper A). This filter is to be integrated in the reception chain of vehicular communications modules, with the main goal of reducing the PSD of the interfering signal in the frequency band of interest. Firstly, the impact of the concurrent transmissions in adjacent channels was captured and measured in a laboratory environment by taking advantage of the IT2S platform described in chapter 2. With these flexible platforms, it was possible to develop an experimental setup where the transmission of a packet takes place at the same time as an interfering signal is present, allowing the visualization of the resulting effect in a receiver node. The obtained results show the need for strongly attenuating the unwanted signal, specially when power transmission levels are high.

Nevertheless, the design of the filter must be efficient, so that the delay introduced in the reception chain is not significant, otherwise it could compromise important functions, such as frame detection and Automatic Gain Control (AGC), or ultimately the real-time requirements of the system. For that reason, a multi-rate system approach was followed by taking advantage of interpolation and polyphase decomposition concepts. Consequently, the resulting two-stage low-pass filter can be analysed as an interpolated low-pass FIR filter in the first stage and a polyphase decomposed low-pass filter in the second stage. The interpolated filter provides most of the required attenuation, $\approx$ 40 dB in the stopband region, while the polyphase decomposed filter is mainly responsible for eliminating the replicated passbands in the filtered signal.

The whole filter was designed with the aid of a MATLAB® toolbox and its performance was also evaluated in the MATLAB® environment, by applying the filtering operation to the raw samples captured from the IT2S platform. The obtained simulation results proved the effectiveness of the proposed filter with a very strong attenuation of the interfering signal.

4.3 Deterministic MAC Protocols

Another important issue with the development of safety-critical vehicular communications systems is related with the operation of the Medium Access Control protocol. The utilized MAC scheme is essential for the implementation of real-time wireless communications, as required by future road safety applications [57]. These applications require timely and reliable communications for the exchange of hazardous messages. As a result, the design of the MAC layer is strongly conditioned by the delivery of these messages, in order to guarantee that critical communication tasks meet their deadlines. The MAC scheme must provide an upper bound on the maximum delay a node can face before getting access to the wireless channel for packet transmission.

As already mentioned in chapter 2, the protocol stacks for vehicular networks (IEEE WAVE and ETSI ITS-G5) rely on the IEEE 802.11 standard for the implementation of the MAC layer. However, this standard employs a CSMA/CA technique for regulating channel access. This CSMA/CA method presents serious drawbacks regarding the timeliness of communications, for the reason that it allows packet collisions to occur in the wireless medium, thus causing unbounded delays before channel access.

A way to handle this problem is to guarantee that the network load is kept low, thus reducing the probability of packet collisions. This can be accomplished for example by utilizing an adaptive message-rate control mechanism as suggested by Bansal *et al.* [58]. Nevertheless, this type of solutions still does not achieve strict real-time guarantees, since collisions may still occur and a worst-case delay value can not be computed from message generation to channel access. As a result, contention-based MAC schemes are inherently non-deterministic, since it can not be ensured that real-time traffic will reach its destination by the pre-defined deadlines.

The solution is to design collision-free MAC algorithms that assure the inexistence of packet collisions in the communications channel and the possibility to calculate a worst-case delivery time. This way, it is possible to guarantee predictable behaviour and high reliability in packet transmission. These deterministic MAC protocols with collision-free conditions can only be achieved if the protocol restricts access to the wireless medium and controls packet transmissions in order to provide appropriate timing behaviour.

Different schemes can be applied to completely avoid channel collisions, like the ones based on Time Division Multiple Access or Frequency Division Multiple Access (FDMA) techniques, where each node utilizes a specific time slot or carrier frequency to transmit. Due to the scarcity of radio channels, the short duration of link connectivity and the broadcast characteristics of vehicular communications, an FDMA scheme may not be the most appropriate solution. On the other hand, a time-slotted approach typically involves fixed packet sizes and periodic transmissions. For that reason, TDMA-based MAC protocol can suit the requirements of periodic CAM messages , but also the DENM packets that typically need to be transmitted or retransmitted by more than one node in the same geographical area. This time-triggered approach usually requires a high precision synchronization scheme that in the case of vehicular networks, can be provided by the GPS receiver systems.

Furthermore, a real-time MAC protocol for vehicular networks can either rely on a purely ad-hoc solution or on the support provided by the road-side infrastructure. By combining both models, an hybrid approach can also be pursued. The presence of the RSUs and the backhauling network facilitates the design of the deterministic protocol, since in the ad-hoc scenario, strict real-time behaviour is hard to achieve, given the high mobility characteristics of vehicular networks. As a result, network topologies are constantly changing and intermittent or short duration link connectivity becomes very frequent. Thus, the required distributed consensus algorithms, e.g. membership agreement and leader election protocols, take a long time to execute, which is not compatible with the dynamics of the system.

With the road-side infrastructure, the operation of the system can be made more predictable, by assigning crucial tasks to the fixed nodes of the network (RSUs), like admission control policies and the execution of transmission scheduling algorithms. Given the static and well-known position of the RSUs inside the network, the connectivity disruption problem can be minimized and with adequate RSU placement, uninterrupted connectivity between the mobile nodes and the road infrastructure may be provided [59]. The backbone network interconnecting all RSUs, enables them with a global vision of the system, which eases the task of cooperatively coordinating resource allocation in the wireless medium. In addition to this, security properties can also be enforced by a centralized entity in the infrastructure-side that effectively manages key distribution and vehicle's identity verification. Through RSUs' operation, received vehicle data can be cross-checked with other sources of information such as cameras or radars, thus helping solve privacy and security issues.

This way, it is possible to analyse the system as an instantiation of the wormhole metaphor, as described by Paulo Veríssimo in [60]. According to this metaphor, the RSUs can be considered as wormholes, since they are able to execute certain tasks faster or more reliably. The uncertainty is not uniform across all networks components and the fixed units possess a higher degree of dependability than the OBU nodes. This can be achieved by implementing fault-tolerance mechanisms in the network architecture. These mechanisms are capable of minimizing the impact of faults in the operation of vehicular communications protocols. Consequently, the determinism and reliability added by the road-side infrastructure helps to enforce real-time properties at the wireless end of the network.

4.3.1 V-FTT Protocol

Based on the above rationale, an infrastructure-based MAC protocol presenting real-time behaviour, served as the basis for the design of a fault-tolerant architecture for vehicular networks. This deterministic MAC protocol, named Vehicular-FTT (V-FTT) [61], is based on a TDMA approach, where each node has the opportunity to transmit in a specific time slot per communications cycle. The RSUs behave as network masters, handling the registration procedure of the OBU nodes and executing the scheduling algorithm that establishes the communications slot allocation.

In this framework, time is divided into consecutive Elementary Cycles (ECs). Each cycle has a fixed duration of 50 ms, in order to fulfil the real-time requirements imposed by human reaction times while driving. The EC comprehends three different phases:

- **Infrastructure Window (IW) -** a time interval used by the RSUs nodes to transmit the scheduling information for the current EC. Safety-critical warnings may also be disseminated by the RSUs during this period.
- **Synchronous OBU Window (SOW) -** composed by the time slots allocated for the OBUs' transmissions. The size of this window is variable, depending on the number of OBUs within communications range.
- **Free Period (FP) -** is utilized by nodes non-compliant with V-FTT protocol to send safety messages or by the OBU devices to first register and authenticate with the roadside infrastructure. This FP window does not follow a TDMA scheme, being ruled by the standard IEEE 802.11 protocol. As a result, a CSMA/CA method is applied during this period, leaving the possibility of packet collisions to occur.

A diagram of the whole EC sequence can be observed in figure 4.2, for the case of N RSU nodes and M vehicle OBUs. In order to guarantee continuous connectivity with the

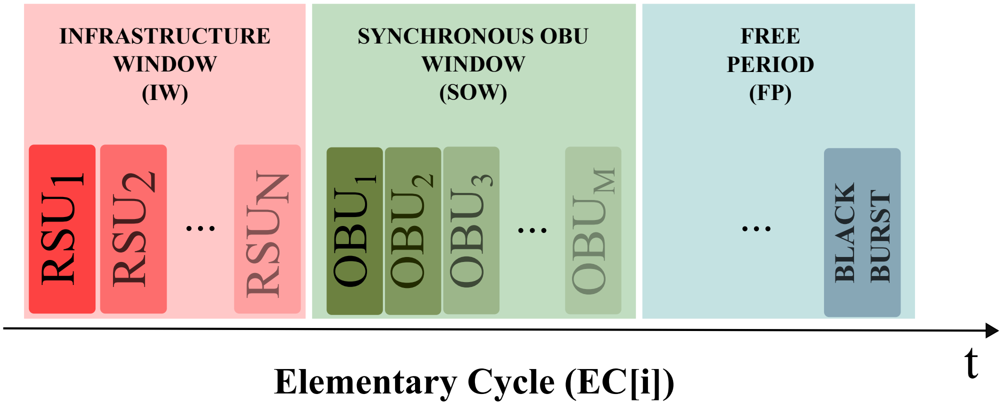


Figure 4.2: Original EC structure of the V-FTT protocol.

infrastructure and to provide some fault-tolerance in the transmission of the scheduling table, V-FTT requires partial overlap in the communications range of the RSU nodes. As a result, an OBU device in a specific location may be able to receive up to N scheduling messages from distinct RSUs.

The protocol also relies on the spatial reuse of time slots for both RSUs and OBUs transmissions [62]. This way, it is possible to efficiently implement the traffic scheduling algorithm along the road infrastructure. Nevertheless, a collaborative execution among the multiple RSUs is necessary, in order to obtain a common and global traffic view. This involves the exchange of data through the backhauling network with information regarding the road situation awareness of each individual RSU station.

In order to ensure the continuity of the TDMA transmissions and avoid any interference from non-compliant nodes, it is necessary to utilize a short Inter-Frame Space between two consecutive messages in the collision-free phases of the protocol, i.e. the IW plus the SOW. For the same reason, it is also required to execute a blackburst transmission right before the beginning of the collision-free interval [63]. This way, the protocol can guarantee low jitter in the first time-triggered transmission of each EC. Otherwise, a message sent by a non-compliant node during the FP could interfere with the beginning of the collision-free phase, thus violating the real-time properties of the protocol.

The original version of V-FTT [61] established the following order for the different windows. First, the Infrastructure Window with the RSU transmissions, immediately followed by the Synchronous OBU Window and then the Free Period. This sequence can be observed in figure 4.2 and it was proposed before implementing the protocol in actual communications platforms. However, when the first prototype of the V-FTT protocol was deployed in an IT2S platform, it could be concluded that it was more appropriate to shift the SOW period to the end of the EC, as depicted in figure 4.3.

The reason for this is based on the fact that the OBU nodes require some amount of time to decode and process the scheduling messages transmitted by the RSU. Only after retrieving the time slot information from these packets, the OBUs are ready to initiate their

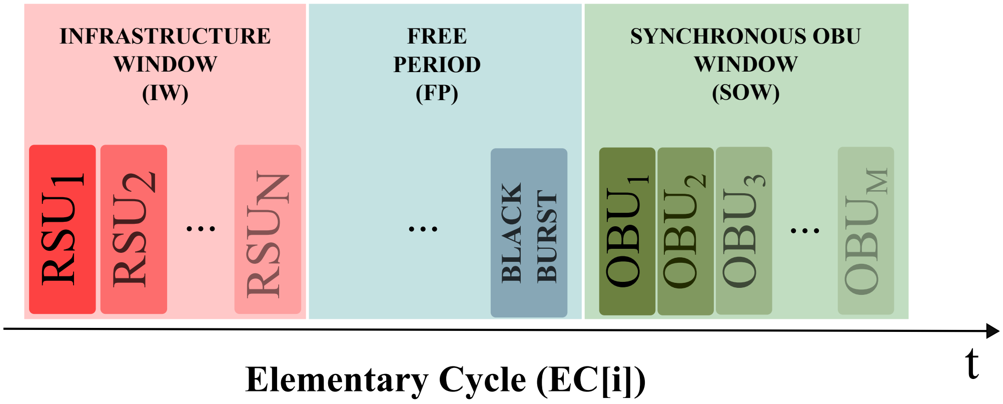


Figure 4.3: Updated EC structure of the V-FTT protocol.

transmissions. However, since in the original scheme the SOW period was immediately after the IW there was not enough time to decode the assigned slots. With the modification presented in figure 4.3, there is an appropriate period available to perform this operation. As a result, the blackburst transmission now happens prior to the beginning of the SOW period, in order to clear the channel just before the collision-free intervals.

4.4 Fault-Tolerant Infrastructure-based Architecture

A vehicular network based on the V-FTT protocol follows a master-slave approach, where the RSU constitute the master nodes of the network and the vehicle OBUs behave as slave units. The RSUs besides managing the registration process of OBU nodes with infrastructure, also control all communications taking place in the wireless medium by establishing the time slot allocation in each Elementary Cycle. The mobile nodes are only responsible for transmitting their information in the specified slot. Clock synchronization among static and mobile nodes is achieved through the GPS signal available in each one of the stations.

The proposed fault-tolerant architecture includes a set of techniques to enhance the dependability of both fixed and mobile units. Figure 4.4 illustrates this scenario, with the additional mechanisms introduced in the OBU and RSU nodes. First of all, it should be noticed that the network allows the participation of nodes non-compliant with the V-FTT protocol, referred as *alien* nodes. These *aliens* are able to transmit during the FP window, the contention-based phase of the protocol.

On the infrastructure side, each RSU node is composed by two IT2S platforms, whose results are compared by a fail silence enforcement entity. The purpose is to only allow the transmission of valid messages to the wireless medium. If this primary or active unit fails, a backup node is ready to immediately replace its operation, as depicted in the image. On the OBU devices, a medium guardian is responsible for monitoring node's operation, verifying all messages produced by the mobile unit. In case of disagreement with the expected behaviour, the transmission interface is instantly disabled by the guardian. As a result, both RSU and

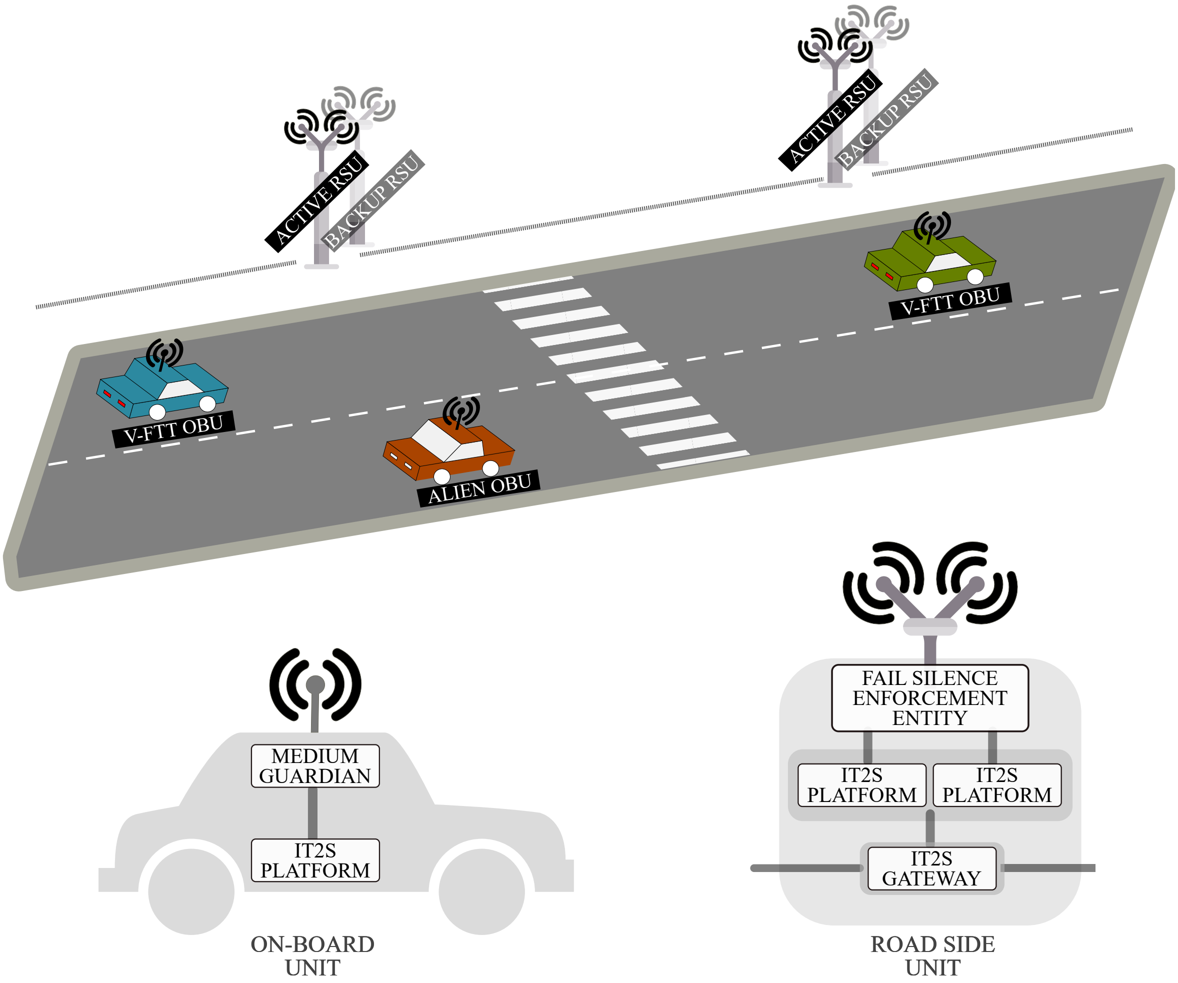


Figure 4.4: Fault-tolerant architecture for vehicular networks.

OBU nodes present fail-silent behaviour, not interfering with the valid transmissions, and the infrastructure exhibits system recovery capabilities with the presence of the backup stations.

In the fault model, it is assumed that, with the proposed mechanisms, nodes may only exhibit the fail-silence failure mode. This is achieved through the design and implementation of the fail silence enforcement entity and the medium guardian device in separate fault containment regions from the nodes they are monitoring. Covered faults include hardware, both transient and permanent, and software faults. Byzantine faults, notably intrusions, are not fully covered, e.g. due to attacks originated in the backbone cabled network that need to be handled at a different system level.

Furthermore, channel permanent faults are not considered in the fault hypothesis since the wireless channel should be protected from unregulated interference by the reserved spectrum policy for vehicular communications. Nevertheless, channel transient faults are likely to occur, due to the constantly changing atmospheric and traffic conditions. The network handles this problem by introducing time and spatial redundancy in nodes' transmissions. For instance, in a specific geographical location, an OBU should be able to receive multiple scheduling messages from distinct RSU nodes. In the same way, an OBU's packet may also reach different RSUs.

4.4.1 Fail Silence Enforcement Mechanism

Given the key role played by the RSU stations, it is critical to ensure that all messages transmitted by these nodes are correct. RSUs are responsible for coordinating all communications in the wireless medium and therefore constitute single points of failure in the network architecture, holding the traffic scheduler and the vehicles registration database. Network activity can be seriously compromised if an RSU starts sending invalid scheduling messages or transmits them out of time.

In order to handle this issue, a fail silence enforcement mechanism is introduced (Paper B), guaranteeing that all messages transmitted by the RSU devices are valid both in the value and time domains. With fail-silent behaviour, nodes can only fail by not sending anything to the medium. However, this can only be attained if additional components are used to enforce fail silence, since nodes may fail uncontrollably.

As can be observed in figure 4.5, fail-silence failure semantics is achieved through internal redundancy of the IT2S platform and the utilization of a fail silence enforcement entity. This entity is implemented using dedicated hardware and belongs to a separate fault containment region. It is responsible for verifying if there is an agreement between the results produced by both IT2S platforms. If there is a match both in value and time domains, the messages can be transmitted to the wireless medium.

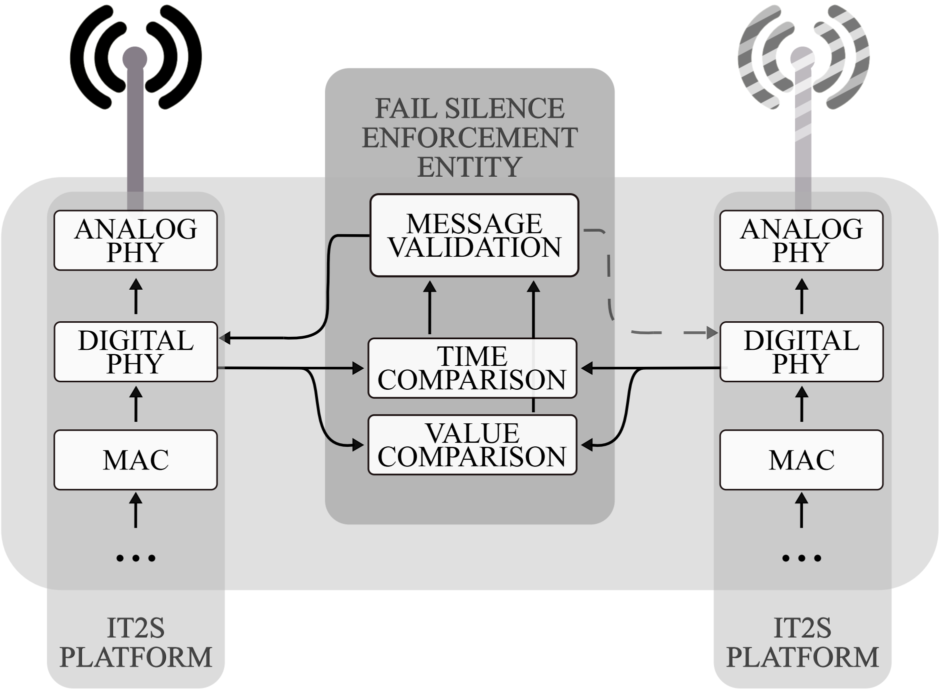


Figure 4.5: Fail-silent RSU node.

In case of agreement, both platforms receive the validation signal, but only one of them forwards the message to the antenna. The other remains silent and waits for the next task to be executed. If a fault is detected, none of the platforms receive the confirmation signal and thereby try to notify the upper layers and the IT2S gateway that the system is faulty and needs maintenance. It should be noticed however that faults in the analogue part of the physical layer are not covered, thus can not be detected by the fail silence enforcement entity. The reason for not including the operation of the analogue part of the system in the fault detection mechanism, lies in the fact that there is no reliable way to analyse the produced messages in the analogue domain and validate them before being transmitted.

4.4.2 RSU Replication Scheme

As already stated, RSUs deliver core services in an infrastructure-based real-time vehicular network. Their activity is fundamental for the operation of the entire road traffic system and if these nodes are affected by severe faults, network communications could be disrupted. This problem could be handled using replication and the solution could rely on voting schemes and majority selection. However, this approach would typically lead to more resource usage, with a higher number of replicas being necessary.

For that reason, a fail silence strategy was followed in this work, which facilitates the design of the proposed replication scheme (Paper C). With fail-silent RSUs, one or more similar nodes can act as backup units and provide fault-tolerance capabilities. An active approach was employed in this primary-backup scheme, meaning that as soon as a fail-silent failure is detected, the backup unit immediately comes into the foreground and transmits the missing message. This way, it is possible to ensure that even in the presence of a failure in the primary RSU node, the scheduling messages containing the EC slot allocation will still be delivered to the OBU stations with real-time guarantees.

The active replication scheme allows the system to maintain protocol communications without any discontinuity of the traffic schedule. Nevertheless, this is only possible to achieve if all RSU replicas are synchronized both in value and time domains. In order to achieve that, the backup RSUs receive and process the exact same sequence of messages in parallel with the primary one. In the same way, the resulting scheduling messages are also equal, but their transmission is deliberately and slightly delayed. This way, when the backup units try to send their messages, they will face the medium busy, as long as the active RSUs do not fail, and their transmission will be cancelled. In this context, the sensing mechanism of the backup RSUs operates as a fault detection technique. In case of primary RSU failure, the channel will be free and the backup node will be able to transmit the exact same message only with a small delay relatively to the omitted primary's message.

Consequently, the recovery procedure is completely automatic and transparent to the slave nodes. If the primary RSU is free of error, the backup unit will sense the medium as occupied, will avoid overlapping with the active node and the OBUs will receive the scheduling messages in the planned instant. On the other hand, if the active system fails, the backup replica will perceive the medium as free, replacing the operation of the primary RSU and the OBUs will receive the scheduling message a little be later in time.

Figure 4.6 illustrates the proposed replication scheme, with both the primary and backup units connected to the same IT2S gateway, that abstracts the RSU redundancy from the rest of the backbone cabled network. Another important aspect is the direct exchange of information between the primary and backup nodes. It was mentioned before that both units need to be synchronized not only in time, but also in the value domain. It was also referred that they are inherently synchronized in the value domain, since they receive and process the same sequence of messages, whose information influences the produced results. However, this is not always the case and one of the replicas may be able to decode the message received via wireless and the other not, despite the fact that both systems and antennas interfaces are located very close to each other.

Based on this, an atomic commit protocol was developed in order to guarantee consistency among both replicas [64]. The proposed solution relies on a dedicated wired link exclusively shared by each primary-backup pair of RSUs. Besides enforcing replica determinism, it also reduces packet loss, since only one of the replicas needs to successfully decode the packet in order for it to become available to both units. This strategy however, introduces some overhead in the packet delivery process to the upper layers of the communications protocol.

The proposed replication scheme introduces low delay in the recovery procedure of the failed primary replica. A timing analysis was conducted (Paper D), proving that the real-time properties of V-FTT protocol can still be preserved under the presence of RSU failures. It is still possible to achieve a small IFS value that assures no *alien* node will be able to interfere with the collision-free period of the protocol. Only under specific circumstances in a multiple RSUs scenario, a non-compliant node would have the opportunity to interfere with the time-triggered transmissions. Nevertheless, some alternatives solutions are available to avoid this effect, as reported in this work.

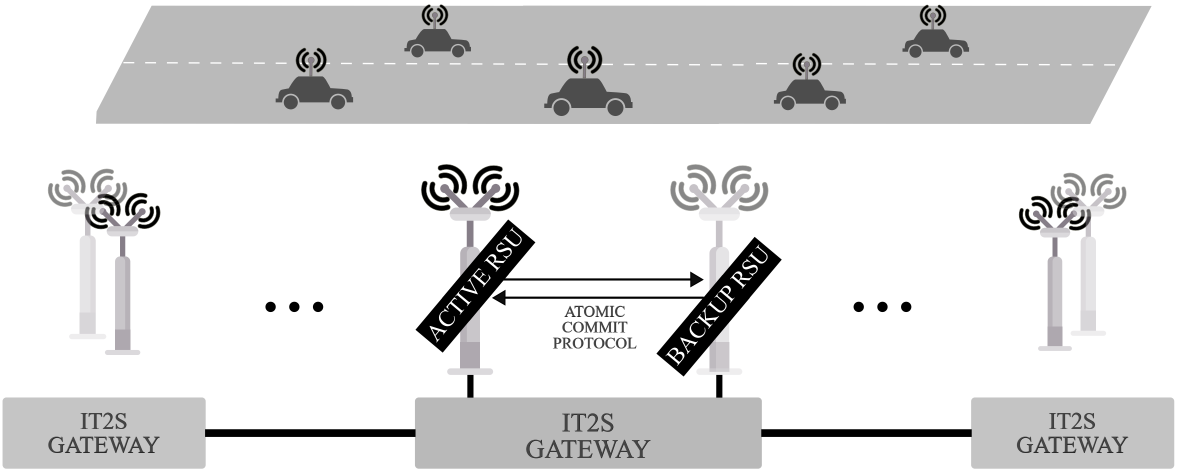


Figure 4.6: RSU replication scheme.

4.4.3 OBU's Medium Guardian

Finally, the mobile nodes should also exhibit fail-silent behaviour, since failures in those units may also affect the remaining communications taking place in the channel. A solution similar to the one employed in the RSU nodes, could also be applied to the vehicle OBUs. However, their role in the deterministic protocol is not as critical as the one from the master nodes and therefore a more inexpensive one can be pursued.

A solution based on the complete duplication of resources can still be adopted in special cases where strict fail-silence enforcement in both value and time domains could be necessary, for instance in police or emergency vehicles. For regular vehicles, an alternative solution is proposed in this work (Paper E) that takes into account the concurrent factors previously mentioned. The suggested method relies not on complete system's replication but on the utilization of behavioural error detection techniques. More emphasis is placed on limiting OBU's ability to transmit uncontrollably, which corresponds to fail-silence enforcement in the time domain.

The followed strategy adds a new device to the OBU's architecture, designated as medium guardian, that monitors node's operation. The medium guardian also receives the scheduling messages from RSU nodes and retrieves information about the expected behaviour of the OBU, i.e. the time slot in which it is supposed to transmit. On the other hand, when the OBU transmits its message, the guardian verifies if the transmission is taking place at the right moment. If not, the OBU's operation is immediately disabled, avoiding any further interference in the wireless medium.

The above operation is depicted in figure 4.7. Additional verifications are also performed by the medium guardian, namely with respect to the frame header of the message containing node's identification and other important information. The obtained results demonstrate the effectiveness of the proposed methodology, with very small error detection latency values.

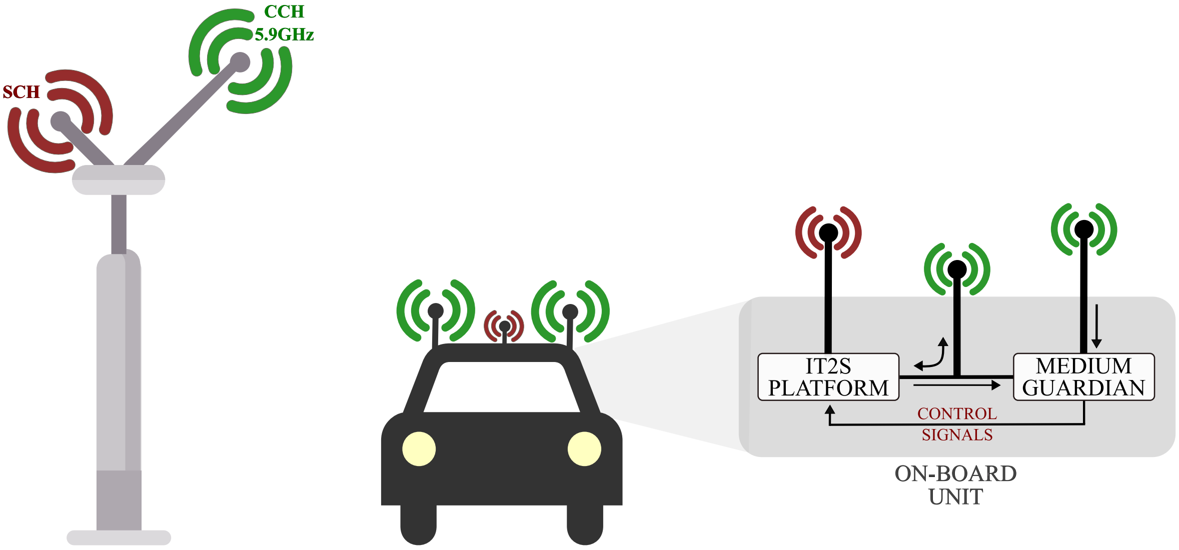


Figure 4.7: OBU's medium guardian.

This way, it is possible to enforce fail-silent behaviour in the mobile nodes of the network and at the same time fulfil the real-time requirements of V-FTT protocol.

4.5 Conclusion

In summary, mechanisms to enhance dependability in real-time vehicular networks are required in order to satisfy the safety-critical requirements posed in such dynamic environments. The presence of the infrastructure plays a key role in the design of a fault-tolerant architecture that relies on the support provided by the RSUs. The design of the proposed mechanisms took advantage of a deterministic MAC protocol (V-FTT) specifically tailored for wireless vehicular communications, in order to meet the real-time requisites of the road traffic system. Nevertheless, the concepts developed here are protocol independent and can be applied to other technologies or wireless systems.

CHAPTER 5

Conclusions and Future Work

This chapter summarizes the main conclusions of this thesis and presents some possible directions for the future work.

5.1 Conclusions

The work developed in the scope of this PhD thesis focused on the design of mechanisms to enhance the dependability attributes of wireless vehicular networks. The main goal was to provide solutions that could support the development of cooperative traffic applications targeting road safety. In this context, the real-time requirements of such safety-critical services are of uttermost importance. Another aspect to take into account consists in the fact that vehicular networks are extremely dynamic and operate in conditions very difficult to predict. The propagation scenario and the frequent connectivity disruptions caused by the inherent mobility of the radio links, pose several challenges to the design of a dependable distributed system like this. For that reason, it is very important to combine system's flexibility with real-time requirements and fault-tolerance capabilities. With appropriate strategies, it is possible to increase reliability and the confidence users can have in the operation of vehicular communications systems.

At the beginning of this document, the basic concepts of dependability and real-time systems were introduced. Important aspects of fault-tolerance and the different types of redundancy techniques were discussed. Similarly, the fundamental background on wireless vehicular communications was also presented. In this part, the most relevant standards were described, with special reference to the distinctive features introduced in the novel set of protocols. Finally, a detailed description of a custom vehicular communications platform was provided, given its importance to the test and implementation of the mechanisms proposed in the scope of this PhD. This reconfigurable station, named IT2S Platform, is compliant with both the IEEE WAVE and ETSI ITS-G5, the corresponding protocol stacks in the United States and Europe, respectively. It is based on reconfigurable hardware and open-source software, thus providing flexibility and the capacity to suit different purposes.

Following this introductory section, a survey on fault-tolerance techniques for wireless vehicular communications was conducted, in order to analyse the state-of-the-art in the research field of this thesis. The selection of papers in journals and conference proceedings followed a systematic review process based on the PRISMA Statement, a methodology often used to identify relevant research work in a specific scientific area. After collecting and screening the results, 19 articles were selected based on a set of criteria. Each one of these papers was analysed and classified according to the type of redundancy used to achieve fault-tolerance properties. Finally, a summary of the main contributions of each research work was provided.

After that, the core contributions of this PhD thesis were presented and discussed. Firstly, an efficient digital filter design was introduced in order to mitigate the interference problems in the receiver nodes of vehicular networks. A multi-rate system approach was followed, with the main goal of optimizing the hardware resources used and the time delay introduced in the reception chain. The simulation results proved that the proposed filter can effectively attenuate the interfering signal while preserving the desired transmission.

The fault-tolerant architecture for infrastructure-based vehicular networks was then introduced, constituting the key contribution of this research work. The proposed network architecture relies on a real-time MAC protocol that guarantees deterministic end-to-end delay values. In this framework, several mechanisms are employed to ensure fault-tolerant behaviour in the mobile nodes as well as in the fixed nodes of vehicular networks. The infrastructure plays an important role in coordinating all communications in the wireless channel.

For that reason, the RSU nodes are equipped with a fail-silence enforcement mechanism that prevents these stations from sending invalid messages to the wireless medium. Additionally, an active replication scheme is utilized to guarantee that in case of failure of the primary node, a backup unit will immediately replace its operation. This way, it is possible to provide a continuous service even in spite of faults that could potentially affect system's performance. An analysis of the timing properties of the deterministic MAC protocol under the presence of these fault-tolerance mechanisms in the RSU nodes, demonstrates that the real-time guarantees can still be met.

On the OBUs, a medium guardian device is proposed in order to monitor node's operation both in value and time domains. This medium guardian concept is inspired in the bus guardian units from fieldbus technologies, guaranteeing error isolation from the rest of the network. All OBU's messages are analysed by the medium guardian and if any fault is detected, the transmission interface of the node is permanently disabled. This way, one can guarantee that the deterministic operation of the communications protocol is not affected by a faulty OBU node.

The proposed fault-tolerance mechanisms aim to improve the dependability attributes of real-time vehicular communications. Only by introducing some type of redundancy in vehicular network nodes, it is possible to make their operation more predictable and reliable. This way, the contributions of this thesis help to pave the way for a more dependable and thus safer road traffic system.

5.2 Future Work

As can be concluded from the state-of-the-art analysis on fault-tolerance techniques for vehicular networks, there is still a lot of room for research work on this topic. Despite the various contributions from this PhD thesis, alternative architectures and mechanisms are required to handle different scenarios that commonly arise in vehicular environments. For instance, there might be situations where the cost of installing road-side infrastructure can be prohibitively expensive and a highly dependable ad-hoc solution is still required. With the deployment and dissemination of self-driving cars, different network schemes might be more appropriate. Also security threats will need to be on the top of the list of priorities during the design phase of future vehicular communications systems.

With respect to the fault-tolerant mechanisms developed in the scope of this thesis, it would be important to develop a reliability analysis of the proposed system architecture. An analytical framework may provide a good starting point for this evaluation. In this context, graph theory and Continuous-Time Markov Chain (CTMC) could constitute interesting tools for the reliability analysis [65]. However, it would be necessary to estimate all system's components failure rates, which is obviously not easy given the lack of information provided by the manufacturers. Additionally, several assumptions would be required to make this task feasible. For instance, it would probably be necessary to assume that all component have constant failure rates, fail independently from each other and there are no multiple failures at the same time.

The subsequent step would be the integration of the fault-tolerant capabilities of the system in an actual field trial. This way, it would be possible to evaluate the dependability attributes of the proposed architecture in a close to the real-world scenario. It would require the installation of the fail-silent RSUs and backup nodes in the road-side infrastructure and medium guardian devices in the mobile OBUs. In order to be effective, this experimental assessment on the field would also require fault injection mechanisms, otherwise the system could undergo a long period of time without experiencing any fault.

Another possible line of work could be the application of the proposed methods to other research contexts. It should be pointed out once more that the concepts and techniques developed during this work are not protocol-dependent and thus can be adapted to other wireless technologies and application scenarios. For example, the dependable network architecture and the corresponding fault-tolerance mechanisms can be adjusted and tested in different wireless domains, such as industrial communications, Unmanned Aerial Vehicles (UAVs), robotics applications, etc.

Finally, an important aspect that should be taken into account in the design of dependable vehicular networks is the fact that there are many recent developments in the area of wireless systems in general. One of the trends is the concept of full duplex radio, which can soon be available to be applied in a myriad of commercial applications. There is already some exploratory research focusing on the integration of full duplex radios in wireless vehicular communications and taking advantage of its properties [66] [67] [68]. Hybrid communications, cognitive radios and the maturity of 5G technology will also play a key role in future wireless communications systems and will be able to provide complementary solutions to the current standards available for the design of vehicular communications [69] [70] [71].

References

[1] World Health Organization, *Global Status Report on Road Safety 2015*, http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/, Accessed 6 December 2017.

[2] E. Comission, *Statistics - accidents data*, http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm, Accessed 21 March 2016, 2016.

[3] Vision Zero Initiative, *Traffic Safety by Sweden*, http://www.visionzeroinitiative.com/, Accessed 6 December 2017.

[4] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds", in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, Mar. 2014, pp. 241–246. DOI: 10.1109/WF-IoT.2014.6803166.

[5] BMW Group, *BMW ConnectedDrive at the IFA 2015 consumer electronics show in Berlin.* https://www.press.bmwgroup.com/global/article/detail/T0232769EN/bmwconnecteddrive-at-the-ifa-2015-consumer-electronics-show-inberlin, Accessed 28 May 2016.

[6] H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications.* Norwell, MA, USA: Kluwer Academic Publishers, 1997.

[7] 5GPP, *The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services*, https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf, Accessed 28 February 2016.

[8] ITU-R, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf, Accessed 28 February 2016.

[9] K. Bilstrup, E. Uhlemann, E. Ström, and U. Bilstrup, "On the Ability of the 802.11p MAC Method and STDMA to Support Real-Time Vehicle-to-Vehicle Communication", *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–13, 2009, ISSN: 1687-1499. DOI: 10.1155/2009/902414. [Online]. Available: http://dx.doi.org/10.1155/2009/902414.

[10] D. Eckhoff, N. Sofra, and R. German, "A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE", in *Wireless On-demand Network Systems and Services (WONS), 2013 10th Annual Conference on*, Mar. 2013, pp. 196–200.

[11] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, Mar. 2012.

[12] S. Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard", in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, Sep. 2007, pp. 2199–2203. DOI: 10.1109/VETECF.2007.461.

[13] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC multi-channel operations and its implications on vehicle safety communications", in *Vehicular Networking Conference (VNC), 2009 IEEE*, Oct. 2009, pp. 1–8.

[14] J. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, ISSN: 0018-9219. DOI: 10.1109/JPROC.2011.2132790.

[15] A. S. Tanenbaum and M. Van Steen, *Distributed Systems*, 3rd. CreateSpace Independent Publishing Platform, 2017.

[16] G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair, *Distributed Systems: Concepts and Design*, 5th. USA: Addison-Wesley Publishing Company, 2011.

[17] G. C. Buttazzo, *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications*, 3rd. Springer Publishing Company, Incorporated, 2011, ISBN: 978-1-4614-0675-4.

[18] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *Dependable and Secure Computing, IEEE Transactions on*, vol. 1, no. 1, pp. 11–33, Jan. 2004.

[19] J. C. Laprie, A. Avizienis, and H. Kopetz, Eds., *Dependability: Basic Concepts and Terminology.* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1992.

[20] S. Chumkamon, P. Tuvaphanthaphiphat, and P. Keeratiwintakorn, "The vertical handoff between GSM and Zigbee networks for vehicular communication", in *ECTI-CON2010: The 2010 ECTI International Confernce on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, May 2010, pp. 603–606.

[21] W. Bronzi, R. Frank, G. Castignani, and T. Engel, "Bluetooth low energy for inter-vehicular communications", in *2014 IEEE Vehicular Networking Conference (VNC)*, Dec. 2014, pp. 215–221. DOI: `10.1109/VNC.2014.7013351`.

[22] M. Uysal, Z. Ghassemlooy, A. Bekkali, A. Kadri, and H. Menouar, "Visible Light Communication for Vehicular Networking: Performance Study of a V2V System Using a Measured Headlamp Beam Pattern Model", *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 45–53, Dec. 2015, ISSN: 1556-6072. DOI: `10.1109/MVT.2015.2481561`.

[23] A. Böhm, K. Lidström, M. Jonsson, and T. Larsson, "Evaluating CALM M5-based vehicle-to-vehicle communication in various road settings through field trials", in *IEEE Local Computer Network Conference*, Oct. 2010, pp. 613–620. DOI: `10.1109/LCN.2010.5735781`.

[24] F. A. Teixeira, V. F. e Silva, J. L. Leoni, D. F. Macedo, and J. M. Nogueira, "Vehicular networks using the IEEE 802.11p standard: An experimental analysis", *Vehicular Communications*, vol. 1, no. 2, pp. 91–96, 2014, ISSN: 2214-2096. DOI: `https://doi.org/10.1016/j.vehcom.2014.04.001`. [Online]. Available: `http://www.sciencedirect.com/science/article/pii/S2214209614000151`.

[25] A. Festag, "Standards for vehicular communication—from IEEE 802.11p to 5G", *E & I Electrical Engineering and Information Technology*, vol. 132, pp. 409–416, 7 Nov. 2015. DOI: `10.1007/s00502-015-0343-0`.

[26] R. Molina-Masegosa and J. Gozalvez, "LTE-V for Sidelink 5G V2X Vehicular Communications: A New 5G Technology for Short-Range Vehicle-to-Everything Communications", *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 30–39, Dec. 2017, ISSN: 1556-6072. DOI: `10.1109/MVT.2017.2752798`.

[27] S. Mumtaz, K. M. S. Huq, M. I. Ashraf, J. Rodriguez, V. Monteiro, and C. Politis, "Cognitive vehicular communication for 5G", *IEEE Communications Magazine*, vol. 53, no. 7, pp. 109–117, Jul. 2015, ISSN: 0163-6804. DOI: `10.1109/MCOM.2015.7158273`.

[28] 5G Automotive Association, *Vision and Mission: Building the future of connected mobility*, http://5gaa.org/about-5gaa/vision-mission/, Accessed 12 January 2018.

[29] J. Choi, V. Va, N. Gonzalez-Prelcic, R. Daniels, C. R. Bhat, and R. W. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", *IEEE Communications Magazine*, vol. 54, no. 12, pp. 160–167, Dec. 2016, ISSN: 0163-6804. DOI: `10.1109/MCOM.2016.1600071CM`.

[30] J. Almeida, "Plataforma multi-rádio para comunicações veiculares DSRC 5.9 GHz", Universidade de Aveiro, 2013.

[31] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz, "Inter-vehicle communication: Quo vadis", *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 170–177, Jun. 2014, ISSN: 0163-6804. DOI: `10.1109/MCOM.2014.6829960`.

[32] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement”, *BMJ*, vol. 339, 2009. DOI: 10.1136/bmj.b2535. [Online]. Available: http://www.bmj.com/content/339/bmj.b2535.

[33] M. Jonsson, K. Kunert, and A. Böhm, “Increased Communication Reliability for Delay-Sensitive Platooning Applications on Top of IEEE 802.11p”, in *Communication Technologies for Vehicles: 5th International Workshop, Nets4Cars/Nets4Trains 2013, Villeneuve d’Ascq, France, May 14-15, 2013. Proceedings*, M. Berbineau, M. Jonsson, J.-M. Bonnin, S. Cherkaoui, M. Aguado, C. Rico-Garcia, H. Ghannoum, R. Mehmood, and A. Vinel, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 121–135, ISBN: 978-3-642-37974-1. DOI: 10.1007/978-3-642-37974-1_10. [Online]. Available: https://doi.org/10.1007/978-3-642-37974-1_10.

[34] E. V. Matthiesen, O. Hamouda, M. Kaâniche, and H.-P. Schwefel, “Dependability Evaluation of a Replication Service for Mobile Applications in Dynamic Ad-Hoc Networks”, in *Service Availability*, T. Nanya, F. Maruyama, A. Pataricza, and M. Malek, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 171–186, ISBN: 978-3-540-68129-8.

[35] R. Kumar and M. Dave, “DDDRC: decentralised data dissemination in VANET using raptor codes”, *International Journal of Electronics*, vol. 102, no. 6, pp. 946–966, 2015. DOI: 10.1080/00207217.2014.945193. [Online]. Available: https://doi.org/10.1080/00207217.2014.945193.

[36] A. Böhm and K. Kunert, “Data age based MAC scheme for fast and reliable communication within and between platoons of vehicles”, in *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2016, pp. 1–9. DOI: 10.1109/WiMOB.2016.7763224.

[37] E. Cambruzzi, J. M. Farines, R. J. Macedo, and W. Kraus, “An adaptive failure detection system for Vehicular Ad-hoc Networks”, in *2010 IEEE Intelligent Vehicles Symposium*, Jun. 2010, pp. 603–608. DOI: 10.1109/IVS.2010.5548015.

[38] E. E. C., S. Zhang, and E. Liu, “Improving Reliability of Message Broadcast over Internet of Vehicles (IoVs)”, in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Oct. 2015, pp. 2321–2328. DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.343.

[39] V. Savic, E. M. Schiller, and M. Papatriantafilou, “Distributed algorithm for collision avoidance at road intersections in the presence of communication failures”, in *2017 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2017, pp. 1005–1012. DOI: 10.1109/IVS.2017.7995846.

[40] K. Abrougui, A. Boukerche, and H. Ramadan, “Performance evaluation of an efficient fault tolerant service discovery protocol for vehicular networks”, *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1424–1435, 2012, Service Delivery Management in Broadband Networks, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2011.10.007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804511001949.

[41] Y.-C. Chang and T.-P. Wang, “A fault-tolerant broadcast protocol for reliable alert message delivery in vehicular wireless networks”, in *7th International Conference on Communications and Networking in China*, Aug. 2012, pp. 475–480. DOI: 10.1109/ChinaCom.2012.6417530.

[42] G. L. Lann, “On the Power of Cohorts – Multipoint Protocols for Fast and Reliable Safety-Critical Communications in Intelligent Vehicular Networks”, in *2012 International Conference on Connected Vehicles and Expo (ICCVE)*, Dec. 2012, pp. 35–42. DOI: 10.1109/ICCVE.2012.15.

[43] D. Sanderson and J. Pitt, “Institutionalised Consensus in Vehicular Networks: Executable Specification and Empirical Validation”, in *2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops*, Sep. 2012, pp. 71–76. DOI: 10.1109/SASOW.2012.21.

[44] N. Aljeri, M. Almulla, and A. Boukerche, “An Efficient Fault Detection and Diagnosis Protocolfor Vehicular Networks”, in *Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet ’13, Barcelona, Spain: ACM, 2013, pp. 23–30, ISBN: 978-1-4503-2358-1. DOI: 10.1145/2512921.2512935. [Online]. Available: http://doi.acm.org/10.1145/2512921.2512935.

[45] A. Casimiro, J. Kaiser, E. M. Schiller, P. Costa, J. Parizi, R. Johansson, and R. Librino, “The KARYON project: Predictable and safe coordination in cooperative vehicular systems”, in *2013 43rd Annual*

IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Jun. 2013, pp. 1–12. DOI: 10.1109/DSNW.2013.6615530.

[46] S. Worrall, G. Agamennoni, J. Ward, and E. Nebot, "Fault Detection for Vehicular Ad Hoc Wireless Networks", *Intelligent Transportation Systems Magazine, IEEE*, vol. 6, no. 2, pp. 34–44, Summer 2014, ISSN: 1939-1390. DOI: 10.1109/MITS.2014.2304974.

[47] J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Fault Tolerance of Cooperative Vehicle Platoons Subject to Communication Delay", *IFAC-PapersOnLine*, vol. 48, no. 12, pp. 352–357, 2015, 12th IFAC Workshop onTime Delay SystemsTDS 2015, ISSN: 2405-8963. DOI: https://doi.org/10.1016/j.ifacol.2015.09.403. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2405896315015062.

[48] N. Fathollahnejad, R. Pathan, and J. Karlsson, "On the probability of unsafe disagreement in group formation algorithms for vehicular ad hoc networks", in *2015 11th European Dependable Computing Conference (EDCC)*, Sep. 2015, pp. 256–267. DOI: 10.1109/EDCC.2015.29.

[49] S. Bhoi and P. Khilar, "Self soft fault detection based routing protocol for vehicular ad hoc network in city environment", *Wireless Networks*, vol. 22, no. 1, pp. 285–305, Jan. 2016. DOI: 10.1007/s11276-015-0970-8.

[50] M. Elhadef, "A Fault-Tolerant Intersection Control Algorithm Under the Connected Intelligent Vehicles Environment", in *Advanced Multimedia and Ubiquitous Engineering*, ser. Lecture Notes in Electrical Engineering, J. Y. Park J. Jin H. and K. M., Eds., vol. 393, Springer Singapore, 2016, pp. 243–253. DOI: 10.1007/978-981-10-1536-6_33.

[51] K. Medani, M. Aliouat, and Z. Aliouat, "Fault tolerant time synchronization using offsets table robust broadcasting protocol for vehicular ad hoc networks", *AEU - International Journal of Electronics and Communications*, vol. 81, pp. 192–204, 2017, ISSN: 1434-8411. DOI: https://doi.org/10.1016/j.aeue.2017.07.026. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S143484111730256X.

[52] L. Lamport, "The Part-time Parliament", *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998, ISSN: 0734-2071. DOI: 10.1145/279227.279229. [Online]. Available: http://doi.acm.org/10.1145/279227.279229.

[53] ETSI TR 102 654 (V1.1.1), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Co-location and Co-existence Considerations regarding Dedicated Short Range Communication (DSRC) transmission equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range and other potential sources of interference*, Jan. 2009.

[54] J. Lansford, J. B. Kenney, and P. Ecclesine, "Coexistence of unlicensed devices with dsrc systems in the 5.9 ghz its band", in *2013 IEEE Vehicular Networking Conference*, Dec. 2013, pp. 9–16. DOI: 10.1109/VNC.2013.6737584.

[55] Y. Park and H. Kim, "On the coexistence of IEEE 802.11ac and WAVE in the 5.9 GHz Band", *IEEE Communications Magazine*, vol. 52, no. 6, pp. 162–168, Jun. 2014, ISSN: 0163-6804. DOI: 10.1109/MCOM.2014.6829959.

[56] C. Campolo, A. Molinaro, and A. Vinel, "Understanding adjacent channel interference in multi-channel VANETs", in *Vehicular Networking Conference (VNC), 2014 IEEE*, Dec. 2014, pp. 101–104. DOI: 10.1109/VNC.2014.7013316.

[57] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication", *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 36–43, Oct. 2006.

[58] G. Bansal and J. Kenney, "Controlling Congestion in Safety-Message Transmissions: A Philosophy for Vehicular DSRC Systems", *IEEE Vehicular Technology Magazine*, vol. 8, no. 4, pp. 20–26, Dec. 2013, ISSN: 1556-6072. DOI: 10.1109/MVT.2013.2281675.

[59] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs", *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 119–125, Nov. 2008.

[60] P. Veríssimo, "Uncertainty and predictability: Can they be reconciled?", in *Future Directions in Distributed Computing*, Springer-Verlag LNCS 2584, May 2003.

[61] T. Meireles, J. Fonseca, and J. Ferreira, “The Case for Wireless Vehicular Communications Supported by Roadside Infrastructure”, in *Intelligent Transportation Systems Technologies and Applications*, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, Eds., John Wiley & Sons, Ltd, 2015, pp. 57–82, ISBN: 9781118894774. DOI: 10.1002/9781118894774.ch4. [Online]. Available: http://dx.doi.org/10.1002/9781118894774.ch4.

[62] L. Silva, P. Pedreiras, and J. Alam Muhammad Ferreira, “STDMA-based Scheduling Algorithm for Infrastructured Vehicular Networks”, in *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira, and J. Fonseca, Eds., Cham: Springer International Publishing, 2016, ch. 4, pp. 81–105, ISBN: 978-3-319-28183-4. DOI: 10.1007/978-3-319-28183-4_4.

[63] A. Khan, J. Almeida, B. Fernandes, M. Alam, P. Pedreiras, and J. Ferreira, “Towards Reliable Wireless Vehicular Communications”, in *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, Sep. 2015, pp. 167–172. DOI: 10.1109/ITSC.2015.36.

[64] J. Almeida, J. Ferreira, P. Oliveira Arnaldo S. R. and Pedreiras, and J. Fonseca, “Enforcing Replica Determinism in the Road Side Units of Fault-Tolerant Vehicular Networks”, in *Future Intelligent Vehicular Technologies*, J. Ferreira and M. Alam, Eds., Cham: Springer International Publishing, 2017, pp. 3–12, ISBN: 978-3-319-51207-5.

[65] D. Gessner, J. Proenza, M. Barranco, and P. Portugal, “Towards a reliability analysis of the design space for the communication subsystem of FT4FTT”, in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Sep. 2014, pp. 1–4. DOI: 10.1109/ETFA.2014.7005298.

[66] C. Campolo, A. Molinaro, and A. O. Berthet, “Improving CAMs broadcasting in VANETs through full-duplex radios”, in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sep. 2016, pp. 1–6. DOI: 10.1109/PIMRC.2016.7794821.

[67] C. Campolo, A. Molinaro, A. O. Berthet, and A. Vinel, “Full-Duplex Radios for Vehicular Communications”, *IEEE Communications Magazine*, vol. 55, no. 6, pp. 182–189, 2017, ISSN: 0163-6804. DOI: 10.1109/MCOM.2017.1600391.

[68] A. Bazzi, C. Campolo, B. M. Masini, A. Molinaro, A. Zanella, and A. O. Berthet, “Enhancing Cooperative Driving in IEEE 802.11 Vehicular Networks through Full-Duplex Radios”, *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, pp. 1–1, 2018, ISSN: 1536-1276. DOI: 10.1109/TWC.2018.2794967.

[69] E. Abd-Elrahman, A. M. Said, T. Toukabri, H. Afifi, and M. Marot, “A hybrid model to extend vehicular intercommunication V2V through D2D architecture”, in *2015 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2015, pp. 754–759. DOI: 10.1109/ICCNC.2015.7069441.

[70] A. Paul, A. Daniel, A. Ahmad, and S. Rho, “Cooperative Cognitive Intelligence for Internet of Vehicles”, *IEEE Systems Journal*, vol. 11, no. 3, pp. 1249–1258, Sep. 2017, ISSN: 1932-8184. DOI: 10.1109/JSYST.2015.2411856.

[71] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, “5G for Vehicular Communications”, *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, Jan. 2018, ISSN: 0163-6804. DOI: 10.1109/MCOM.2018.1700467.

Appended Papers

Paper A

Mitigating Adjacent Channel Interference in Vehicular Communication Systems

João Almeida, Muhammad Alam, Joaquim Ferreira and Arnaldo S. R. Oliveira

in *Digital Communications and Networks*, vol. 2, no. 2, pp. 57-64, 2016

The format has been revised.

Mitigating Adjacent Channel Interference in Vehicular Communication Systems

João Almeida, Muhammad Alam, Joaquim Ferreira and Arnaldo S. R. Oliveira

Abstract

In the last decades, dedicated wireless channels were specifically allocated to enable the development and implementation of vehicular communications systems. The two main protocol stacks, the WAVE standards proposed by the IEEE in the United States and the ETSI ITS-G5 in Europe, reserved 10 MHz wide channels in the 5.9 GHz spectrum band. Despite the exclusive use of these frequencies for vehicular communication purposes, there are still cross channel interference problems that have been widely reported in the literature. In order to mitigate these issues, this paper presents the design of a two-stage FIR low-pass filter, targeting the integration with a digital baseband receiver chain of a custom vehicular communications platform. The filter was tested, evaluated and optimized, with the simulation results proving the effectiveness of the proposed method and the low delay introduced in the overall operation of the receiver chain.

A.1 Introduction

Vehicular communications play a key role in the development of Intelligent Transportation Systems (ITS), whose main goal is the improvement of road safety and traffic efficiency. By extending the driver's field of view, vehicular networks can increase the time available to make decisions or to react in case of traffic hazards. This way for instance, collisions in low visibility intersections and chain reaction crashes can be drastically reduced. In addition to this, value-added infotainment services can also be provided by vehicular communication systems, such as broadband internet connection or prices and locations of parking slots or gas stations.

There are two main protocol stacks for vehicular communications systems [1], enabling exchange of data among vehicles (V2V communications) and between vehicles and the road-side infrastructure (V2I/I2V). These two families of standards correspond to the IEEE Wireless Access in Vehicular Environments (WAVE), adopted in the United States, and the ETSI ITS-G5 in Europe. At the physical and medium access control layers, both protocol stacks rely on the IEEE 802.11p standard, an amendment to the IEEE 802.11 Wi-Fi reference [2]. In comparison with the typical Wi-Fi operation, there was just a few number of modifications that were introduced to enhance the behaviour of the communicating nodes under such dynamic scenarios. For instance, the channel bandwidth was reduced from 20 MHz to 10 MHz, in order to mitigate the effects of multi-path propagation and Doppler shift. As a consequence, the data rate is half of what can be obtained with standard Wi-Fi, i.e., from 3 Mb/s to 27 Mb/s instead of 6 to 54 Mbit/s. Another example is the introduction of non-IP messages that are broadcast outside the context of a Basic Service Set (BSS), avoiding the overhead introduced by the registration and authentication procedures, commonly present in wireless local area networks.

In order to guarantee that vehicular communications do not suffer any type of interference from unlicensed devices, the Federal Communications Commission (FCC) in the United States and the European Conference of Postal and Telecommunications Administrations (CEPT) in Europe, allocated a dedicated spectrum band at 5.9 GHz (Figure A.1). In America, a bandwidth of 75 MHz was reserved, while in Europe only 50 MHz were assigned. This spectrum was divided into smaller 10 MHz wide channels and in the American case, a 5 MHz guard band at the low end was also included. As a result, there are 7 different channels for IEEE WAVE operation and 5 for the case of ETSI ITS-G5. In Europe, 30 MHz (3 channels) are reserved for road safety in the ITS-G5A band and 20 MHz are assigned for general purpose ITS services in the ITS-G5B band. As a general rule, a control channel (CCH 178 in the USA and CCH 180 in Europe) is exclusively used for cooperative road safety and control information. The remaining channels are designated as service channels (SCH). In the United States, concerns about the reduced capacity for road safety messages led to the decision to allocate SCH 172 specifically for applications regarding public safety of life and property [3]. Moreover, it is mandatory in Europe to have two radios in each vehicular communications platform, in order to guarantee at least one radio always tuned in the dedicated safety channel

[4].

Notwithstanding the decision to allocate specific wireless channels for vehicular communications purposes, there are still issues with the operation of these systems, caused by the cross channel interference in the IEEE- WAVE/ETSI-ITS-G5 band and with the European tolling systems operating in the 5.8 GHz frequency band. The interference risks in the latter case were early identified by CEPT in 2007 [5] and several studies [6][7][8], simulation and experimental tests [9] were then conducted in order to evaluate the impact of ITS-G5 communications in a coexistence scenario with electronic toll collection (ETC) systems. In these tests [9] organized by ETSI, the results have shown that under certain conditions, the ITS-G5 signals can harmfully interfere with ETC systems, causing a loss or non-completion of ETC transactions and/or a disruption of the stand-by mode of ETC on-board units (OBUs), i.e. the devices placed inside the vehicles.

Based on these findings, it was clear that the simultaneous operation of both systems at toll plazas could be seriously disturbed. This could lead to safety and congestion problems in these areas and cause substantial loss of revenues for road operators. It was also concluded that this interference is inevitable, unless ITS-G5 will adapt the transmitted power within a certain range around the tolling station or reduce the duty cycle of the message transmission. As a result, ETSI has introduced mandatory requirements for ITS-G5 stations to switch to a “protected mode” [7]. This shall be done when receiving information from any other ITS station containing the location of a tolling station. The ITS station that sends out the information about the tolling station location may either be a fixed located transmitter - road-side unit (RSU) - in the vicinity of the tolling station, or it may also be an OBU in any vehicle that, in addition, is equipped with a 5.8 GHz toll detector.

Furthermore, there is also a perspective to use IEEE 802.11p for ETC communications, but studies [10] have shown it is possible that 802.11a based on-board devices operating in the 5 GHz band could degrade the performance of ETC systems based on vehicular communications. Simulation and real-world experiments [10] demonstrated an increase in the packet error rate (PER) of the ETC 802.11p based system, when both technologies were working simultaneously. It was also shown that this effect cannot be removed by simply increasing the power transmitted by the 802.11p ETC units. In general, one can conclude that wireless communication systems operating near the 5.9 GHz frequency band pose serious problems to the performance of vehicular networks.

Nevertheless, the major source of interference in vehicular communications systems is the cross channel interference, generated by nodes communicating in the adjacent channels [11]. This adjacent channel interference (ACI) can severely compromise the integrity of the messages received by a radio unit, whenever simultaneous communications occur in the nearby channels. Therefore, and in order to reduce the effect of ACI in vehicular communications radio links, this paper presents the design of a two-stage Finite Impulse Response (FIR) filter, which guarantees an efficient suppression of the unwanted components of the received signal. At the same time, it is also ensured that few digital hardware resources are utilized and only a small delay is introduced in the receiver chain of the ITS-G5 station. The rest of the paper is organized as follows. Section A.2 presents some related work and background on the topic of ACI in vehicular networks. Section A.3 shows the effects of cross channel interference in the received signal of a custom vehicular communications platform, while section A.4 describes the design of the proposed digital filter and presents the obtained simulation results. Finally, section A.5 summarizes the concluding remarks and discusses some future work.

A.2 Related Work and Background

The IEEE WAVE and ETSI ITS-G5 protocol stacks establish a multi-channel architecture for vehicular communications, where different vehicles in the same geographical area can simultaneously transmit over the multiple channels presented in Figure A.1. This design decision produces obvious throughput improvements, however, since the parallel usage of adjacent channels can occur when vehicles are in the radio range of each others, interference between different nodes' transmissions may arise. This adjacent channel interference (ACI) can cause two main negative effects in the network communications [11]: an increased PER and a reduced transmission opportunity. In the former case, the signal-to-interference-plus-noise-ratio (SINR) of a packet being received by a node can be increased by another unit communicating in an adjacent channel, which may lead to the impossibility of correctly processing and decoding the frame. This will cause the loss of the packet and, if the situation is not momentary, it can result in large values of PER. The second mentioned effect occurs when an node wants to transmit a frame, but it perceives the channel as occupied due to a packet transmission in an adjacent channel. This channel busy indication is given by the clear channel assessment (CCA) mechanism, being triggered by the power level sensed in the wireless medium, raised by the interferer in the nearby channel. In this situation, the potential transmitter will follow the back-off procedure specified by the CSMA method of IEEE 802.11 standard and thus the access to the wireless medium and the transmission of the intended message will be deferred. Moreover, it can happen that the packet decoding process in the potential receivers is not affected by the interferer, but the transmitter is still wrongly

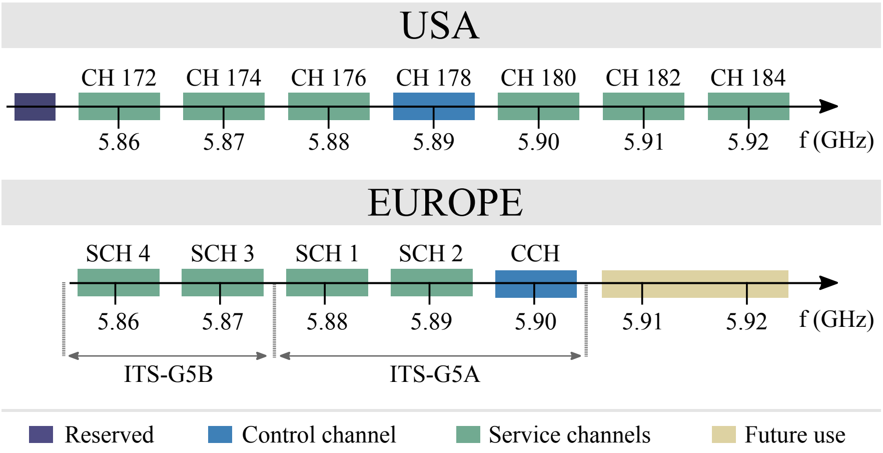


Figure A.1: Spectrum allocation for vehicular communications (adapted from [1]).

prevented to send its message. The ACI problem could be amplified in dual-radio units, as the ones in Europe, with antennas simultaneously operating on nearby channels and located in the same place, either in the same vehicle or road-side site.

In order to limit cross channel interference, the standard [2] specifies a spectrum emission mask that defines the out-of-band energy allowed for a transmitting device. This spectral mask is defined up to 15 MHz far from the center frequency and it becomes more stringent and difficult to comply with higher transmit power classes (A to D) [12]. On the receiver side, the standardization rules also establish a minimum adjacent channel rejection (ACR) ratio for each modulation, measured by the power difference between the interfering signal and the signal in the desired channel. These masks are sufficient to avoid the most harmful interferences, particularly in the cases related to the blocking transmission effect. Nevertheless the impact on the PER can still be very severe under certain circumstances. Some preliminary field test results, proved the large number of packet errors when an interferer working in an adjacent channel is close to the receiver node [13]. The distance for which the ACI effect starts to be critical (a PER higher than 10%) was measured and occurs whenever the interferer is closer than the intended transmitter to the receiver by an order of magnitude or more. Similar results were obtained in experimental simulations [14] [15] and other field trial tests [16] [17], confirming that the effect of cross channel interference cannot be neglected, specially under heavy traffic load conditions.

This issue is partially addressed in [18] by a token ring MAC protocol named MCTRP, aiming to improve throughput over all WAVE channels. The adaptive algorithm establishes virtual rings where groups of vehicles are organized, each one communicating in a specific service channel. By switching to a different SCH when the interference level increases, the protocol is able to reduce the ACI of a virtual ring. In [14], a preliminary solution to mitigate cross channel interference is proposed (Cross Channel CSMA/CA or 3CSMA/CA protocol), by reducing transmission power on the adjacent channel and by delaying potential transmissions until the reception on the adjacent channel is completed. This last measure is only taken depending if a potential receiver node is within a defined distance range or not. In order to protect safety messages exchanged on the control channel, [19] suggests the use of adjacent channels solely for vehicles temporarily stopped at sufficient distance from the road, such as in a gas station for refuelling. This way, it is possible to prevent a performance degradation in the CCH and at the same time, not completely waste the spectrum resources in the adjacent channels. To further reduce the effects of cross channel interference, disjoint contention window durations and arbitrary inter-frame spacing (AIFS) values [20] may be used by nearby channels to avoid collisions, as suggested in [11]. All in all, further efforts are required in the design of more efficient techniques to face ACI, since this is serious problem for the simultaneous multi-channel operation in scenarios where nodes are in close proximity.

ACI is also a concern for future 5G mobile networks, since dynamic spectrum access will likely be employed to exploit spectrum holes in existing cellular networks. Therefore, new waveforms with high spectral efficiency and low adjacent channel leakage ratio (ACLR) will be required in order to cause minimum impact in legacy systems, such as current 4G networks. Several experimental studies [21] [22] are being conducted with the main goal of analysing the possible coexistence of 5G and current LTE systems. Candidate waveforms such as Generalized Frequency Division Multiplexing (GFDM) that present lower ACLR and peak-to-average power ratio (PAPR) than traditional OFDM systems, are being tested and evaluated under these scenarios.

A.3 Effects of ACI in the Received Signal

This work addresses the problem of cross channel interference on the receiver nodes of a vehicular network, through the design of a digital two-stage FIR filter. The role of this filter is to attenuate the interfering signal on the adjacent channels as much as possible, while preserving the signal received in the desired frequency. As a first step in this design process, a experimental setup was devised to capture the raw samples at the receiver platform, when both the interferer node and the intended transmitter were sending messages. This way, an analysis can be performed on the characteristics of the received signal when ACI is present and thus, the filter design process can be optimized to strongly reject the spectral components of the unwanted signal.

A.3.1 Experimental Setup

The setup used to fully characterize the ACI effect in the received digital baseband signal, took advantage of a research platform compliant with the IEEE 802.11p protocol [23]. The architecture of this flexible vehicular communications station, named IT2S platform, is presented in Figure A.2. There are two main components: a Single Board Computer where the higher layers of the protocol stack are implemented; and the IT2S Board, responsible for the MAC and physical layer's functionalities of IEEE 802.11p standard. In this experiment, the focus was on the analog to digital interface of the IT2S board, where the raw digital

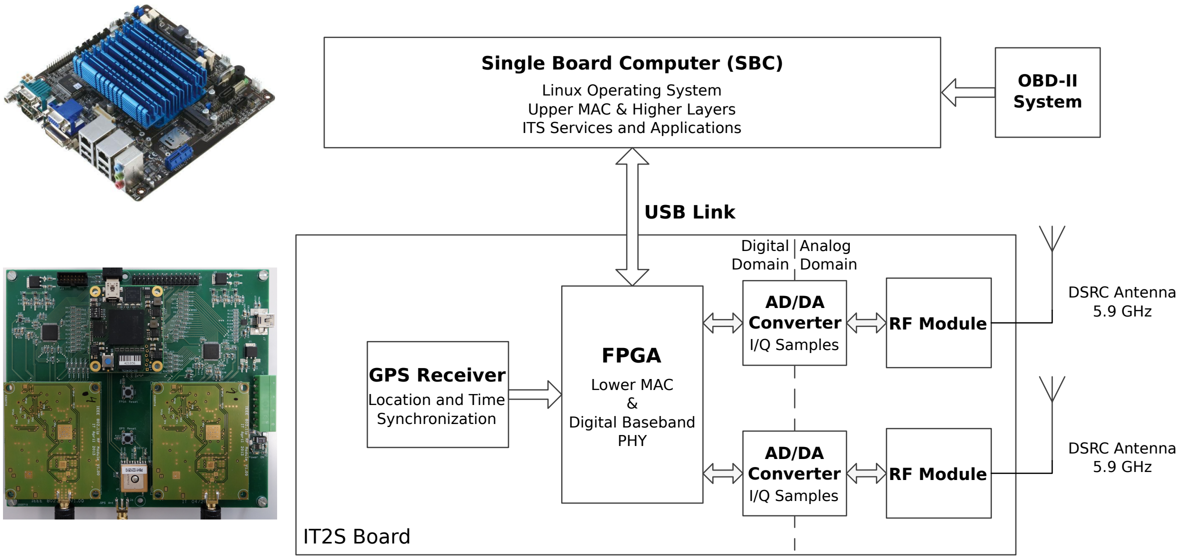


Figure A.2: IT2S platform architecture.

in-phase/quadrature (I/Q) samples were captured for analysis. The RF module down-converts the wireless signal to baseband, where it occupies half of the RF bandwidth, i.e. 5 MHz instead of 10 MHz, and then the AD/DA Converter, working at a sampling frequency of 40 MHz, digitizes the signal before sending it to the FPGA.

The experiment was conducted in the scenario depicted in Figure A.3. Two IT2S platforms were employed, and since these are dual-radio devices as required by the ETSI ITS-G5 standards [4], a total of four radio units were available. Hence, one of the platforms was used as a transmitter and as an interferer simultaneously, with one radio tuned in the American control channel (CCH #178) and the other interfering in a adjacent service channel (SCH #180). The remaining IT2S platform was working as a receiver node with the radio where the digital I/Q samples were captured, operating in the CCH #178. All measurements were taken in a well controlled environment, with all platforms directly connected through coaxial cables. A power combiner was used to couple the transmitted signal with the interfering one into the receiving radio. This way, the attenuation between the transmitter and the receiver was always constant and equal to the attenuation between the interferer and the receiver. The packet transmission in both radios was internally synchronized by the FPGA, forcing interference to actually happen. In the receiver node, the digital baseband samples coming from the AD/DA Converter were first stored and then retrieved from the FPGA directly to a computer, in order to be processed by a MATLAB® script. The automatic gain control (AGC) mechanism was disabled in the receiving platform and a fixed gain value was used instead, in order to ensure that measurements were always taken under the same conditions.

A.3.2 Baseband ACI Effect

Firstly, only the radio tuned in the control channel #178 was transmitting, which allows the analysis of the received signal without interference. This way and after processing the digital raw I/Q samples recorded at the FPGA input, one can obtain a power spectral density (PSD) estimate of the signal captured at the receiver node. Figure A.4 shows the baseband frequency

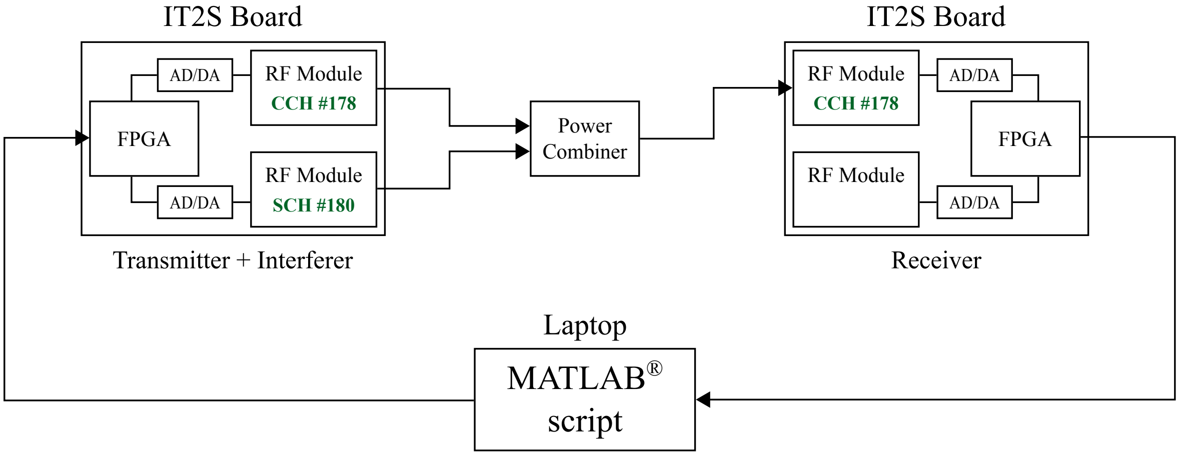


Figure A.3: Experimental setup used to analyse the effects of ACI in the received signal.

domain representation of the signal transmitted on channel #178 with approximately 7.5 dBm of power. The graphics depicts the PSD estimate from 0 to 40 MHz - the ADC's sampling frequency. As it can be observed, the bandwidth of the signal is in fact 5 MHz, half of the 10 MHz occupied in the 5.9 GHz frequency band.

By keeping the same radio sending messages and adding the other one transmitting on SCH #180, one can observe the effect of ACI in the receiver node. This result is presented in Figure A.5, where it is visible the presence of the interfering baseband signal in a channel adjacent to the transmitter. The transmit power was the same in both channels and it was equal to the one used in the experiment of Figure A.4, i.e. ≈ 7.5 dBm. It is clearly evident the difference in the spectral components from the case where there was no interferer. In baseband and from the perspective of the receiver tuned in channel #178, the interferer occupies a bandwith of approximately 10 MHz, from 5 to 15 MHz. For these transmit power levels, the peak of the unwanted signal in the frequency domain is approximately 15 dB below the signal received on the desired channel.

For the worst case scenario, i.e. when the transmitter is sending messages with the lowest power level available and the interferer is transmitting at full power, the PSD shown in Figure A.6 is obtained. In this situation, the peak of the interfering signal has almost the same value of the signal in the band of interest, being only 2 or 3 dB below. In conclusion, if no filtering operation is applied to the digital I/Q samples, the decoding process of the messages received in the scenarios presented in Figures A.5 and A.6, will be seriously compromised. This problem derives from the fact that the unwanted signals in the nearby channels are not

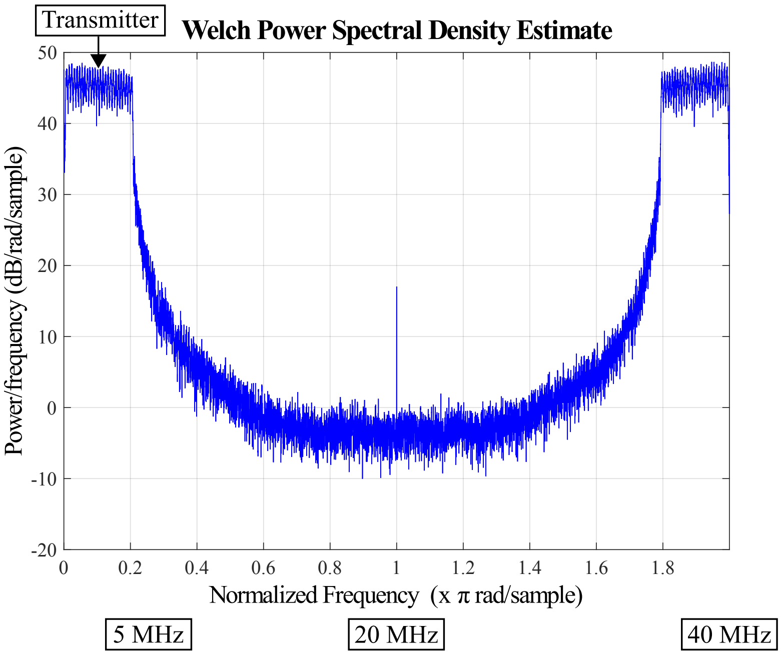


Figure A.4: Estimated power spectral density of the signal sent by the transmitter (tuned on CCH #178 and with a transmit power level of ≈ 7.5 dBm) at a sampling frequency of 40 MHz.

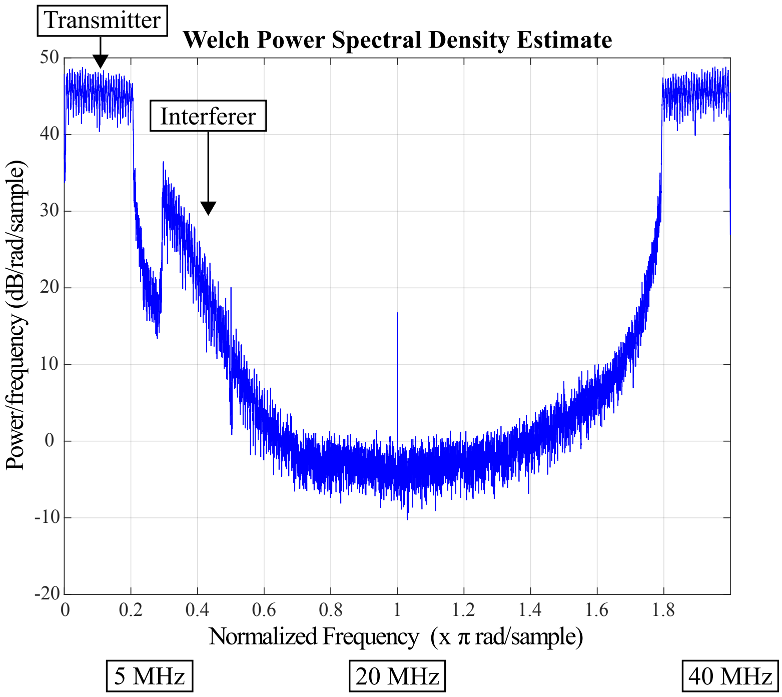


Figure A.5: Estimated power spectral density of the signals sent by the transmitter (CCH #178, ≈ 7.5 dBm) and the interferer (SCH #180, ≈ 7.5 dBm) at a sampling frequency of 40 MHz.

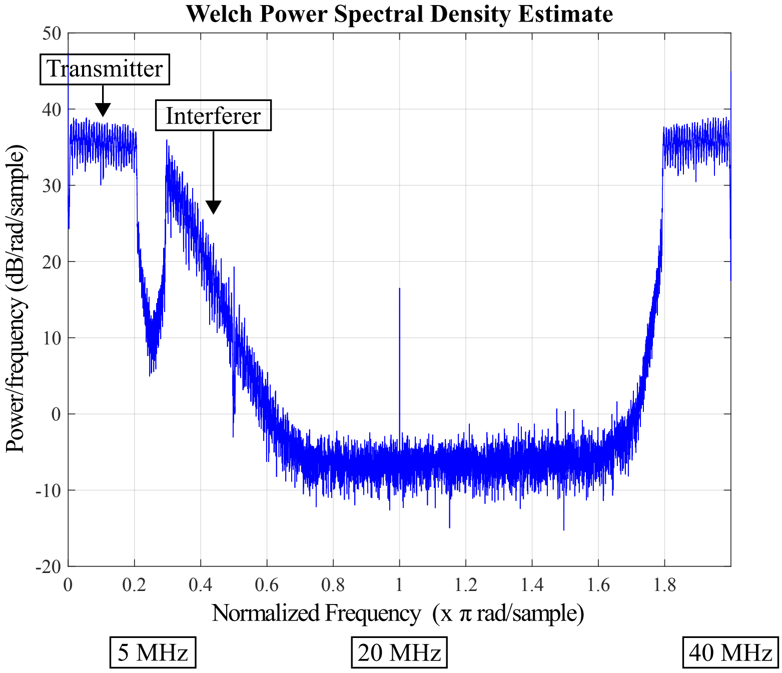


Figure A.6: Estimated power spectral density of the signals sent by the transmitter (CCH #178, ≈ -3 dBm) and the interferer (SCH #180, ≈ 27 dBm) at a sampling frequency of 40 MHz.

completely eliminated by the RF modules in the analog domain. In the IT2S platform, the RF module applies a low-pass filter with a cut-off frequency of 7,5 MHz, after down-converting the signal. Notice that in baseband the desired channel has a bandwidth of approximately 5 MHz and the immediate adjacent channel goes from $\approx$ 5 MHz to $\approx$ 15 MHz, thus the referred value of cut-off frequency is clearly insufficient. Under these circumstances, a more stringent filtering operation should be performed in the digital domain, using a lower cut-off frequency and a shorter transition band.

A.4 Digital Interpolated FIR Filter

Based on the previous results, it can be concluded that an interfering signal in an adjacent channel could severely affect the proper reception of messages sent by a transmitter node tuned in the channel of interest. The level of the signal generated by the interferer that appears at the FPGA input could be approximately equal (Figure A.6) or even greater than the desired signal (a situation that would occur if an attenuator was added between the transmitter and the power combiner in the setup above, making the path loss of the interferer lower than the one of the transmitter). This interference has to be filtered in order to increase the probability of correctly decode the received messages and to avoid the false blocking transmission effect described in section A.2. In this paper, the design and evaluation of a two-stage FIR low-pass filter is presented, with the main goal of reducing the interference due to the adjacent channels. The first stage is constituted by an interpolated FIR filter, which is more efficient than a simple FIR filter, since it can achieve steeper slopes with the same filter order. However, it needs another low-pass filter to eliminate the undesired passbands resulting from interpolation. The design of this second low-pass filter is not so stringent, i.e. requires a lower filter order, and it could be implemented with a polyphase decomposed architecture, consuming few FPGA resources and taking advantage of the decimation factor of 4 that could be applied to the I/Q samples. This decimation can take place since there was an oversampling factor of 4 in the AD/DA Converter. In other words, the signal with a bandwidth of 5 MHz was sampled at 40 MHz, four times more than the required by the Nyquist theorem.

The block diagram, both in time and frequency domains, of the two-stage low-pass filter is presented in Figure A.7. The signal x(n) or X(z) represents the digital raw I/Q samples at the FPGA input. Then, h(n) or H(z) correspond to the first stage of the filtering process - the interpolated FIR (IFIR) filter, responsible for implementing the narrow transition band immediately after the spectrum components of the signal in the desired channel. The second stage is constituted by the polyphase decomposed filter i(n) or I(z), taking advantage of the decimation factor of 4, whose goal is to eliminate the frequency replicas not attenuated by the interpolated FIR filter. Finally, y(n) or Y(z) represents the filtered signal that will feed the digital receiver chain at a sampling rate of 10 Msps. The detailed block diagram of this two-stage low-pass filter is depicted in Figure A.8. This scheme could be easily implemented in digital hardware (FPGA) using simple processing blocks, like adders, multipliers and registers for the time delays.

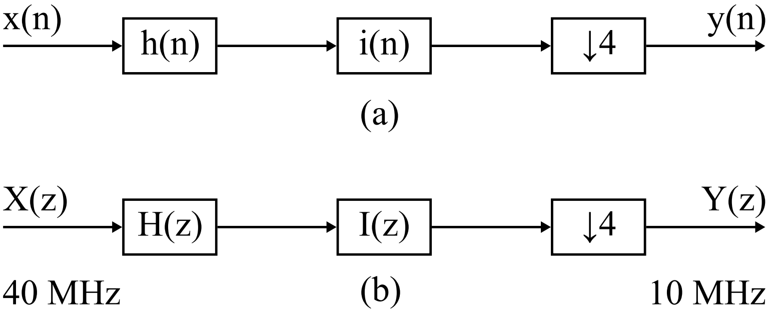


Figure A.7: Block diagram of the two-stage low-pass filter, both in (a) time and (b) frequency domains.

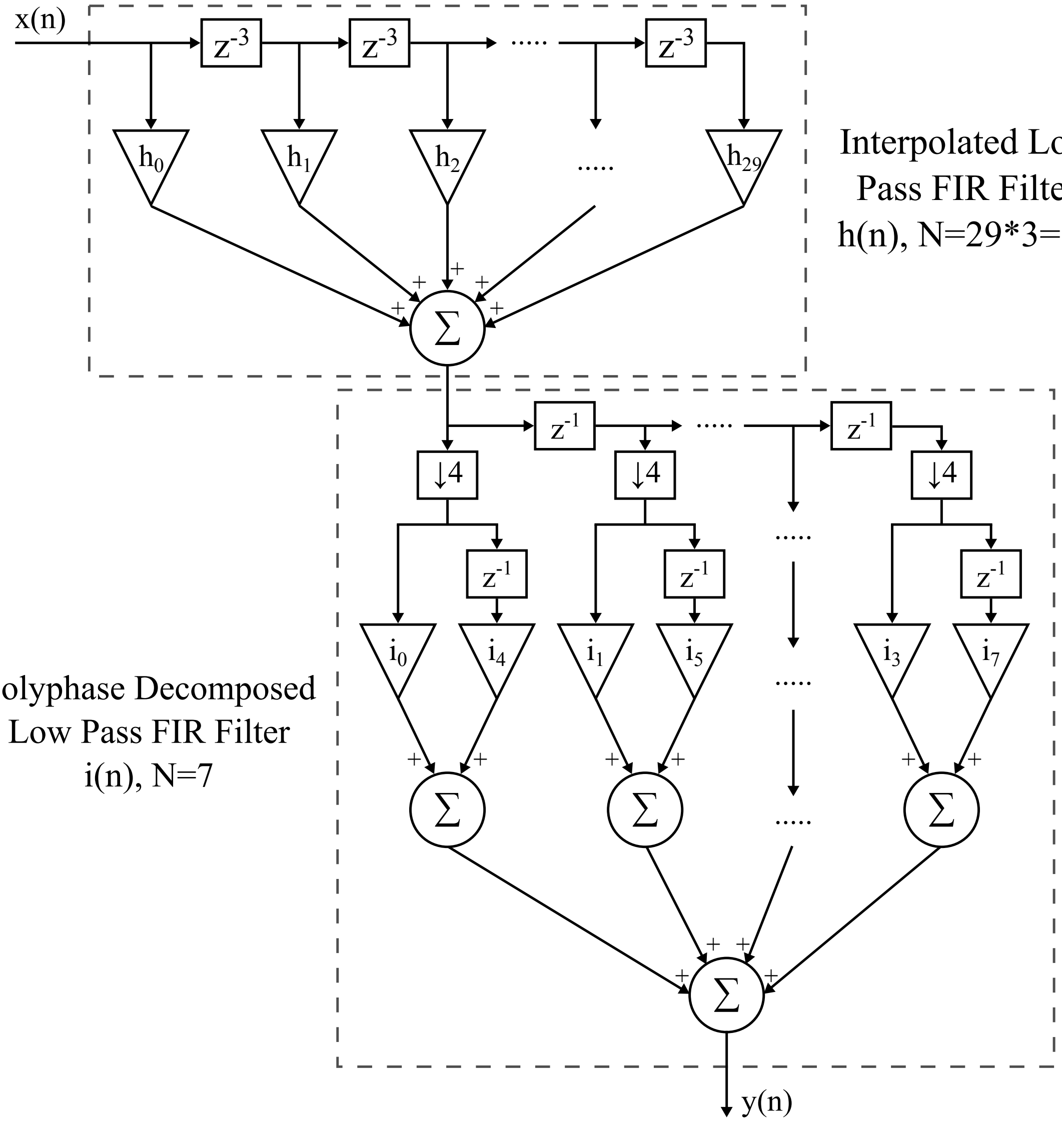

x(n)
z⁻³
z⁻³
.....
z⁻³
h₀
h₁
h₂
.....
h₂₉
Σ
Interpolated Low Pass FIR Filter h(n), N=29*3=87
z⁻¹
.....
z⁻¹
↓4
↓4
↓4
z⁻¹
z⁻¹
z⁻¹
i₀
i₄
i₁
i₅
i₃
i₇
Σ
Σ
Σ
Σ
Polyphase Decomposed Low Pass FIR Filter i(n), N=7
y(n)

Figure A.8: Detailed block diagram of both the interpolated low-pass FIR filter (top) and the polyphase decomposed low-pass FIR filter (bottom).

The coefficients for the design of both filters were obtained in MATLAB® with the aid of Filter Design and Analysis Tool (fdatool). For the IFIR filter, these coefficients were first computed for an equiripple FIR filter without interpolation. However, since an interpolation factor of 3 was then applied, the specified transition band was three times larger than the desired filter. After that, the design of the final IFIR filter can be concluded, by adding two null coefficients between each two consecutive coefficients previously obtained in fdatool. These zero value coefficients are naturally omitted in the top part of Figure A.8 but are implicit in the delays of 3 units (z^{-3}). The complete specifications used in the fdatool for this filter with minimum order are presented in Table A.1. A passband frequency of 4.14 MHz was specified instead of 5 MHz, since the standard imposes a small band guard value of ≈ 800 kHz in each side of vehicular channels, so the actual RF bandwidth is not exactly 10 MHz but approximately 10-(2*0.8) MHz. For the given input parameters, a minimum filter order of N=29 was obtained. The frequency response of the IFIR filter is presented in Figure A.9. The additional passbands resulting from the interpolation process are easily noticed, occupying a baseband spectrum between ≈ 0.45 and 0.9 π rad/sample in normalized units, which corresponds to the frequency range between ≈ 9 and 18 MHz.

Following the design phase, the IFIR filter was applied to the original signal from Figure A.6, using MATLAB® code that simulates an efficient implementation in hardware, where the multipliers corresponding to the null coefficients were eliminated, just like in Figure A.8. The PSD of the signal obtained at the output of the IFIR filter is shown in Figure A.10. One can observe the strong attenuation of nearly 40 dB in the peak of the original interfering signal (the grey one). However, there are replicated passbands that have to be eliminated by the second low-pass filter I(z). This filter was also created in fdatool with the parameters displayed in Table A.2. In this case, a filter order of N=7 was specified and a stopband frequency of 8.42 MHz was required in order to remove the replicas starting at ≈ 9 MHz. The frequency response of this second filter is presented in Figure A.11. As it can be seen, the transition

Response Type	Lowpass
Filter Order (Minimum Order)	29
Design Method	FIR Equiripple
Sampling Frequency (Fs)	40 MHz
Absolute Passband Frequency (Fpass)	3*4.14 MHz = 12.42 MHz
Normalized Passband Frequency (wpass)	3*0.207π rad = 0.621π rad
Absolute Stopband Frequency (Fstop)	3*4.88 MHz = 14.64 MHz
Normalized Stopband Frequency (wstop)	3*0.244π rad = 0.732π rad
Passband Attenuation (Apass)	0.5 dB
Stopband Attenuation (Astop)	40 dB

Table A.1: Interpolated FIR filter parameters in fdatool.

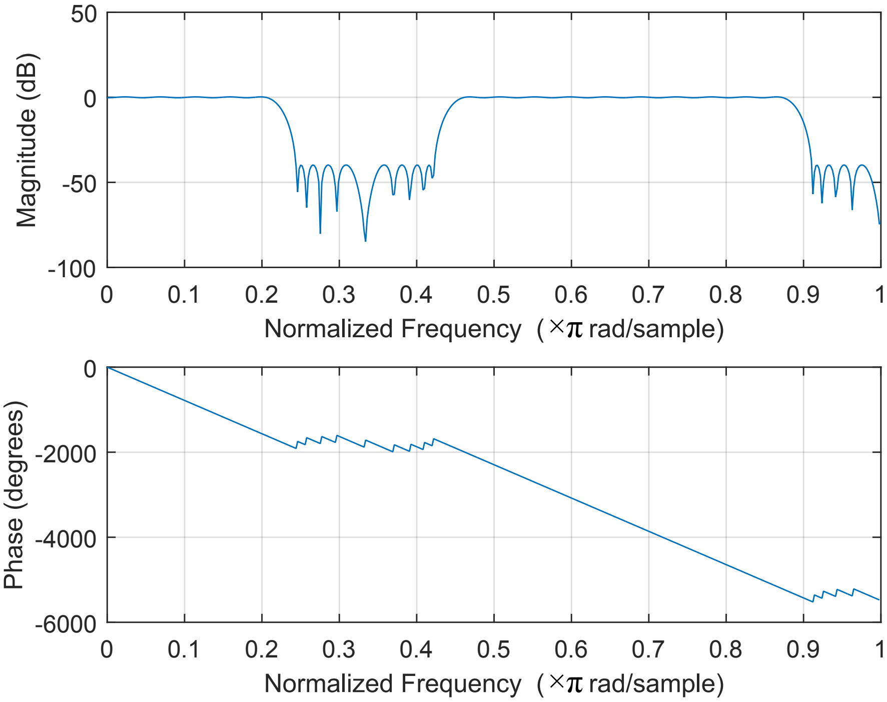


Figure A.9: Frequency response of the H(z) low-pass IFIR filter.

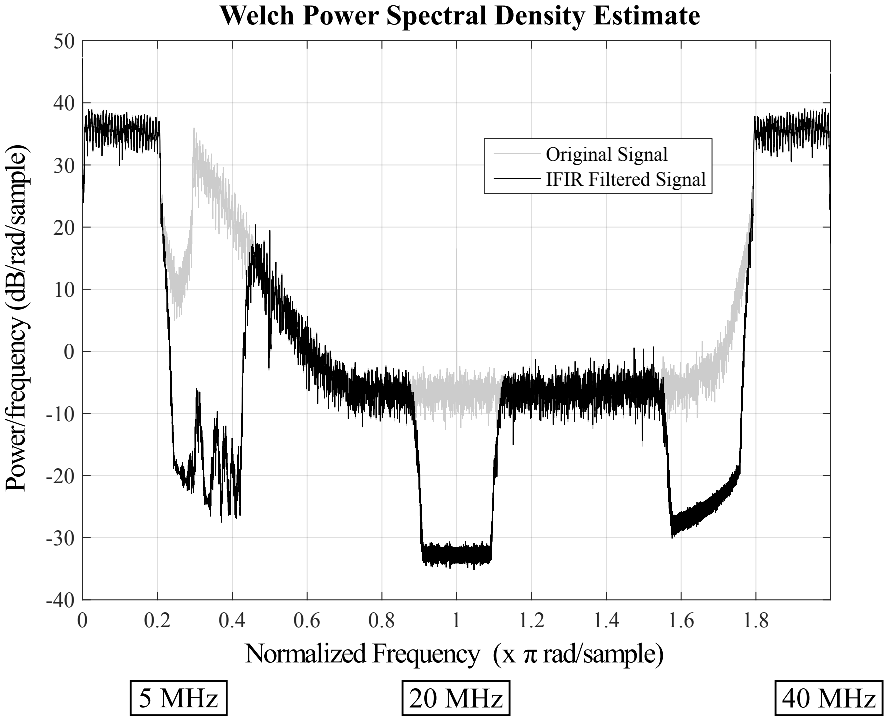


Figure A.10: Estimated power spectral density comparison between the original signal from figure A.6 (in grey) and the signal obtained after the H(z) filter (in black) at a sampling frequency of 40 MHz.

Response Type	Lowpass
Filter Order (Specify Order)	7
Design Method	FIR Equiripple
Sampling Frequency (Fs)	40 MHz
Absolute Passband Frequency (Fpass)	4.14 MHz
Normalized Passband Frequency (wpass)	0.207π rad
Absolute Stopband Frequency (Fstop)	8.42 MHz
Normalized Stopband Frequency (wstop)	0.421π rad
Passband Weight Value (Wpass)	10
Stopband Weight Value (Wstop)	1

Table A.2: Polyphase decomposed FIR filter parameters in fdatool.

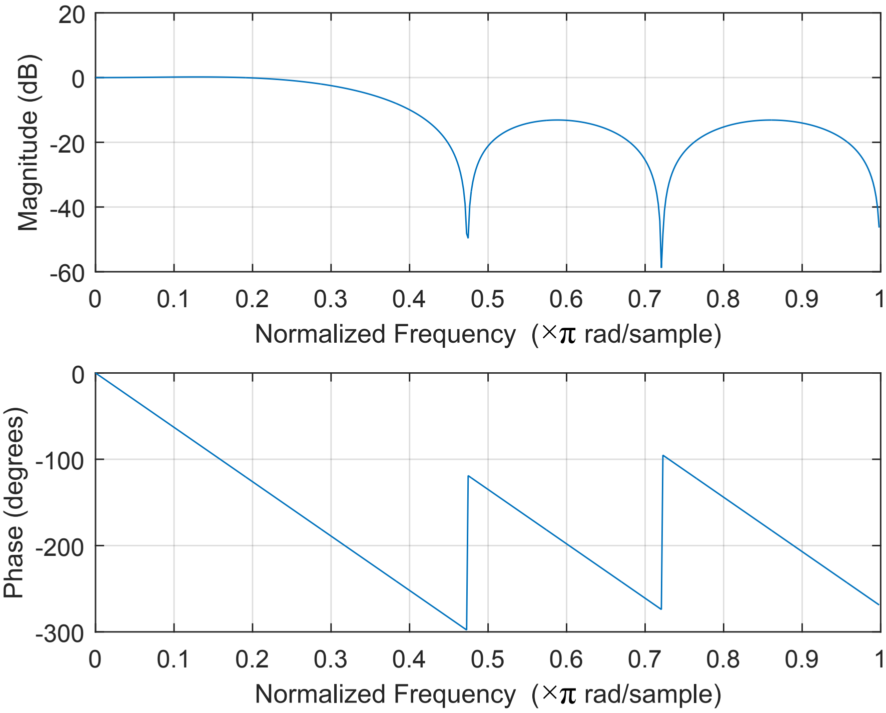


Figure A.11: Frequency response of the I(z) low-pass FIR filter.

band is more relaxed and the attenuation in the stopband is lower than the case of the IFIR filter, because a lower filter order was utilized and the frequency requirements were not so stringent. Nevertheless, these filter characteristics are sufficient to mitigate the impact of the replicated passbands in the filtered signal, represented by the black PSD in Figure A.12. The result presented in this Figure is obtained before the decimation block in Figure A.6, which means that in this case the polyphase decomposition property was not applied yet. The PSD of the output signal shows that the peak value of the interferer (≈ -5 dB/rad/sample at ≈ 0.5

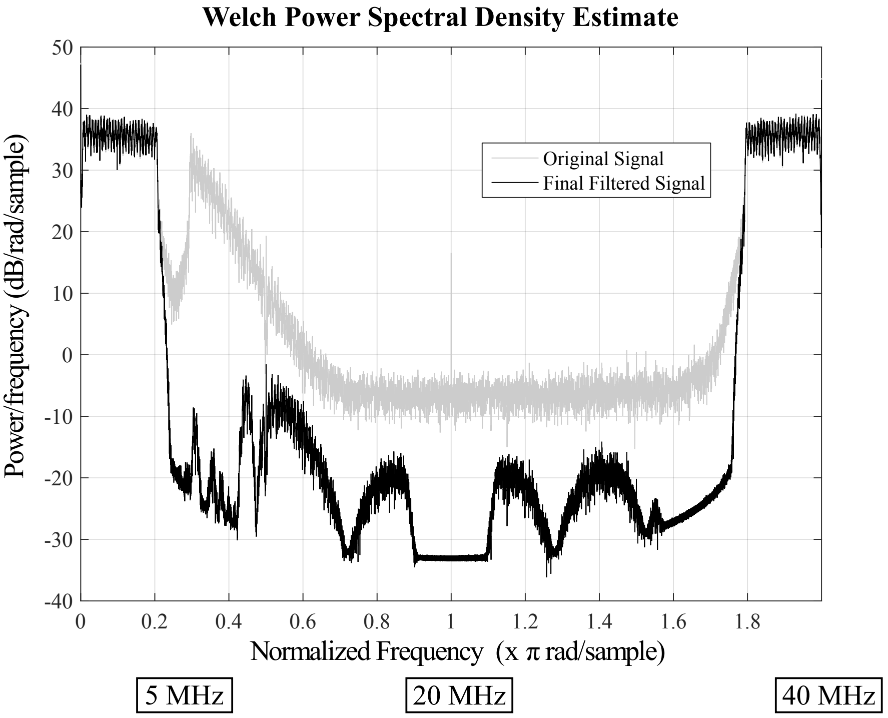


Figure A.12: Estimated power spectral density comparison between the original signal from figure A.6 (in grey) and the signal obtained after the I(z) filter (in black) at a sampling frequency of 40 MHz.

π rad) was attenuated by 40 dB when compared to the original signal ($\approx$ 35 dB/rad/sample at $\approx$ 0.3 π rad). This constitutes a strong reduction in the amount of interference present in the received signal and increases the probability of successfully decoding the packets by the receiver node.

By taking advantage of the decimation factor of 4 (Figure A.7), the implementation of the I(z) filter can be made more efficient, being the filtering operation performed at a lower data rate (10 Msps instead of 40 Msps). In this way, a polyphase decomposition with 4 phases can be employed, as depicted in Figure A.13. Thus, the polyphase decomposed I(z) filter takes the shape of the block diagram presented in the bottom part of Figure A.8.

Finally, a comparison can be performed between the original situation, where the captured

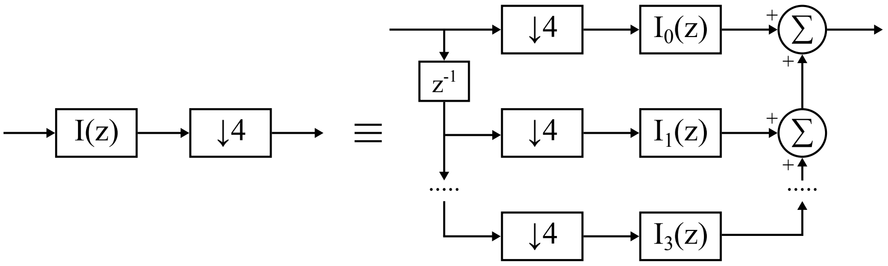


Figure A.13: Polyphase decomposed filter with a decimation factor of 4.

data was solely decimated before being processed by the digital receiver chain, and the case where the two-stage low-pass filter proposed in this paper was employed. The spectrum analysis of both resulting signals is shown in Figure A.14. The PSDs presented here correspond to the samples that would be supplied as an input to the receiver chain operating at a sampling rate of 10 Msps, thus already include the effect of the decimation by a factor of 4. As it can be observed, the transition band of the filtered signal is much sharper and an attenuation of almost 30 dB has been achieved at half of the sampling frequency.

In terms of the delay introduced in the receiver chain, its value is given by adding the delay imposed by both filters. Regarding the IFIR filter, the order of the filter built in the fdatool has to be multiplied by 3, to take into account the effect of interpolation and the zero-value coefficients added at the end. Consequently, the IFIR filter order is equal to N=29*3=87 and therefore, the group delay is equivalent to ((87+1)/2) = 44 clock cycles at 40 MHz, which corresponds to an absolute delay of 1.1 μs. In what concerns to the polyphase decomposed FIR filter, giving that its order is N=7, a group delay of (7+1)/2=4 clock cycles at 40 MHz is introduced, corresponding to an absolute delay of 0.1 μs. As a result, a total delay of 1.2 μs is added to the receiver chain by the cascade of the two low-pass filters. This value is perfectly acceptable for the system's operation, given the 12.8 μs available to perform frame detection and automatic gain control [2].

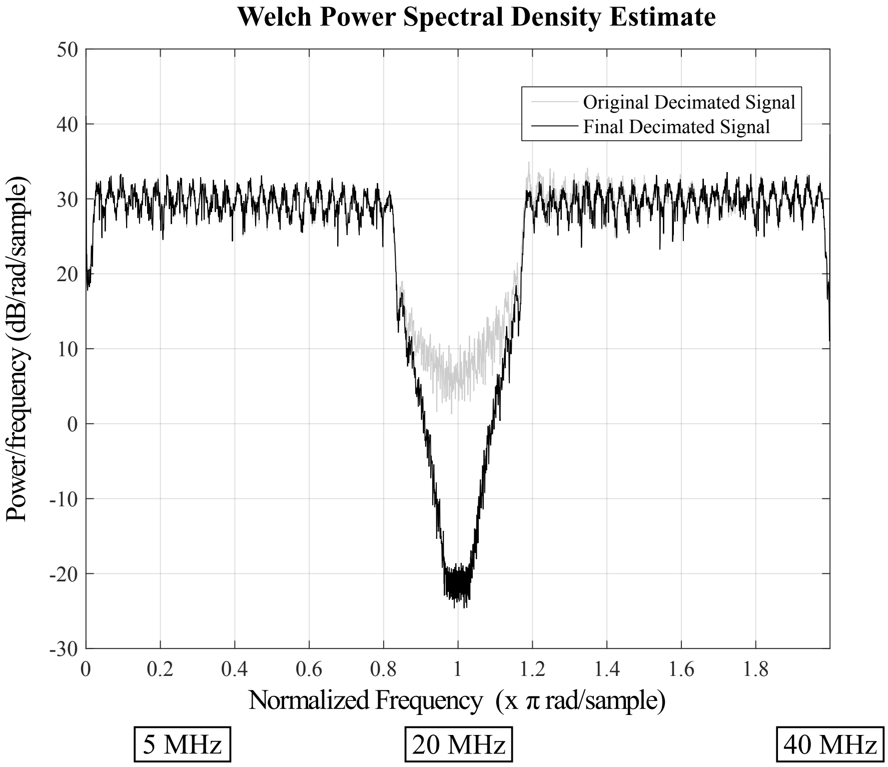


Figure A.14: Estimated power spectral density comparison between the original signal solely decimated (in grey) and the final signal obtained after the designed two-stage low-pass filter (in black) at a sampling frequency of 10 MHz.

A.5 Conclusions and Future Work

In this paper, a two-stage low-pass FIR filter has been proposed with the main goal of mitigating the effects of adjacent channel interference in vehicular communication systems. First, an interpolated FIR filter with a narrow transition band was designed to strongly attenuate the spectral components of the interfering signal close to the desired channel. And then, a polyphase decomposed FIR filter was employed to eliminate the passband replicas of the IFIR filter. The design followed a multi-rate approach, taking advantage of the decimation block in the interface between the analog and the digital domains of the receiver chain.

The behaviour of this two-stage filter was simulated and tested in MATLAB® and the results have shown that the proposed solution significantly reduces the impact of the adjacent channel transmissions in the signal of interest. Furthermore, the cascade of the two filters can be efficiently implemented in an FPGA, consuming simple digital hardware blocks. In addition, only a small delay is introduced in the decoding process of the receiving platform.

As future work, the designed filter will be implemented in an FPGA and integrated in the operation of the IT2S platform. This way, it will possible to evaluate the performance of the proposed solution in a real-world scenario. Metrics such as packet error rates, could be analysed under the presence of an interfering node, and the statistics could be compared with the present situation, where no filtering operation is involved.

Acknowledgements

This work is funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia under the PhD scholarship ref. SFRH/BD/52591/2014 and the project PEst-OE/EEI/LA0008/2013, by the European Union's Seventh Framework Programme (FP7) under grant agreement n. 3176711 and by BRISA, under research contract with Instituto de Telecomunicações - Aveiro.

References

[1] C. Campolo and A. Molinaro, "Multichannel communications in vehicular Ad Hoc networks: a survey", *IEEE Communications Magazine*, vol. 51, no. 5, pp. 158–169, 2013, issn: 0163-6804. doi: 10.1109/MCOM.2013.6515061.

[2] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, Mar. 2012.

[3] J. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, issn: 0018-9219. doi: 10.1109/JPROC.2011.2132790.

[4] Final draft ETSI ES 202 663 V1.1.0 (2009-11), *Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band*, Nov. 2011.

[5] ECC Report 101, *Compatibility studies in the band 5855- 5925 MHz between Intelligent Transport Systems (ITS) and other systems*, Bern, Feb. 2007.

[6] ETSI TR 102 654 (V1.1.1), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Co-location and Co-existence Considerations regarding Dedicated Short Range Communication (DSRC) transmission equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range and other potential sources of interference*, Jan. 2009.

[7] ETSI TS 102 792 (V1.2.1), *Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range*, Jun. 2015.

[8] ETSI EN 302 571 (V1.2.0), *Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive*, May 2013.

[9] ETSI TR 102 960 (V1.1.1), *Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (RTTT DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range; Evaluation of mitigation methods and techniques*, Nov. 2012.

[10] Kun-chan Lan and Chien-Ming Chou and Da-Jhong Jin, “The effect of 802.11a on DSRC for ETC communication”, in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, Apr. 2012, pp. 2483–2487. DOI: `10.1109/WCNC.2012.6214215`.

[11] C. Campolo, A. Molinaro, and A. Vinel, “Understanding adjacent channel interference in multi-channel VANETs”, in *Vehicular Networking Conference (VNC), 2014 IEEE*, Dec. 2014, pp. 101–104. DOI: `10.1109/VNC.2014.7013316`.

[12] T. Pham, I. McLoughlin, and S. Fahmy, “Shaping Spectral Leakage for IEEE 802.11p Vehicular Communications”, in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*, May 2014, pp. 1–5. DOI: `10.1109/VTCSpring.2014.7023089`.

[13] V. Rai, F. Jai, J. Kenney, and K. Laberteaux, *Cross-Channel Interference Test Results: A report from the VSC-A project*, Jul. 2007.

[14] R. Lasowski, F. Gschwandtner, C. Scheuermann, and M. Duchon, “A Multi Channel Synchronization Approach in Dual Radio Vehicular Ad-Hoc Networks”, in *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, May 2011, pp. 1–5. DOI: `10.1109/VETECS.2011.5956640`.

[15] C. Campolo, H. Cozzetti, A. Molinaro, and R. Scopigno, “Overhauling ns-2 PHY/MAC simulations for IEEE 802.11p/WAVE vehicular networks”, in *Communications (ICC), 2012 IEEE International Conference on*, Jun. 2012, pp. 7167–7171. DOI: `10.1109/ICC.2012.6364771`.

[16] W. Cho, G. Lee, and B. Park, “PER Measurement of Vehicular Communication Systems with Adjacent Channel Interferences”, English, in *Convergence and Hybrid Information Technology*, ser. Communications in Computer and Information Science, G. Lee, D. Howard, D. Ślęzak, and Y. Hong, Eds., vol. 310, Springer Berlin Heidelberg, 2012, pp. 46–52, ISBN: 978-3-642-32691-2. DOI: `10.1007/978-3-642-32692-9\_7`.

[17] N. Vivek, S. Srikanth, P. Saurabh, T. Vamsi, and K. Raju, “On field performance analysis of IEEE 802.11p and WAVE protocol stack for V2V amp; V2I communication”, in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, Feb. 2014, pp. 1–6. DOI: `10.1109/ICICES.2014.7033960`.

[18] Y. Bi, K.-H. Liu, L. Cai, X. Shen, and H. Zhao, “A multi-channel token ring protocol for QoS provisioning in inter-vehicle communications”, *Wireless Communications, IEEE Transactions on*, vol. 8, no. 11, pp. 5621–5631, Nov. 2009, ISSN: 1536-1276. DOI: `10.1109/TWC.2009.081651`.

[19] C. Campolo and A. Molinaro, “Improving multi-channel operations in VANETs by leveraging stopped vehicles”, in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, Sep. 2013, pp. 2229–2233. DOI: `10.1109/PIMRC.2013.6666514`.

[20] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, “Modeling Prioritized Broadcasting in Multichannel Vehicular Networks”, *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, Feb. 2012, ISSN: 0018-9545. DOI: `10.1109/TVT.2011.2181440`.

[21] M. Danneberg, R. Datta, and G. Fettweis, “Experimental Testbed for Dynamic Spectrum Access and Sensing of 5G GFDM Waveforms”, in *Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th*, Sep. 2014, pp. 1–5. DOI: `10.1109/VTCFall.2014.6965979`.

[22] F. Kaltenberger, R. Knopp, M. Danneberg, and A. Festag, “Experimental analysis and simulative validation of dynamic spectrum access for coexistence of 4G and future 5G systems”, in *Networks and Communications (EuCNC), 2015 European Conference on*, Jun. 2015, pp. 497–501. DOI: `10.1109/EuCNC.2015.7194125`.

[23] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Development of an ITS-G5 station, from the physical to the MAC layer”, in *Intelligent Transport Systems: from Good Practice to Standards*, P. Pagano, Ed., CRC Press, Taylor and Francis Group, 2016, ch. 1, pp. 1–37. DOI: `10.1201/9781315370866-2`.

Paper B

Fail Silence Mechanism for Dependable Vehicular Communications

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

in *International Journal of High Performance Computing and Networking*, vol. 10, no. 6, pp. 534-545, 2017

The format has been revised.

Fail Silence Mechanism for Dependable Vehicular Communications

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

Abstract

This paper presents a fault-tolerant architecture to improve the dependability of infrastructure-based vehicular networks. For that purpose, a fail silence enforcement mechanism for road-side units (RSUs) was designed, implemented and tested. Vehicular communications based on IEEE 802.11p are inherently non-deterministic. The presence of RSUs and a backhauling network, adds a degree of determinism that is useful to enforce real-time and dependability, both by providing global knowledge and supporting the operation of collision-free deterministic MAC protocols. One of such protocols is V-FTT, for which the proposed mechanism was designed as a case study. Notice, however that this mechanism is protocol independent and can be adapted to any wireless communications system. The proposed technique is capable of validating a frame for transmission by identifying faults both in value and time domains. Experimental results show that the fail silence enforcement mechanism has low latency and consumes few FPGA resources.

B.1 Introduction

Wireless vehicular networks, as a fundamental area of research in modern Intelligent Transportation Systems (ITS), aim to improve vehicle and road safety ([1]), passenger's comfort, efficiency of traffic management ([2]) and road monitoring. Vehicular communications rely on the recent IEEE 802.11-2012, IEEE 1609 and ETSI ITS-G5 family of standards, in which there are still some open problems concerning the timeliness and dependability of the exchanged messages ([3]). The medium access control (MAC) layer defined in IEEE 802.11 adopts a carrier sense multiple access with collision avoidance, in which collisions may occur indefinitely, due to the non-determinism of the back-off mechanism. Therefore, native IEEE 802.11 alone does not support real-time communications, however this property is crucial for safety applications, where warning messages have to be always delivered with a bounded delay.

The probability of collisions occurring may be reduced if the load of the network is kept low, which can be accomplished by using an adaptive and distributed message-rate control algorithm, as described in ([4]). Although this type of solution can reduce the probability of collisions, it does not provide strict real-time guarantees. Collision-free MAC protocols are considered deterministic as data collisions do not occur and a worst-case delay from packet generation to channel access can be calculated. This can only be achieved if the protocol restricts and controls the medium access to provide a deterministic behaviour.

In the design of a deterministic MAC protocol for vehicular communications, there are basically two main possible choices. The protocol could rely on the road side infrastructure ([5], [6], [7]) or it could be based on completely ad-hoc networks ([8], [9], [10], [11]). A hybrid approach that takes advantage of both models could also be implemented. For instance, a protocol could be devised in which vehicles are aggregatted in clusters by some ad-hoc based algorithm and then the communications with the infrastructure are established between the clusters' heads and the road-side units (RSUs). Strict real-time behaviour and safety guarantees are typically difficult to attain in ad-hoc networks, but they are even harder to achieve in high speed mobility scenarios, where the response time of distributed consensus algorithms, e.g. for cluster formation and leader election, may not be compatible with the dynamics of the system. Therefore, the presence of the infrastructure, i.e. RSUs and the backbone cabled network, adds a degree of determinism that is useful to enforce real-time and dependability at the wireless end of the network. This deterministic behaviour at the communications level translates into a higher certainty in some properties of the system, such as a fair and controlled access to the wireless medium by all network nodes and an ordered scheduling of transmission opportunities that enhances performance and ensures a collision free channel.

In addition to this, if the road-side infrastructure can be made more predictable than the other parts of the network, by executing certain tasks faster or in a more reliable way, the system could be seen as an instantiation of the *wormhole* metaphor ([12]). In general terms, a *wormhole* constitutes an alternative subsystem whose behaviour is trustworthy and well-defined no matter of how uncertain the system is. This *wormhole* subsystem is able to implement functionalities difficult to accomplish in the normal system, where most of computing and communications activities run. In a infrastructure-based vehicular network, the uncertainty would neither be uniform nor permanent across all system components, and the road-side units which are connected through the backhauling network, can be regarded as *wormholes*, since they can easily be made more reliable and predictable than the mobile nodes of the network (the on-board units - OBUs). Furthermore, RSUs may also play a key role in improving the security of network communications, by managing key distribution protocols ([13]) or through the validation of road events by using other sources of information, such as cameras.

Based on these arguments, a deterministic medium access control (MAC) protocol was proposed ([14], [15]), taking advantage of the road-side infrastructure. This protocol, entitled Vehicular Flexible Time-Triggered (V-FTT), adopts a multi-master multi-slave spatial time division multiple access (STDMA). The road-side units (masters) are responsible for registering the on-board units (slaves) with the infrastructure and for scheduling their transmission slots. These masters are synchronized through GPS receivers placed in each one of the nodes. They also share common knowledge of the road traffic system, which is attained by exchanging update messages holding the current state of each individual RSU's database. These messages are transmitted through the backhauling network (e.g. fiber optics), enabling RSUs with a global vision of the entire vehicular network.

The protocol is divided into periodic elementary cycles (ECs) with 100 ms duration and, as can be seen in figure B.1, each EC is further divided into three different parts. It starts with an Infrastructure Window, that is used by the road-side units to transmit trigger messages with the schedule of the registered on-board units (OBUs). The second part corresponds to the Synchronous OBU Window, where each OBU has a fixed size slot to send information to RSUs, either regular data (like vehicle's speed and heading) or a safety event. The Synchronous OBU

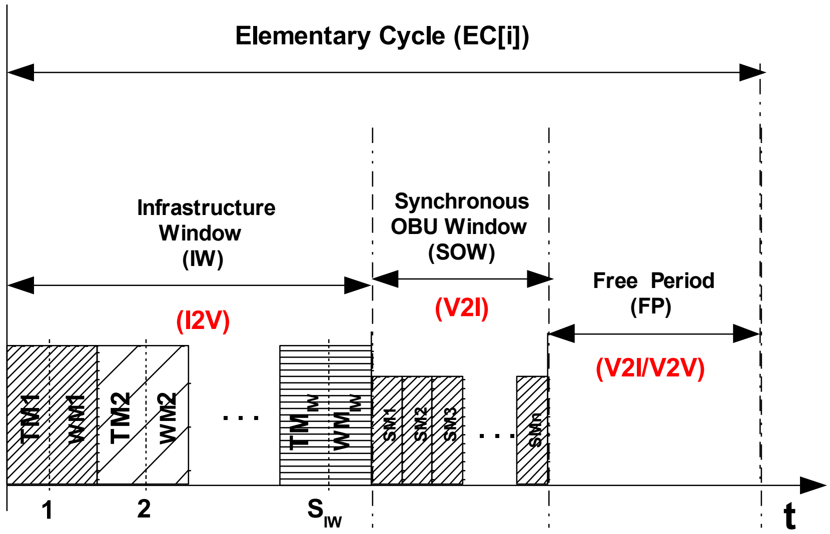


Figure B.1: Elementary Cycle of Vehicular Flexible Time-Triggered protocol ([14]).

Window duration is variable, depending on the number of OBUs scheduled in that particular Elementary Cycle. At the end of the EC, there is a free period, during which non-VFTT enabled OBUs can communicate, and the V-FTT nodes (both RSUs and OBUs) can exchange non-safety messages.

In the proposed protocol, RSUs play an extremely important role, since they are responsible for all traffic scheduling and admission control mechanisms. If an RSU stops working properly, all communications in its coverage area can be severely compromised. There are no guarantees any more regarding the timeliness and deterministic properties of the protocol. This leads to the development of fault-tolerance mechanisms that are able to improve the dependability of V-FTT and other deterministic protocols with the same characteristics. This paper presents some ideas concerning fault-tolerance techniques that could be applied to V-FTT protocol, and in particular, an architecture that was developed to enforce fail silent behaviour in road-side units.

The rest of the paper is organized as follows. Section B.2 describes the basic design decisions to provide fault-tolerance in V-FTT. Section B.3 presents a brief description of the platform used for development and the architecture of the fail-silent road-side unit, while section B.4 provides some results regarding the operation of the fail-silent system. Finally, section B.5 presents the concluding remarks.

B.2 Achieving fault-tolerance in V-FTT

In master-slave networks, as V-FTT, the most obvious issue that must be dealt with, when addressing fault-tolerance and dependability, is the single point of failure formed by the master holding the traffic scheduler and vehicles registration database. In fact, if a master node (RSU) fails to transmit trigger messages with the EC-schedules, transmit them out of time or with erroneous contents, then all network activity could be seriously compromised or even disrupted.

This can be handled using replication, with one or more similar nodes acting as backup masters. In this way, as soon as a missing trigger message is detected, a backup master comes into the foreground and transmits it, maintaining the communication without any discontinuity of the traffic schedule. However, this is only possible if all master replicas are synchronized, with respect to value and time.

To ease the task of designing mechanisms that enforce masters replication, it is considered that nodes are fail-silent, i.e., nodes can only fail by not issuing any message to the network. This, however, must also be enforced by using adequate components as nodes can fail uncontrollably. These additional elements should guarantee that the messages sent to the medium by the RSUs are correct both in time and value domain.

After guaranteeing that all active RSUs exhibit fail-silence behaviour, an active replication scheme ([16]) can be used to ensure that even in the presence of a failure in the primary RSU, the trigger messages with the EC-schedules will still be delivered to the OBU nodes. In this active scheme, the backup RSUs receive and process the exact same sequence of messages in parallel with the active one, and produce the same trigger messages in each EC. However, the packet transmission operation in the backup RSUs is deliberately delayed by a small amount of time, in the order of few μs, relatively to the primary one. This is done with the objective of facilitating the recovery procedure in case of RSU failure, by making it completely automatic and transparent to the slave nodes. This way, if the active RSU is able to transmit the trigger message in the planned instant, the replica will sense the wireless medium as occupied and will conclude that the primary system is free of error. Hence, it will not issue any message to the air, avoiding any overlap with the active node. On the other hand, if at that moment the medium is perceived as free, the replica will continue the transmission of its message and will replace the operation of the previously active RSU. As a result, the trigger messages will still be transmitted on time, since only a small delay is introduced at the beginning of the EC.

Alternatively, one may think on a different solution to signal the backup RSUs that a fail silent failure in a primary node has occurred. For instance, instead of relying in in-band wireless communications, it is possible to make use of a distinct channel to inform the backup replicas about the failure. Since vehicular communications platforms are dual-radio devices ([17]), i.e. with two radios that can be used simultaneously, even if one of the radios stops working properly and causes the failure in the primary RSU to occur, the other radio can be used to communicate the incident. Nevertheless, this constitutes a risky solution, since the problem could affect both radios at the same time and thus no message would be transmitted at all in this situation. Another possibility, is to use the backhauling network to communicate the failure event to the other nodes, yet this method takes more time to disseminate the information and therefore at least one entire EC would be completely wasted before the backup RSU starts to retransmit the trigger messages.

OBUs (slaves) should also exhibit fail-silence behaviour and although one could adopt the same mechanism used in master nodes, that would be expensive. The cost of that solution probably could not be supported by the vehicles' owners. Thus, slave nodes fail-silence enforcement both in time and value domain should only be adopted in special cases where the slave node information (value and timing) is absolutely essential, e.g., for police and emergency vehicles. For regular vehicles, a more inexpensive solution must be considered. Given the fact that slave nodes are not responsible for any type of network coordination, limiting OBUs ability to transmit uncontrollably will suffice. This corresponds to enforce fail-silence behaviour in the time domain only. From the OBU's perspective, a schedule is valid only within the scope of an elementary cycle, thus an entity policing the node only needs to be aware of the node schedule in a EC by EC basis. This entity can be regarded as a medium guardian that avoids node's transmissions outside the time slot assigned to it by the masters of the network - the RSUs. For that, this medium guardian just needs to decode every trigger message contents and block any unscheduled transmission from the node.

B.2.1 Fault Hypothesis

Figure B.2 presents the overall architecture of the network based on the road side infrastructure. The fault-tolerance mechanisms are also depicted, giving rise to the following fault hypothesis:

- **Node faults** - Master nodes (RSUs) are assumed to exhibit fail-silence failure semantics,

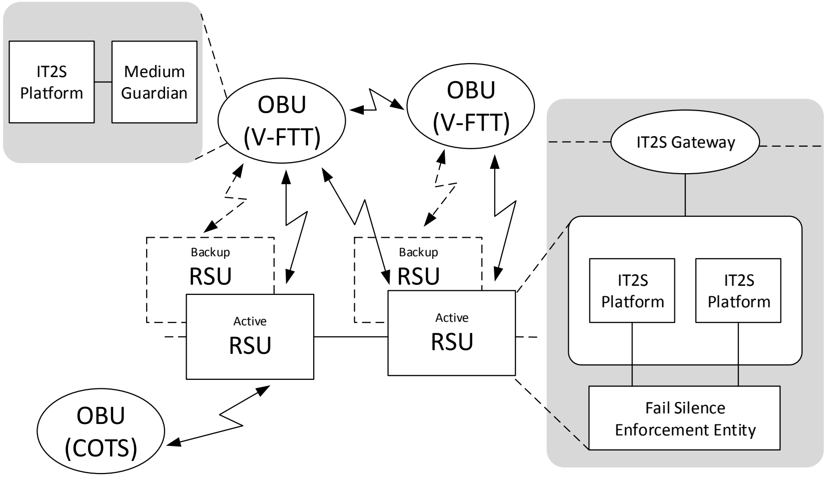


Figure B.2: Fault-tolerance mechanisms in V-FTT network.

which is guaranteed by their internal redundancy and a fail silence enforcement entity that validates the agreement both in value and time domains. This mechanism is the main focus of this paper and is explained in more detail in section B.3. Besides that, RSUs are also replicated (Backup RSUs), in order to undertake a failure in the active nodes (Active RSUs). In OBUs (slave nodes), medium guardians are used, to enforce fail silence only in time domain.

In this scheme, the fail silence enforcement entity (as well as the medium guardian when considering OBUs) belongs to a fault containment region that is assumed independent of the one constituted by the remaining components of the node. The covered faults within each node include hardware faults, both transient and permanent, and software faults. However, as it will be shown, faults in the analogue part of the physical layer are not considered. Byzantine faults, notably intrusions, are not totally covered, since such kind of faults need to be handled also at the IT2S Gateway level, a component that provides communication with other RSUs through the backhauling network.

- **Channel transient faults** - Vehicular communications are regularly affected by transient faults, since the wireless channel conditions may vary, depending on atmospheric and traffic conditions. This effect is much larger than the one observed in communication protocols for wired environments ([18]). A way to circumvent the higher packet error rate is by introducing time and spatial redundancy in the Trigger Message transmission by the RSUs, as depicted in figure B.1. This can be achieved by deploying a more dense RSU distribution along the road, leading to a partial overlap of the RSUs' radio coverage areas. This way, a single OBU transmission can be scheduled by a configurable number of adjacent RSUs, typically 3, for the same transmission slot. In this case, time and space diversity are employed together, since several RSUs placed in distinct locations transmit the same EC-schedule at different time instants. The required RSUs coordination for the execution of this redundancy mechanism is guaranteed through the backhauling network. It is thus assumed that every OBU receives at least one Trigger

Message every elementary cycle, i.e., channel transient faults do not impact the trigger message transmission. In this RSU redundant scheme, space diversity is also attained for the transmission of OBU messages, since several RSUs can receive the same packet. Moreover, critical nodes could be assigned with several time slots to re-transmit their messages.

- **Channel permanent faults** - The transmission medium is a single point of failure for vehicular networks. Permanent faults may occur in the wireless medium, e.g. due to unregulated interference, however, such faults are not considered in this paper. Depending on the severity of channel interference, medium redundancy could be included, by detecting the disturbance and commuting the operation of V-FTT protocol to another channel in the available frequency spectrum. As the band assigned for wireless vehicular communications is reserved by law, unregulated interference can be considered as malicious faults.
- **Synchrony assumptions** - Nodes synchronization, both masters and slaves, is ensured by a GPS receiver located at each one of the nodes. The accuracy provided by this system is typically below 333 μs (the maximum value used to determine if a device is synchronized to UTC or not ([19])) and it must be sufficient to cope with the synchronization requirements of V-FTT. However, if by some reason, the GPS signal is not available or is not sufficiently accurate at some instant in time, another strategy could be used. The alternative relies on the fact that the trigger message transmitted by the master node, besides conveying the scheduling information, can also act as a synchronization mark to all network nodes. This way, master nodes are also time masters, and it is assumed that in between two consecutive trigger messages (typically 100 ms), the clock counters of each node do not diverge more than a negligible amount of time.

B.2.2 Fail Silence Failure Mode

A faulty node of a distributed system that sends unsolicited messages at arbitrary points in time (babbling idiot failure mode ([20])) without respecting the media access rules can disable nodes with legitimate messages to access the network. However, this failure mode can only occur if a node fails in an uncontrolled way. Network topologies that support the operation of fail uncontrolled nodes are costly ([21]). Thus a node should only exhibit simple failure modes and ideally it should have just a single failure mode, the fail silent failure mode ([22]), i.e., it produces correct results or no results at all. In this matter, a node can be fail-silent in the time domain, i.e., transmissions occur at the right instants, only, or in the value domain, i.e., messages contain correct values, only. With fail silence behaviour, an error inside a node cannot affect other nodes and thus each node becomes a different fault confinement region ([22]). Furthermore, if k failures of a functional unit in a system must be tolerated, then $k + 1$ replicas of that unit are needed as long as they are fail silent. If the replicas are fail uncontrolled, then $3k + 1$ will be required. Thus, the use of fail silent nodes also reduces the complexity of designing fault-tolerant systems.

The alternatives to enforce fail silent behaviour may be generically divided in two main groups. The ones that result from adding redundancy to each node and ones that rely on behavioural error detection techniques ([22]). Using replicated processing within a node with output comparison or voting calls for the use of mechanisms to keep the replicas perfectly synchronized and to avoid replicas to diverge due, e.g. to asynchronous events. Synchronization at processor instruction level is the most obvious way to achieve replica synchronism, driving identical processors with the same clock source and evaluating their outputs (either comparing or voting) at critical instants, e.g. every bus access. Special care must be taken with asynchronous events that must be delivered to the processors so that all perceive the same event at the same point of their instruction streams.

Over the years many systems were designed based in double-processor fail silent nodes such as Sequoia ([23]) and Stratus ([24]). However, these systems have some drawbacks ([25]). First of all, the processors must exhibit the same deterministic behaviour every clock cycle and do not care states are not allowed so that they produce identical outputs. Secondly, the use of special purpose hardware as comparators or voters, reliable clock sources and asynchronous event handlers greatly increases the design complexity. Finally, due to their operation in lock step, a transient fault could affect both processors in the same way, making the node susceptible to common mode failures. An alternative approach to eliminate the hardware level complexity of the solutions referred above is to transfer the replica synchronism to a higher level using software protocols over a set of standard processors operating independently of each other in a node. Task synchronization approaches were used in SIFT ([26]) and Voltan ([27]).

Behavioural error detection mechanisms, either in software or in hardware, are another alternative for enforcing fail-silence behaviour. Mechanisms such as checksums, watchdog timers and processor monitoring, are usually implemented using commercial-off-the-shelf (COTS) components. Error detection latency is the major bottleneck of these systems since the error detection mechanisms are only able to detect errors a relatively long time after they occur, possibly forcing other nodes to put in place some sort of error recovery policy. Bus guardians, which are autonomous devices with respect to the node network controller and host processor, also implement behavioural error detection mechanisms. Usually used in wired networks to enforce fail silence, bus guardians act as failure mode converters, i.e., the failure modes of the component are, at the interface to other components, replaced by the failure modes of the guardian.

In order to be fail-independent with respect to the interface it monitors the bus guardian must belong to a separate fault confinement region. A guardian would be of no use if it failed whenever the node that it is guarding also failed. Some potential sources of common mode failures are: clocks, CPU/hardware, power supply, protocol implementation, operating system, etc. Designing a bus guardian with independent hardware, with no common components and design diversity can help to avoid common failure modes. Despite the possible design compromises made between independence, fault coverage and simplicity/cost in any bus guardian architecture it is mandatory for the guardian to have some a priori knowledge of the timing behaviour of the node it is policing. In time-triggered (TDMA) networks this implies that each bus guardian needs to have its own copy of the schedule and an independent knowledge of the time.

Almost all the work developed in the area of fail silent systems is for wired industrial, or automotive systems ([28], [29]). Although the principles are similar, nodes of wireless vehicular networks pose some additional problems implementing fail silent behaviour, arising both from the open nature of such networks, in contrast with closed wired networks found in industrial and automotive systems, and from the physical impossibility of having a radio receiving the transmission of another one located a few centimetres away. Furthermore, the use of centralized bus guardians as in star topologies is not possible. However, in wireless communications, one can think in medium guardians as devices that protect non-faulty wireless network nodes from erroneous ones.

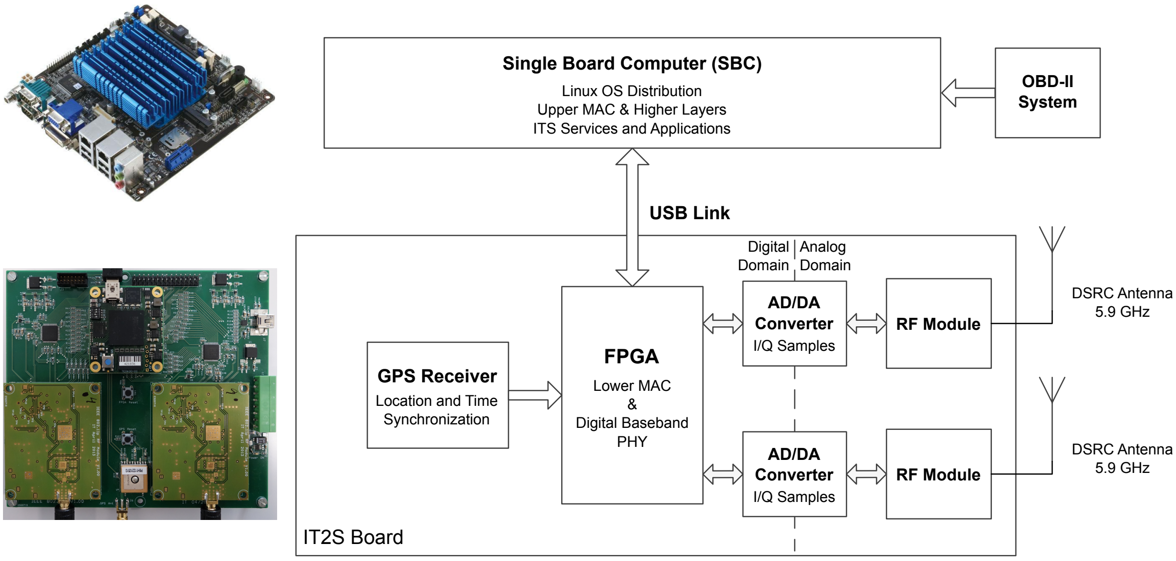
In master-slave networks, as V-FTT, fail silence in the master nodes must be enforced both in time and value domains. This is mandatory for the master nodes, to guarantee the correctness of the EC-schedules that are broadcast to the network. A medium guardian policing functionality cannot be used in RSU nodes because of the causal relations between the RSUs computed schedules and the medium guardian operation. Fail silence enforcement in V-FTT roadside units require a replicated processing/voting scheme. For the case of slave nodes (OBUs), fail silence could be enforced using either medium guardians or internal replication and temporized agreement.

To the best of authors' knowledge, there is no prior work of enforcing fail silence behaviour in wireless distributed embedded systems. Most of the works found in the literature focus on the implementation of fail silent nodes for safety-critical applications in fieldbus or wired technologies. Therefore, the fail silence mechanism proposed in this paper constitutes a novel contribution to the area of dependable vehicular communications. The research and development of wireless fail silent nodes was not undertaken before, probably because there are still few high criticality applications that rely on wireless communications. Nevertheless, with the proliferation of wireless systems and their expansion to safety environments, such as the vehicular scenario, the need for this type of dependable behaviour will certainly increase.

B.3 Enforcing fail-silence in V-FTT

B.3.1 IT2S platform: A brief description

The proposed system architecture takes advantage of a flexible implementation of an IEEE-802.11/ETSI-ITS-G5 controller, the IT2S platform. This platform (figure B.3) has been developed from scratch at Telecommunications Institute (Aveiro site) and it is essentially constituted by two main modules: the Single Board Computer and the IT2S board. The latter one implements the entire physical (PHY) layer of the protocol stack and some low-level functionalities of the MAC layer. It includes two RF front-ends and two AD/DA processors, providing access to two different wireless channels at the same time. This is a requirement specified in the standards ([17]), in order to ensure that nodes can simultaneously be used to



Single Board Computer (SBC)
Linux OS Distribution
Upper MAC & Higher Layers
ITS Services and Applications
OBD-II System
USB Link
Digital Domain
Analog Domain
GPS Receiver
Location and Time Synchronization
FPGA
Lower MAC & Digital Baseband PHY
AD/DA Converter I/Q Samples
RF Module
DSRC Antenna 5.9 GHz
AD/DA Converter I/Q Samples
RF Module
DSRC Antenna 5.9 GHz
IT2S Board

Figure B.3: Main blocks of the IT2S platform.

improve road safety (in one radio) and to provide infotainment services (in the other one). A FPGA implements the digital baseband PHY and part of the MAC layer (Lower MAC) and a GPS receiver is used for time synchronization and location purposes. The Single Board Computer is responsible for implementing the higher layers of the protocol stack, from the MAC to the Application layer. This platform could operate either as an RSU or as an OBU.

B.3.2 Fail-silent RSU design

In order to implement a fail-silent RSU, all the possible device failure modes must be converted in fail-silent failure mode, enforced by a simpler, thus less prone to failures, component. The complexity of this fail silence enforcement entity can be greatly reduced if it is implemented at the lower layers of the OSI stack, in which the number of possible defects of system's design decrease and are easily identified ([20], [30]). The design of the fail silence mechanism at the lower layers of the protocol stack is simplified given the white box access to a flexible vehicular research platform. Implementing a similar solution in a COTS platform would probably imply higher latency, caused by the API.

As briefly discussed in section B.2, the operation of the proposed fail silence mechanism consists in an internal redundancy scheme, based on the replication of the IT2S platform (right side of figure B.2). Two complete sets of single board computers and IT2S Boards are used to produce messages, whose purpose is to be disseminated through the air medium. The fail silence enforcement entity then compares the values and the timing of the messages produced by these two sets and, if everything is working correctly, it validates the frame and allows its transmission by one of the platforms. On the other hand, if the frames differ or are significantly out of phase, the entity silences the system until a restart signal is received.

Notwithstanding the decision to implement the fail silence mechanism at the lower layers of the protocol stack, there are still several design choices that should be taken when choosing the ideal place and method to perform the comparison of the samples produced by both platforms. As shown in figure B.4, there are three main possible checkpoints where this verification can be executed, if one considers MAC and PHY as the appropriate layers to implement this mechanism. The rationale to choose only these lower levels is, as already explained, based on the observation that moving it higher on the protocol stack, will increase the design complexity and will potentiate design defects ([30]). The three different checkpoints, numbered as 1, 2 and 3, correspond to the output interfaces of MAC, digital and analogue PHY layers, respectively.

Output comparison at checkpoint number 1 could be attained using a voting scheme between both MAC frames produced at the output of Lower MAC sublayer in the FPGA. The verification at this point, however, will not include possible faults in the operation of the digital physical layer, which basically comprises the baseband processing of the OFDM transmission chain. This could be attained if the fail silence mechanism is implemented at checkpoint 2, in the interface between the FPGA and the AD/DA processor, by comparing the In-phase/Quadrature samples that constitute the OFDM modulated frame. A verification at this stage already encompasses any discrepancy at higher levels of the IT2S platform, validating all the processing done at the SBC and at the FPGA. If, for instance, a software fault occurs at the higher layers, leading the SBCs to attempt transmitting different frames due, e.g., from distinct views of the network or from inconsistent scheduling computation, the outputs at this checkpoint will differ and that fault can be detected. Nevertheless, in an ideal scenario, checkpoint number 3 would be the best place to verify the correctness of the outputs produced by both transmission chains, since it would also include the operation of the

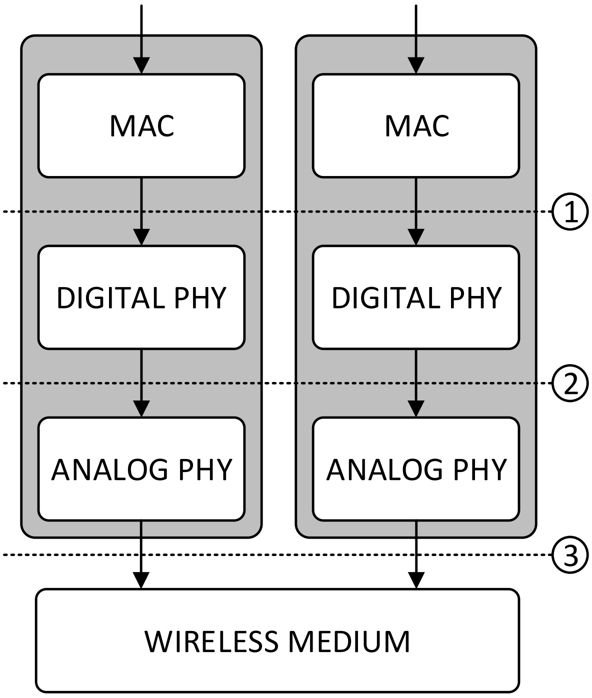


Figure B.4: Possible checkpoints for the fail silence mechanism.

analogue part of the IT2S platform. However, implementing an online verification algorithm of high frequency analogue signals is a very complicated task, since signal comparison would probably require a downconversion to a lower frequency, which will add an excessive delay and will demand for resources in the analogue part that may not be available. Furthermore, both transmission chains could produce correct signals although slightly different, due to minor mismatches on the digital to analogue conversion and on the radio frequency amplification processes.

From the previous analysis, one can conclude that checkpoint 2 is the most appropriate place to implement the fail silence mechanism. A basic implementation, presented in figure B.5, would be to perform a runtime comparison of the output produced by both digital PHYs and signal an error that would abort the ongoing transmission whenever a mismatch is detected. Due to the slight differences between the internal clocks of both platforms, which are synchronized through independent GPS receivers, the samples will not be produced at exactly the same instant. Therefore, in this scheme, the first platform to have the samples ready for transmission at the end of the digital PHY, will be the one that actually transmits them. This way, there will be no delay on the transmission of the messages, because the samples produced at the end of the digital PHY will be immediately forwarded to the analogue part, with no a prior validation. This method, however, would not prevent the medium from being occupied during at least part of an incorrect frame transmission, since a small tolerance must be allowed at the moment the results are produced. This time tolerance is needed to cope with slight variations between the internal clocks of both platforms that are synchronized through independent GPS receivers. As a consequence, the described solution would not

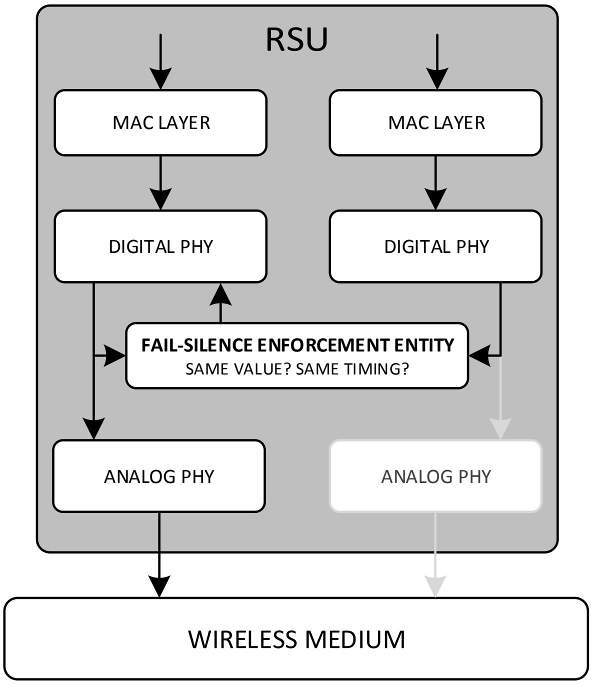


Figure B.5: Basic fail silent master RSU scheme.

result then in a true fail silent enforcement entity.

A possible improvement on the previous scheme is presented in figure B.6, where each of the samples produced by the digital PHY is only allowed to proceed to the analogue PHY after successful validation. In this case, each sample will be sent to the analogue part immediately after being compared with the corresponding one from the other platform. Thus, the first generated samples just need to wait a small interval before being transmitted, which corresponds to the time the other platform needs to have the samples available, due to the non perfect synchronization between the internal clocks of both platforms. This solution, although providing protection against frames that are completely different or out of time, still does not provide true fail silence behaviour, because a single error occurring at the middle of a message would invalidate the complete transmission. The medium could therefore be occupied with samples that although correct when analysed independently, were invalid in the context of a full frame. Beyond that, given the fact that in the proposed real-time protocol, the RSU coordinates all the communications in the wireless channel, if an RSU transmission is interrupted, a complete elementary cycle will be wasted.

A possible solution for this problem is to modify the transmission chain to produce the samples that are to be sent over the air in advance, relative to the moment when they are supposed to be sent. If enough advance is provided, the samples of an entire frame can be compared and validated before that frame transmission has even started. In this scheme, the validated samples are then fed back to the digital PHY that will, using a very simple mechanism, apply them at the correct moment to the analogue PHY for transmission. If any difference is observed at any part of the frame or if the measured delay between the instants

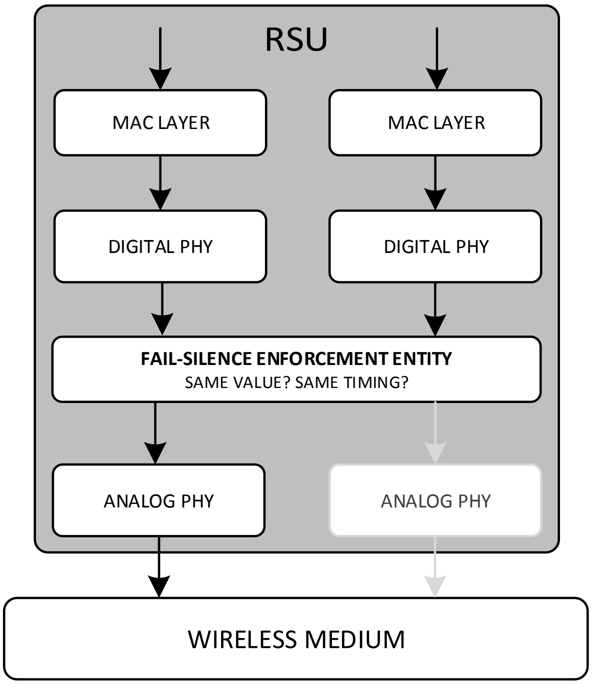


Figure B.6: Improved fail silent master RSU scheme.

when samples are provided is greater than a certain fixed tolerance, the fail silent entity will not allow any of two units to transmit. In this case, the medium will not be occupied inadequately, contrarily to the previous proposals.

Based on these arguments, figure B.7 presents the proposed scheme for the fail silent RSU and the final location of the fail silence enforcement entity inside the protocol stack. This entity was placed in the closest point possible to the antenna, at the end of the digital physical layer and before the analogue part. This way, it is possible to validate the operation of the entire system and protocol, except the analogue side of the physical layer. Ideally, and as already mentioned, the analogue path should also be included, however and as already mentioned, implementing a runtime verification algorithm of high frequency analogue signals is a very difficult task. Moreover, in order to guarantee that the fail silence enforcement entity belongs to a different fault containment region, with no common failure mode, it was developed in a external PCB with separated power supply and clock source.

In addition to this and as already referred, to truly implement a fail silent system, both transmission chains have to produce and send the frames to the fail silence enforcement entity in advance, so that the entire message could be verified before a single bit is transmitted through the antenna. More details regarding the internal architecture of the fail silence entity will be provided next.

B.3.3 Fail Silence Enforcement Entity

Figure B.8 depicts the interfaces and the internal structure of the fail silence enforcement entity, which was implemented in a Xilinx FPGA Spartan-6. It receives the data generated

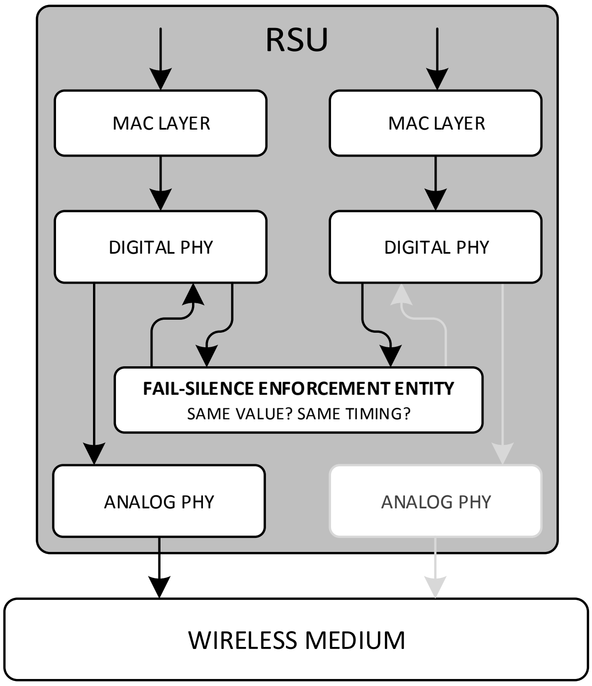


Figure B.7: Final fail silent master RSU scheme.

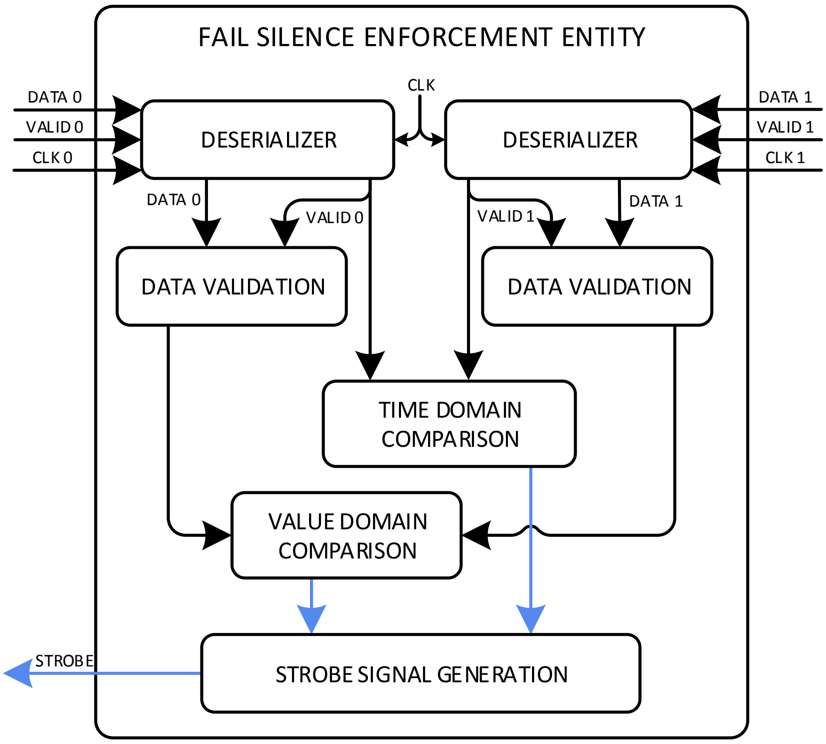


Figure B.8: Block diagram of the Fail Silence Enforcement Entity.

by the digital transmission chains of the two IT2S Boards (10 bits of In-phase + 10 bits of Quadrature samples @10Msps), which corresponds to signals DATA 0 and DATA 1. For each of these signals, there is a valid signal (VALID 0 or VALID 1) to indicate whether a frame is being transmitted or not in the data bus. After deserializing and removing the invalid bits, data from both sources of information are compared in the Value Domain Comparison module. Furthermore, the fail-silence entity also verifies if the two platforms are synchronized, i.e., producing information at the same time. It only allows a small time offset, to cope with the fact that the platforms may not be precisely aligned in time. However, this time tolerance should be small enough to guarantee the timely behaviour of the communications protocol (e.g., V-FTT). This operation is performed in the Time Domain Comparison module, based on the analysis of phase offset between the two valid signals.

For a given frame, if the results produced by these two comparison modules are both positive, a strobe signal is generated and sent to the primary platform (the one that will effectively send the message to the air). Otherwise, if at least one of the values is negative, no signal is generated and the entire RSU operation will stop until a restart signal is received in the fail silence enforcement entity.

The interaction of the IT2S Board with the fail silence enforcement entity is presented in figure B.9. It depicts the architecture of the digital PHY in transmission mode and its integration with the fail silent scheme. A frame coming from the LMAC sublayer is handled in the PHY Controller module, which forwards its content to the digital transmission chain (OFDM modulator). Then, the resulting I/Q data samples are sent to the Serializer, in order

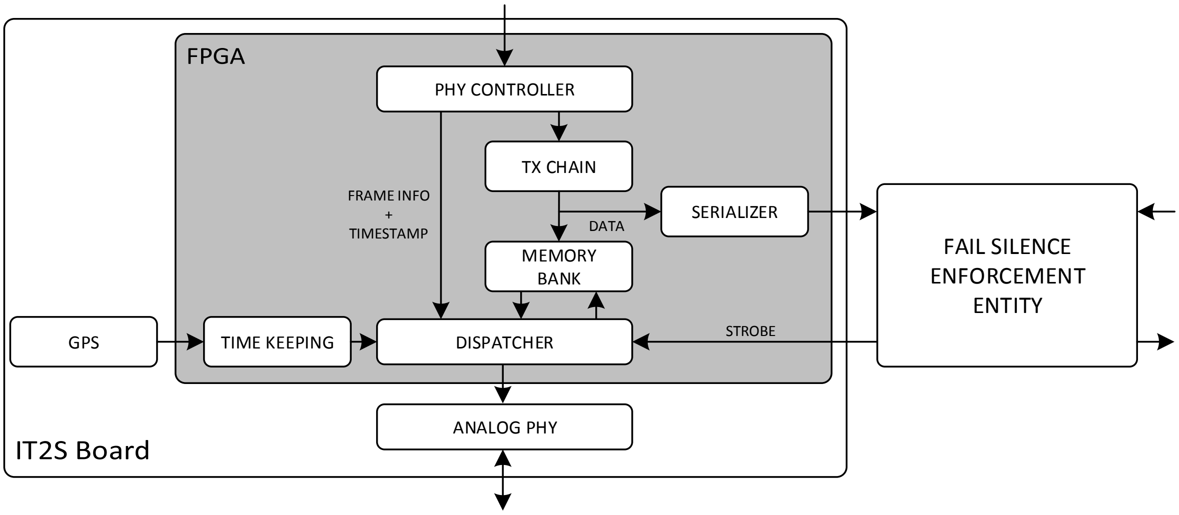


Figure B.9: Digital PHY scheme with fail silence behaviour.

to be verified by the fail silence enforcement entity, which will compare them with the ones provided by the other IT2S platform. The same samples are stored in a Memory Bank, waiting for the strobe signal to be sent to the wireless medium.

In case of successful frame validation, the Dispatcher module will receive the strobe indication and will start to prepare the transmission of the frame. Hence, it will compare the timestamp provided by the PHY Controller module, specifying in which moment the message should be sent, with the current time of the system, available from the GPS receiver. When both time values are equal, the Dispatcher reads the samples stored in the Memory Bank and send them to the Analog PHY. On the other hand, if the verification process performed by the fail silence entity fails, no strobe signal is received by the Dispatcher and consequently, no message will be issued to the wireless medium.

B.4 Experimental Evaluation and Results

The proposed architecture (figure B.8) was successfully implemented in a Spartan-6 LX150 FPGA using the Trenz TE0300 carrier board. To validate the proposal, both comparison modules were tested. When two equal frames were sent with a phase offset below the maximum time tolerance limit, the strobe signal was successfully generated. However, when at least one bit error was introduced in one of the frames (figure B.10), the value domain comparison module was able to detect it, identifying a fault in the normal operation of the system. In this case, no strobe signal was generated and the fail silence entity entered into an idle state until a reset signal was received. This fault injection mechanism successfully tested the operation of the fail silence entity when the frames sent to validation were completely different as well as when there was only one error bit randomly inserted in a sample of one of the frames (as illustrated by the red striped mark in figure B.10). The same result was achieved when a delay greater than the maximum tolerance allowed was introduced in the transmission of one of the frames (figure B.11). In this situation, the time domain comparison module detected

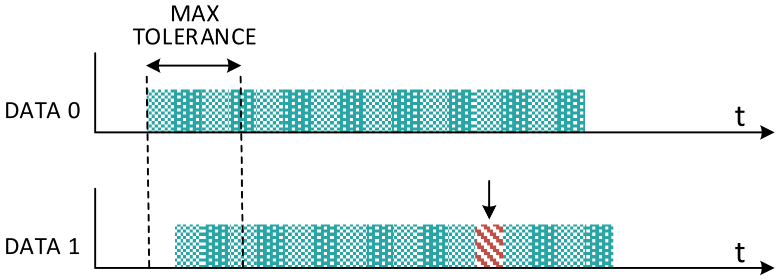


Figure B.10: Fault detection in value domain.

the excessive time difference between the beginning of the two frames and, similarly to the previous case, it signalled a fault to the strobe signal generation module.

As a proof of concept, the fail silence enforcement entity was developed in the same FPGA model that was used to implement the Lower MAC and the physical layer of the IT2S platform. However, when comparing the resource usage of both projects, it can be concluded that the fail silence enforcement entity occupies much less resources (table B.1), around 1% of the total available, than the project for the IT2S platform (table B.2).

This result proves that the fail silence entity is much simpler than the entire vehicular communications platform and therefore, it is less prone to design errors and possible faults that can occur during system's operation. The simplicity of this unit is an extremely important characteristic that can be used to achieve a higher level of reliability, thus improving the dependability of the road-side infrastructure. Furthermore, in a future iteration of the fail silence enforcement entity, a smaller, less expensive FPGA, should be considered in order to reduce the implementation cost of this mechanism.

The frame verification time by the fail silence entity is another important aspect that should be considered when this mechanism is used to validate the operation of a deterministic wireless protocol, such as V-FTT. Figure B.12 shows the total delay introduced by the operation of the fail silence enforcement entity (FSEE) for various frame durations, from $1\mu s$ to $1ms$. This verification time ($T_{verificationTime}$) is essentially constituted by two components:

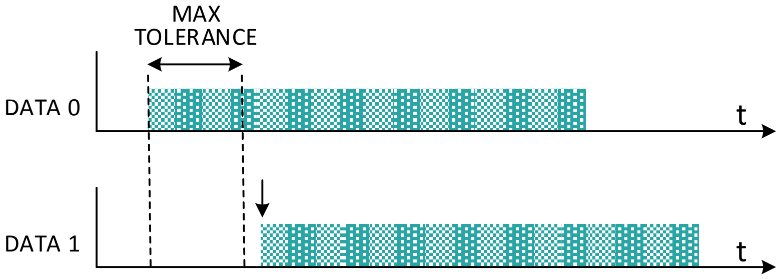


Figure B.11: Fault detection in time domain.

Logic Resources	Used	Total	Percentage used
Flip Flops	314	184304	1%
LUTs	284	92152	1%
RAMB16BWERs	4	268	1%
RAMB8BWERs	4	536	1%
DSP48A1s	0	180	0%
Logic max. frequency - 160.805 MHz			

Table B.1: Fail Silence Enforcement Entity - Resource Usage on Spartan-6 LX150 FPGA.

Logic Resources	Used	Total	Percentage used
Flip Flops	39292	184304	21%
LUTs	38111	92152	41%
RAMB16BWERs	196	268	73%
RAMB8BWERs	48	536	8%
DSP48A1s	80	180	44%
Logic max. frequency - 158.188 MHz			

Table B.2: IT2S Platform - Resource Usage on Spartan-6 LX150 FPGA.

the time that takes to transmit the entire message to the fail silence entity ($T_{frameDuration}$) and the delay introduced by the digital hardware blocks inside the FPGA (T_{FSEE}). The latter one is constant and is approximately equal to $1.05\mu s$, while the first one is equal to the frame duration. Thus, the delay introduced inside the fail silence entity becomes negligible when the frame size increases, and in that case the frame verification time is approximately equal

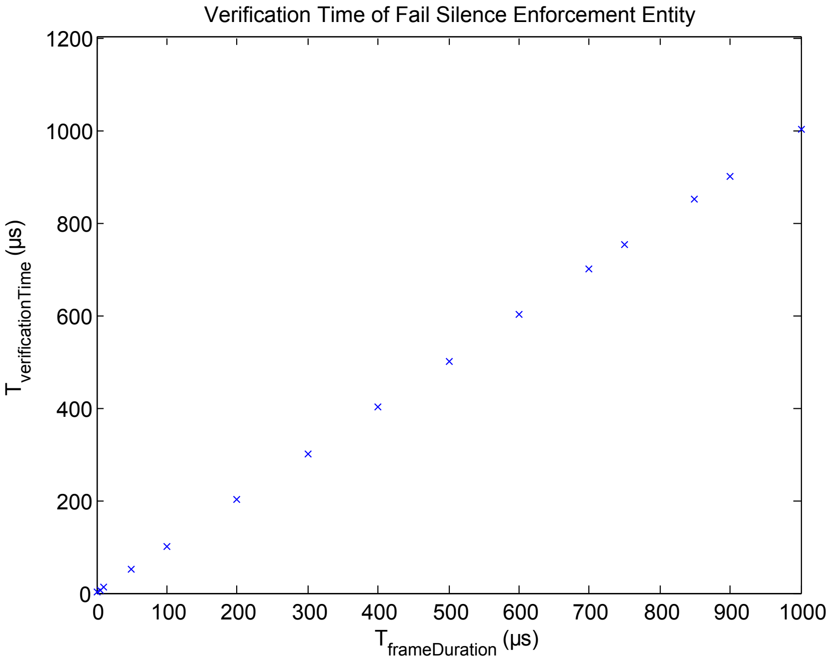


Figure B.12: Verification time as a function of frame duration.

to the frame duration. For instance, the total verification time of a frame with $1000\mu s = 1ms$ duration is equal to $1001.5\mu s$. In this case, the delay added by the blocks that process the frames inside the fail silence enforcement entity (T_{FSEE}) is very small when compared to the time it takes to send the complete set of samples for comparison. Therefore, in this situation, the total verification time is strongly influenced by the value of the $T_{frameDuration}$.

$$T_{verificationTime} = T_{frameDuration} + T_{FSEE} \tag{B.1}$$

Therefore, the samples should start to be sent to the fail silence enforcement entity, with a time advance ($T_{advance}$) greater than the one given by equation B.2, so the message could be send to the air at the exact planned instant. The maximum tolerance allowed also contributes to this guard interval, since the verification time was measured when both platforms transmitted the same message at the same time, not considering a possible misalignment in the absolute clock sources.

$$T_{advance} \geq T_{verificationTime} + T_{maxTolerance} \tag{B.2}$$

This $T_{advance}$ time added to the normal operation of the system during the transmission of a message is completely acceptable, since the RSUs can start to prepare the packets for transmission with a large time advance. Given the fact that RSUs have a global vision of the road trough the backhauling network, they can easily compute the schedule of the next Elementary Cycle at the beginning of the current one. This represents an advance of approximately 100 ms (the total EC duration), which is more than enough to allow the inclusion of the fail silence mechanism in the operation of the system.

B.5 Conclusions

In this paper, a fail silence enforcement mechanism for road side units was presented and evaluated. This mechanism is part of a wider strategy that aims to provide determinism and fault-tolerant behaviour in infrastructured vehicular networks. The fail-silence mechanism compares the output messages produced by two vehicular communications platforms, both in value and time domain. Ideally, these two systems should produce the same outputs based on completely different hardware and software implementations. This should be done to avoid common mode failures. However, as a proof of concept, two identical IT2S platforms were used.

The obtained results show that the developed mechanism successfully detects system faults both in time and value domain. The mechanism can be implemented in an FPGA with few resources, but it should belong to a separate fault confinement region with different power supply and clock source. Moreover, the delay introduced by the operation of the fail silence entity could be significant for large frame sizes, so it should be taking into consideration when analysing the whole performance of the wireless communications protocol.

As future work, security attacks that could destroy the desired fail silent behaviour will be analysed and a strategy to handle those intrusions at the IT2S Gateway level will be deployed.

The goal is to eliminate or at least strongly reduce the architecture's vulnerability to this type of byzantine faults, which may arise when both IT2S platforms process the same incorrect information received through the IT2S Gateway. Additionally, this work on the design of dependable vehicular networks will proceed with the development and implementation of the remaining mechanisms that constitute the fault-tolerant architecture proposed on section B.2. These mechanisms include RSU's replication to cope with failures on the primary fail silent road side unit and the development of medium guardians to temporally isolate the transmission slots of the mobile nodes of the network (OBUs).

Acknowledgements

This work is funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia under the PhD scholarship ref. SFRH/BD/52591/2014 and the project PEst-OE/EEI/LA0008/2013, by the European Union's Seventh Framework Programme (FP7) under grant agreement n. 3176711 and by BRISA, under research contract with Instituto de Telecomunicações - Aveiro.

References

[1] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety", *Communications Magazine, IEEE*, vol. 44, no. 1, pp. 74–82, Jan. 2006, ISSN: 0163-6804. DOI: 10.1109/MCOM.2006.1580935.

[2] L. Pu, X. Xu, H. He, H. Zhou, Z. Qiu, and Y. Hu, "A flexible control study of variable speed limit in connected vehicle systems", *IJES*, vol. 7, no. 2, pp. 180–188, 2015. DOI: 10.1504/IJES.2015.069997. [Online]. Available: http://dx.doi.org/10.1504/IJES.2015.069997.

[3] J. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, ISSN: 0018-9219. DOI: 10.1109/JPROC.2011.2132790.

[4] G. Bansal and J. Kenney, "Controlling Congestion in Safety-Message Transmissions: A Philosophy for Vehicular DSRC Systems", *IEEE Vehicular Technology Magazine*, vol. 8, no. 4, pp. 20–26, Dec. 2013, ISSN: 1556-6072. DOI: 10.1109/MVT.2013.2281675.

[5] T. K. Mak, K. P. Laberteaux, and R. Sengupta, "A Multi-channel VANET Providing Concurrent Safety and Commercial Services", in *Proceedings of the 2Nd ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET '05, Cologne, Germany: ACM, 2005, pp. 1–9. DOI: 10.1145/1080754.1080756. [Online]. Available: http://doi.acm.org/10.1145/1080754.1080756.

[6] A. Böhm and M. Jonsson, "Real Time Communications Support for Cooperative, Infrastructure-Based Traffic Safety Applications", *International Journal of Vehicular Technology*, 2011. DOI: 10.1155/2011/541903.

[7] V. Milanes, J. Villagra, J. Godoy, J. Simo, J. Perez, and E. Onieva, “An Intelligent V2I-Based Traffic Management System”, *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 1, pp. 49–58, Mar. 2012, ISSN: 1524-9050. DOI: 10.1109/TITS.2011.2178839.

[8] N. Lu, X. Wang, P. Wang, P. Lai, and F. Liu, “A distributed reliable multi-channel MAC protocol for vehicular ad hoc networks”, in *Intelligent Vehicles Symposium, 2009 IEEE*, Jun. 2009, pp. 1078–1082. DOI: 10.1109/IVS.2009.5164431.

[9] ETSI TR 102 862 V1.1.1, *Intelligent Transport Systems (ITS); Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part*, Dec. 2011.

[10] K. Xing, T. Gu, Z. Zhao, L. Shi, Y. Liu, P. Hu, Y. Wang, Y. Liang, S. Zhang, Y. Wang, and L. Huang, “Approaching reliable realtime communications? A novel system design and implementation for roadway safety oriented vehicular communications”, in *INFOCOM, 2013 Proceedings IEEE*, Apr. 2013, pp. 115–119. DOI: 10.1109/INFCOM.2013.6566746.

[11] J. Rezgui and S. Cherkaoui, “About Deterministic and non-Deterministic Vehicular Communications over DSRC/802.11p”, *Wireless Communications and Mobile Computing*, vol. 14, no. 15, pp. 1435–1449, 2014, ISSN: 1530-8677. DOI: 10.1002/wcm.2270. [Online]. Available: http://dx.doi.org/10.1002/wcm.2270.

[12] P. Veríssimo, “Uncertainty and predictability: Can they be reconciled?”, in *Future Directions in Distributed Computing*, Springer-Verlag LNCS 2584, May 2003.

[13] A. Durresi, M. Durresi, V. Bulusu, and L. Barolli, “Secure broadcast for inter vehicle communications”, *IJHPCN*, vol. 5, no. 1/2, pp. 54–61, 2007. DOI: 10.1504/IJHPCN.2007.015764. [Online]. Available: http://dx.doi.org/10.1504/IJHPCN.2007.015764.

[14] T. Meireles, J. Fonseca, and J. Ferreira, “The Case for Wireless Vehicular Communications Supported by Roadside Infrastructure”, in *Intelligent Transportation Systems Technologies and Applications*, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, Eds., John Wiley & Sons, Ltd, 2015, pp. 57–82, ISBN: 9781118894774. DOI: 10.1002/9781118894774.ch4. [Online]. Available: http://dx.doi.org/10.1002/9781118894774.ch4.

[15] S. Khan, P. Pedreiras, and J. Ferreira, “Improved Real-Time Communication Infrastructure for ITS”, in *INForum 2014*, Sep. 2014, pp. 430–445.

[16] F. B. Schneider, “Implementing Fault-tolerant Services Using the State Machine Approach: A Tutorial”, *ACM Computing Surveys*, vol. 22, no. 4, pp. 299–319, Dec. 1990.

[17] C. Campolo and A. Molinaro, “Multichannel communications in vehicular Ad Hoc networks: a survey”, *IEEE Communications Magazine*, vol. 51, no. 5, pp. 158–169, 2013, ISSN: 0163-6804. DOI: 10.1109/MCOM.2013.6515061.

[18] L. Z. and Weiping Wang, J. Gao, and J. Wang, “Lossy links diagnosis for wireless sensor networks by utilising the existing traffic information”, *IJES*, vol. 6, no. 2/3, pp. 140–147, 2014. DOI: `10.1504/IJES.2014.063811`. [Online]. Available: `http://dx.doi.org/10.1504/IJES.2014.063811`.

[19] “IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation”, *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pp. 1–89, 2011. DOI: `10.1109/IEEESTD.2011.5712769`.

[20] H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications.* Norwell, MA, USA: Kluwer Academic Publishers, 1997.

[21] D. Powell, I. Bey, and J. Leuridan, Eds., *Delta Four: A Generic Architecture for Dependable Distributed Computing.* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1991, ISBN: 0387549854.

[22] C. Temple, “Avoiding the babbling-idiot failure in a time-triggered communication system”, in *Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on*, Jun. 1998, pp. 218–227. DOI: `10.1109/FTCS.1998.689473`.

[23] P. Bernstein, “Sequoia: A Fault-Tolerant Tightly Coupled Multiprocessor for Transaction Processing”, *IEEE Computer*, vol. 21, no. 2, pp. 37–45, 1988.

[24] S. Webber and J. Beirne, “The Stratus Architecture”, *Digest of Papers FTCS-21*, pp. 79–85, 1991.

[25] F. V. Brasileiro, P. D. Ezhilchelvan, S. K. Shrivastava, N. A. Speirs, and S. Tao, “Implementing Fail-Silent Nodes for Distributed Systems”, *IEEE Transactions on Computers*, vol. 45, no. 11, pp. 1226–1238, Nov. 1996, ISSN: 0018-9340. DOI: `10.1109/12.544479`. [Online]. Available: `http://dx.doi.org/10.1109/12.544479`.

[26] J. Wensley, L. Lamport, J. Goldberg, M. Green, K. Levitt, P. Melliar-Smith, R. Shostak, and C. Weinstock, “SIFT: Design and analysis of a fault-tolerant computer for aircraft control”, *Proceedings of the IEEE*, vol. 66, no. 10, pp. 1240–1255, Oct. 1978, ISSN: 0018-9219. DOI: `10.1109/PROC.1978.11114`.

[27] S. Shrivastava, P. Ezhilchelvan, N. Speirs, S. Tao, and A. Tully, “Principal Features of the Voltan Family of Reliable Node Architectures for Distributed Systems”, *IEEE Transactions on Computers (Special Issue on Fault-Tolerant Computing)*, vol. 41, no. 5, pp. 542–549, 1992.

[28] FlexRay Consortium, *FlexRay Requirements Specification, version 2.0.2*, 2002.

[29] TTTech, *Time-Triggered Protocol TTP/C High-Level Specification Document (edition 1.0)*, `http://www.ttagroup.org`, 2002.

[30] J. Proenza and J. Miro-Julia, “MajorCAN: A modification to the Controller Area Network to achieve Atomic Broadcast”, *IEEE Int. Workshop on Group Communication and Computations. Taipei, Taiwan*, 2000.

Paper C

An RSU Replication Scheme for Dependable Wireless Vehicular Networks

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

in *EDCC 2016 - 12th European Dependable Computing Conference*, pp. 229-240, 2016

The format has been revised.

An RSU Replication Scheme for Dependable Wireless Vehicular Networks

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

Abstract

This paper presents an active replication scheme for the road-side units (RSUs) of an infrastructure-based vehicular network. This mechanism is part of a wider strategy that aims to enhance dependability and provide real-time guarantees in wireless vehicular communications. For that purpose, a fault-tolerant network architecture was proposed, which includes, besides the redundancy scheme presented in this paper, the design of fail-silent RSUs and medium guardians for the on-board units (OBUs) placed inside the vehicles. These strategies target the integration with the operation of a deterministic medium access control (MAC) protocol named Vehicular Flexible Time Triggered (V-FTT), in order to ensure the timeliness properties of this protocol. Nevertheless, the proposed mechanisms are protocol independent and can be employed in other wireless communications domains. The need for such mechanisms is explained in this paper, as well as the architecture, implementation and experimental validation of the proposed replication scheme.

C.1 Introduction

Intelligent Transportation Systems (ITS) focus on the development of strategies to enhance traffic safety, efficiency and comfort. In the scope of this wide subject that embraces land, air and water modes of transportation, there is a trending topic that holds the promise to completely revolutionize the current road traffic systems. This very promising field of research is commonly known as vehicular ad-hoc networks (VANETs), in which the basic goal is to provide communication capabilities among vehicles and between them and the road-side infrastructure. This direct communication with the surrounding environment enables vehicle's driver and passengers with information regarding dangerous road conditions, hazardous events, road works, traffic jams, the presence of emergency vehicles, etc. But the most important fact is that vehicular communications allow drivers to access this information long before these safety events enter their field of vision.

Besides road safety, there are other advantages, such as traffic efficiency and infotainment services. For instance, vehicles equipped with this technology can receive notifications from intelligent road signs or traffic lights and even negotiate their approach to a smart intersection. Vehicular communications rely on the IEEE 802.11-2012 standard, which operates autonomously and in an ad-hoc manner, not depending on the frequently slow and unstable mobile connections provided by network operators. This standard was therefore tailored according to the specific needs of the automotive industry and the high mobility road traffic scenarios. For example, the channel bandwidth was reduced to 10 MHz in comparison with the 20 MHz typically used in Wi-Fi devices, in order to mitigate the impact of Doppler effect. Another important modification was the removal of association and authentication procedures during communication link establishment, commonly used in the IEEE 802.11 family of standards. This enables quicker non-IP data exchange, which is essential for the cases when communication links only exist for a short amount of time.

Despite the great potential of vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communications, there are still problems that current protocol stacks and associated standards are unable to solve [1]. Scalability is one of the main issues, since native IEEE 802.11 is not capable to provide timeliness guarantees under dense traffic scenarios [2]. This is due to the non-deterministic behaviour of the carrier sense with collision avoidance (CSMA/CA) method used by the MAC layer. In order to avoid or at least mitigate this problem, several MAC protocols have been proposed in the literature. Some of these proposals are based on ad-hoc and sometimes self-organized networks [3] [4], while others take advantage of the support provided by the road-side infrastructure [5]. Vehicular Flexible Time Triggered (V-FTT) protocol [6] is an example of the latter case, in which the road-side units (RSUs) are responsible for all traffic scheduling and admission control mechanisms. The design of the replication mechanism described in this work, despite not being attached to any particular protocol or technology, targeted the integration with the operation of V-FTT protocol. Therefore, the properties and characteristics of this protocol will be explained in more detail in section C.2.

V-FTT is a multi-master multi-slave MAC protocol, where the RSUs behave as master nodes that dictate all the network rules and assign the time slots for the communications of on-board units (OBUs) placed inside the cars. The reasons for this design choice, focused on the support provided by the infrastructure, are many. First of all, the presence of a road-side infrastructure is fundamental during an initial market penetration phase where not all vehicles are able to communicate with each other. In a completely ad-hoc scenario, a certain penetration rate is required before road users can start benefiting from the deployment of vehicular communications systems [7]. This is one of the reasons why a 1300 km stretch of road, named “ITS corridor”, is being created between The Netherlands, Germany and Austria [8]. The idea is to develop a fully integrated intelligent traffic control system in a continuous segment of road, with the main goal of promoting its benefits in a real world environment. This way, drivers and passengers can experience the advantages of vehicular communications and accelerate their adoption by different governments, motorway operators and automotive industries.

Moreover, there are several applications where the exchange of information with the road-side infrastructure could be very beneficial or even extremely necessary. As demonstrated in [9], information from infrastructure sensing can be absolutely important for self-driving cars in situations where their field-of-view is occluded by other vehicles or obstacles. For safe navigation, the knowledge about vehicles and pedestrians in the occluded area is critical. Therefore in such situations, an infrastructure sensor, like a camera or a radar, would provide a more complete view of the road scenario. This way, autonomous vehicles would have access to additional information about the surrounding environment, thus enabling them to perform better decisions. The same task would be very difficult to accomplish, solely with data from the onboard sensors of the cars. Furthermore, this approach could be very attractive for traffic administrators, such as governments or motorway operators, since they can have more information and control over the road traffic situation.

Similarly, road-side infrastructure can also be very useful for the deployment of infotainment related applications, such as cloud-based multimedia services [10]. By integrating cloud computing and storage with road traffic nodes, vehicular networks can evolve to the Internet-of-Vehicles (IoV) concept [11], in which vehicles are regarded as sensor platforms that collect information from the traffic environment, then feeding it to the infrastructure, in order for that to become available in the cloud. Posteriorly, a traffic management operator can use this data to optimize global traffic efficiency, redirect vehicles in case of accidents or road works, etc.

Nevertheless, the main purpose of vehicular networks is to increase road safety and thus save thousands of lives that are annually lost in car accidents [12]. Hence, vehicular communications should be designed in a dependable and secure way, so they can assist the execution of real-time tasks that operate in this safety critical environment. The road-side infrastructure can assume an essential role in this scenario, since it can be made more reliable than the other parts of the network. One of the arguments that supports this statement is the fact that the cost of the infrastructure can be shared by all road users. As a result, more expensive solutions could be deployed in that side of the network, rather than including them on the individual vehicles. This way, dependability could be easier enforced in these fixed units, and the system could be seen as an instantiation of the *wormhole* metaphor [13]. In this case, the RSUs would be the *wormholes* of the network, since they could for instance, execute certain tasks faster or implement some fault-tolerance techniques that would enhance their dependability attributes. Such level of trustworthiness in system's operation could not probably be attained in an completely ad-hoc scenario, where the cost of developing very reliable nodes and protocols would significantly increase the price of the vehicles.

Another argument for this potential higher level of dependability and security that can be provided by the road-side infrastructure is based on the fact that RSUs are enabled with a global vision of the road, due to the back-hauling network that connects all units. As a consequence, they can use the information shared through this backbone link to develop more informed decisions or to cross-validate safety events. For instance, a malicious node can be detected by comparing the information received by an RSU in its coverage area with the data retrieved from other fixed units and from external sensors such as traffic cameras.

Notwithstanding the importance of improving dependability attributes in vehicular communications, there are very few research works focused on this topic, either for ad-hoc or infrastructure based solutions. Another important aspect is the fact that current standards for vehicle safety only consider accidental failures. Failures due to security threats were excluded, since it was assumed in the past that no external entity communicates with the in-vehicle network of sensors and Electronic Control Units (ECUs). This problem is pointed out in [14] and a solution towards extended safety that encompasses security threats is proposed. Regardless of the little research done in this field, the overall perspective has changed in the last few years and the scientific community in inter-vehicle communication has identified the need for collaboration with some computer science fields, such as fault tolerance, reliable consensus and cognition [15]. Some examples of research works performed in this area are described next.

The HIDENETS - Highly Dependable IP-based Networks and Services - project [16] aimed to develop end-to-end resilience solutions for ubiquitous communication scenarios, such as car-to-car/infrastructure communications. In the scope of this project, a platooning application [17] was deployed as a proof-of-concept for the ability to detect and react to timing faults, to assure safety and to handle certain malicious intrusions. The same scenario was addressed in [18], where a safe distance between the members of a platoon is continuously computed based on the availability of sensor data in each moment in time. The proposed algorithm calculates this safe distance for the Cooperative Adaptive Cruise Control (CACC) system, according to a graceful degradation scheme that adjusts the settings of CACC to keep as much functionality as possible, even in the presence of sensor failures. In [19], a fault detection mechanism is employed to detect not only complete loss of radio communication, but also partial degradation of the wireless link. This situation can arise, for example, in case of damage to an external cable, antenna or connector.

In the context of V-FTT protocol, a fault-tolerant network architecture was proposed [20], with the main goal of enhancing the dependability of real-time vehicular communications. In this paper, an RSU replication scheme is presented as part of that wider strategy that provides fault-tolerant behaviour in infrastructure-based vehicular networks. The contributions of this work include the introduction of a backup replica in every RSU node and the development of a new time-triggered transmission mode for these backup units based on delayed packet transmission and wireless channel sensing. These mechanisms support the operation of a low delay recovery procedure that replaces the activity of primary RSUs in case of failure. The rest of the paper is organized as follows. Section C.2 describes the operation of V-FTT protocol, together with the main features of the proposed fault-tolerant architecture. Section C.3 presents a brief summary of the replication strategies typically found in the literature, while section C.4 depicts the architecture of the implemented RSU replication scheme. Section C.5 presents the experimental setup used to validate the proposed mechanism, as well as the obtained results. Finally, section C.6 summarizes the conclusions and future work.

C.2 Fault-tolerant Architecture for Infrastructure-based Vehicular Networks

C.2.1 V-FTT protocol

V-FTT [6] is a MAC protocol that relies on the spatial Time Division Multiple Access (TDMA) technique, rather than the standard CSMA/CA method utilized in the IEEE 802.11 standard, for controlling the access to the wireless medium in vehicular networks. This way and by using an inter frame spacing smaller than the one allowed by the standard [21], the protocol is able to guarantee strict delay bounds from message generation to channel access.

Despite the fact that V-FTT can be applied to any vehicular scenario, the protocol was devised for traffic areas where there is a series of RSUs interconnected through a backhauling network (e.g., fiber optics). These road sections could be dense traffic zones or accident-prone locations, also know as blackspots, in which the record of accidents is historically high. In V-FTT, these segments with RSU coverage are entitled Safety Zones (figure C.1). Inside these Safety Zones (SZ), the RSUs behave as master nodes of the network, being responsible for scheduling the OBUs' (slaves) transmission slots. These masters are synchronized through GPS receivers placed in each one of the nodes. They also share common knowledge of the road traffic system, which is attained by exchanging update messages holding the current state of each individual RSU's database. These messages are transmitted through the backhauling network, enabling RSUs with a global vision of the road traffic scenario. According to this scheme, RSUs can be analysed as a single entity having all the information about the SZ.

The association of a vehicle with the RSUs of a SZ is as follows. Whenever an OBU enters in the radio coverage of a SZ, it must register with the infrastructure, so that RSUs can start scheduling that vehicle for periodic transmission. This registration process takes place in a contention-based period, ruled by the standard CSMA mechanism, in which each OBU is assigned a temporary identifier. Whenever a vehicle leaves the SZ it will be deregistered from the system. After being registered, the OBUs will be dynamically assigned with specific time

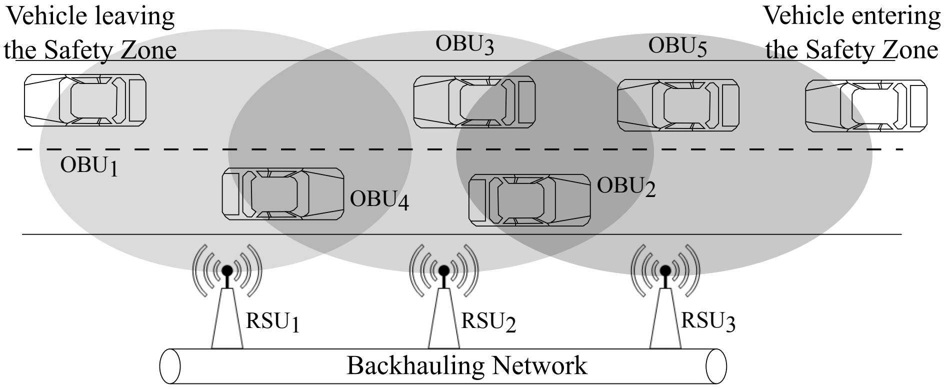

Vehicle leaving the Safety Zone
OBU3
OBU5
Vehicle entering the Safety Zone
OBU1
OBU4
OBU2
RSU1
RSU2
RSU3
Backhauling Network

Figure C.1: Safety Zone concept in V-FTT protocol (adapted from [6]).

slots for sending their packets. In order to ensure an efficient utilization of network resources, a spatial TDMA technique is employed, allowing transmission slot reuse along the road [22].

The protocol is divided into consecutive elementary cycles (ECs) with 100 ms duration and, as can be seen in figure C.2, each EC is further divided into three different parts. It starts with an Infrastructure Window (IW), that is used by the RSUs to transmit two types of messages: trigger messages (TM) with the schedule of the registered OBUs; and warning messages (WM) with cross-validated information regarding safety events that occurred in the road. The second part corresponds to the Synchronous OBU Window (SOW), where each OBU has a fixed size slot to send information to RSUs, either regular data (like vehicle's speed and heading) or a safety event. The Synchronous OBU Window duration is variable, depending on the number of OBUs (denoted as n in figure C.2) scheduled in that particular Elementary Cycle. During both IW and SOW, the nodes do not contend for channel access, since the TDMA algorithm assigns the transmission slots in advance and a small inter-frame space is used between consecutive transmissions, avoiding unwanted transmission from non V-FTT compliant OBUs. On the other hand, there is a contention-based period at the end of each EC, during which *alien* nodes (i.e. OBU nodes not aware of V-FTT protocol and

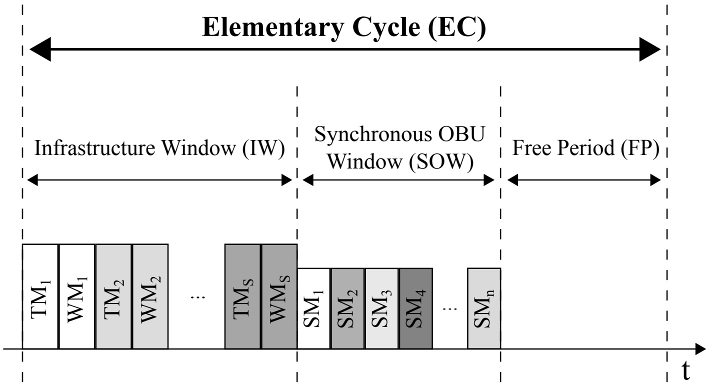


Figure C.2: Elementary Cycle of V-FTT protocol (adapted from [6]).

thus operating according to the standard or another alternative protocol) can communicate, and the V-FTT nodes (both RSUs and OBUs) can exchange non-safety messages. This Free Period (FP) is also used by V-FTT nodes to register themselves with the infrastructure when they initially enter inside the range of a SZ.

In order to increase the probability of successful reception of a TM or a WM by an OBU, several RSUs' coverage areas can partially overlap, causing the same OBU to receive TMs/WMs from different RSUs [23]. This redundancy level (S variable in figure C.2) can be dynamically configured, depending on the number of RSUs in the same region and on the transmission power and sensitivity levels of the nodes of the network. However, some coordination is required among RSUs in order to ensure that for a given OBU, the transmission slot allocated to it in the SOW is the same in all TMs transmitted by the distinct RSUs. This is based on the fact that each OBU will only transmit one message per EC. In a similar way, the OBUs' messages can be received by several different RSUs during the SOW period. Moreover, critical nodes could be assigned with several time slots to re-transmit their messages.

C.2.2 Dependability enhancements in V-FTT networks

A real-time communications protocol, such as the one previously discussed, can attain a higher probability of deliver correct safety services if dependability attributes are considered and mechanisms to enhance them are implemented. This is necessary since several types of faults may occur in vehicular environments. As usual, these faults can be divided into different categories. For instance, regarding the persistence of the fault, both transient and persistent faults can arise in the wireless channel, due to atmospheric conditions in the first case or to unregulated interference in the latter one. Another example is given by considering its intent, that could be accidental, such as a problem with an antenna connector, or malicious, in case of an intrusion in the backbone network that interconnects the RSUs. Other classifications can be applied to distinguish between design-time and run-time faults, timing (omission, crash) and value faults, etc.

From the description of V-FTT protocol, one can conclude that RSUs play a very important role, since they are responsible for all traffic scheduling and admission control mechanisms. If one of these master nodes stops working properly, all communications in its coverage area can be severely compromised. In fact, when an RSU fails to transmit trigger messages with the EC-schedules, transmit them out of time or with erroneous contents, then all network activity could be disrupted, since the result of the TDMA slot assignment algorithm is not delivered to the mobile nodes or simply becomes invalid. There are no guarantees anymore regarding the timeliness and deterministic properties of the protocol. Given this, the RSUs should be regarded as single points of failure in the vehicular network and appropriate measures should be taken accordingly. For that purpose, fault-tolerant techniques need to be included in vehicular communication systems, in order to cope with the presence of unpredicted operating problems.

A failure in a fixed node of a vehicular network (i.e, an RSU), can be handled using a replication strategy with similar nodes acting as backup ones. This is the solution proposed in this paper and that is depicted in figure C.3. There are active masters that regularly communicate and send messages with the TDMA schedules and there are also backup replicas that in case of failure, replace the operation of the primary RSUs. To ease the task of designing a replication scheme, a fail silence mechanism was proposed in [24]. This mechanism ensures that RSUs present fail silent behaviour, i.e, they can only fail by not issuing any message to the network. With fail silence behaviour and by properly handling omissions, an error inside a node cannot affect other nodes and thus each node becomes a different fault confinement region [25]. The use of fail silent nodes also reduces the complexity of designing fault-tolerant systems, since in order to tolerate k failures, only $k + 1$ replicas are needed instead of the $3k + 1$ that are required if the replicas can fail uncontrolled. In this case, the fail-silence failure semantics is attained by using an internal redundancy scheme with output comparison. Two vehicular communications systems (the IT2S platforms in the left side of figure C.3) are producing the same sequence of messages, whose agreement, both in value and time domains, is validated by an external fail silence enforcement entity. If the contents of both messages, at the end of digital physical layer, are equal and the platforms are synchronized, the fail silence entity will allow the transmission of the frame to the air medium. On the other hand, if the messages differ, even if it is only in a single bit, or if they are out of phase, no packet will be sent to the wireless channel.

The mobile nodes of the network should also present fail silence behaviour, both in value and time domains. However, the solution implemented in the RSUs would probably be considered too expensive if applied individually to each one of the vehicles, since in this case the cost is not supported by the road operator, but instead by each vehicle's owner. Moreover and despite the importance of the messages exchanged by the mobile units, they are not responsible for supporting any critical network functionality, e.g. traffic scheduling. Hence,

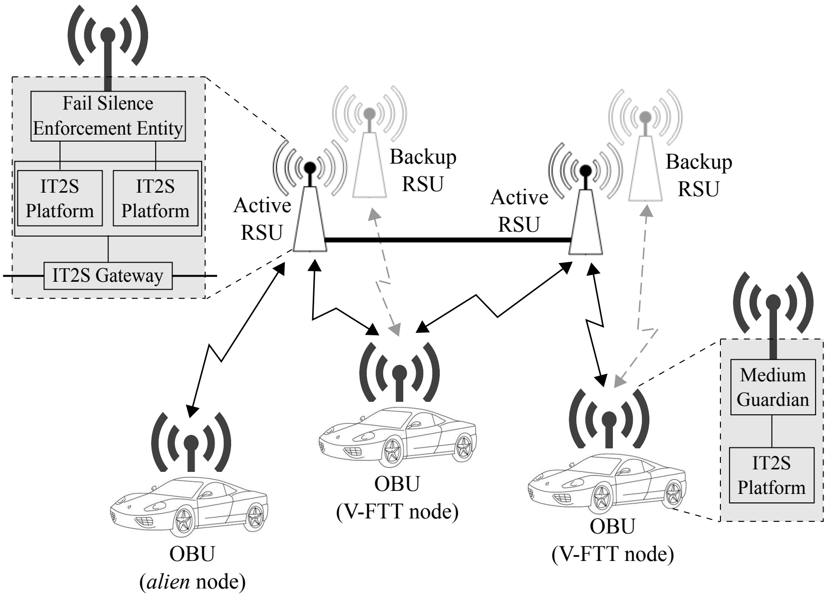


Figure C.3: Fault-tolerance mechanisms in V-FTT network (adapted from [20]).

a more inexpensive solution should be considered for the OBUs. By carefully analysing the operation of V-FTT protocol, it can be concluded that the slave nodes are not responsible for any type of network coordination and therefore, the information transmitted by them, do not affect the remaining communications in the wireless channel. As a consequence, it would be enough to validate the messages transmitted by an OBU only in the time domain, in order to ensure that OBU's transmissions only occur in the designated time slots. From the OBU's perspective, a schedule is valid only within the scope of an elementary cycle, thus an entity policing the node, only needs to be aware of the node schedule in an EC by EC basis. This entity can be regarded as a medium guardian that avoids node's transmissions outside the time slot assigned to it by the masters of the network - the RSUs. For that, this medium guardian just needs to decode every trigger message contents and block any unscheduled transmission from the node. Fail-silence enforcement both in time and value domain should only be adopted in special cases where the slave node information (value and timing) is absolutely essential, e.g., for police and emergency vehicles.

After guaranteeing that all active RSUs exhibit fail-silence behaviour, a replication strategy can be used to ensure that even in the presence of a failure in a primary RSU, the trigger messages with the EC-schedules will still be delivered to the OBU nodes. The replication scheme proposed in this paper will be described in more detail in section C.4. The next section reviews the main categories of replication techniques typically found in the literature.

C.3 Replication Strategies

The replication of subsystems that fail in an independent way is one of the most common methods to build fault-tolerant distributed systems. The goal of this approach is to give other subsystems the idea that the delivered service is provided by a single entity. In order to enforce consistency among the replicas, there are two main categories of replication schemes: active and passive replication.

Active replication [26] [27], also called state machine approach, is characterized by having all the replicas receiving and processing the same sequence of requests in parallel, and producing the same output result at the end. In order to ensure that the state of these replicas is kept consistent, i.e. that they will produce the same output, it has to be guaranteed that all of them are fed with the same inputs in the same order, typically by employing an atomic broadcast protocol to disseminate the commands [28]. These requests are handled independently but must be processed in a deterministic way. In active replication, there is no need for an explicit recovery procedure when one of the replicas fails, since the other ones will continue to provide correct service. Therefore, this technique is simple and transparent to the clients in case of node failure. However there are some disadvantages with this approach. For example, the determinism constraint may be difficult to enforce (e.g. in a multithreaded node) and it is resource demanding, because the operation of each replica requires a full set of resources.

Passive replication, also known as primary backup [29], is more economic than the active scheme, because only one replica, the primary one, processes the commands and produces the output results. The remaining replicas, called secondary or backup, remain in idle state and only interact with the primary to update and log all commands. When the primary system fails, the output result can not be delivered immediately with this technique. Instead, one of the backup replicas is selected as the new primary and it will resume operation from the last well known state of the system with the aid of the information available in the log repository. In this case, the client will time-out and resend the request after detecting the new primary replica. This significantly increases the response time of the system in case of failure, making this method unsuitable for some time sensitive applications. In passive replication, no determinism constraint is necessary but special care must be put on the mechanisms that enforce agreement between primary and backups.

Semi-active and semi-passive replication are two variants of the replication schemes referred above. The idea behind semi-active replication [30], also called leader-follower, is that the replicas do not need to process requests in a deterministic way. Only one replica (the leader) is responsible for making non-deterministic decisions and inform the followers of these choices. In semi-passive replication [31] [32], client requests are received by all replicas and every replica delivers its responses back to the client. This way, the clients do not need to know the identity of the primary and there is no need for time-outs to detect the crash of the primary, being system failures completely masked to the client. Semi-passive replication is fully based on failure detectors and thus it does not require an agreement method (e.g. membership service) to select the primary replica. This reduces the response time in case of crash of the primary, when compared with the passive replication approach.

The earlier replication strategies proposed in the literature were mostly focused on applications for which real-time behavior was not an essential requisite. However, real-time applications usually operate under stringent timing and dependability constraints thus, several replication strategies had been developed [33] [34] [35] [36], in order to solve the additional challenges posed by safety-critical applications.

C.4 RSU Replication Scheme

Given the timeliness requirements of deterministic vehicular communications protocols, such as V-FTT, the RSU replication strategy proposed in this paper follows an active or state machine approach. In this way, as soon as a missing trigger message is detected, a backup master comes into the foreground and transmits it, maintaining the communication without any discontinuity of the traffic scheduling. Nevertheless, this is only possible if all master replicas are synchronized, with respect to value and time. The detailed strategies to ensure replica consistency between active and backup RSUs are not addressed in this paper and will be object of study in future work. For now, one can think of a simple mechanism where the messages transmitted over the air are consistently delivered to all replicas by employing one of the atomic broadcast protocols previously proposed in the literature. To save network resources (namely channel usage), the atomic broadcast could be enforced through a dedicated wired link between the replicas rather than by using the wireless medium, which is also more prone to message errors. The core contribution of this work consists in a technique developed at the lower layers of the protocol stack that guarantees low-delay in the recovery procedure of RSUs in case of failure. To the best of authors' knowledge, this type of mechanism has never been proposed in the design of fault-tolerant wireless systems in general and can play a key role in the development of replication schemes targeting wireless real-time applications.

In this active scheme, it is thus assumed that the backup RSUs receive and process the exact same sequence of messages in parallel with the active one, and produce the same trigger messages in each EC. However, the packet transmission operation in the backup RSUs is deliberately delayed by a small amount of time, in the order of few μs, relatively to the primary nodes. This is done with the objective of facilitating the recovery procedure in case of RSU failure, by making it completely automatic and transparent to the slave nodes. This way, if the active RSU is able to transmit the trigger message in the planned instant, the backup will sense the wireless medium as occupied and will conclude that the primary system is free of error. Hence, it will not issue any message to the air, avoiding any overlap with the active node. On the other hand, if at that moment the medium is perceived as free, the backup will initiate the transmission of its message and will replace the operation of the previously active RSU. As a result, the trigger messages will still be transmitted on time, since only a small delay is introduced at the beginning of the EC. This delay can be accommodated by the subsequent inter frame space (IFS), and consequently all the following transmission instants of the remaining RSUs' and OBUs' messages can be kept unchanged.

In this paper, only one backup replica is included in the architecture of each RSU node, as depicted in figure C.3. This results from a trade-off between the cost of the infrastructure and the level of reliability attained at the fixed nodes of the network. Furthermore, in order to maintain the deterministic properties of the real-time vehicular communications protocol, the number of backups per RSU should be kept low. Otherwise, the time delay required to recover from a failure in the primary unit could be excessively high, compromising the timings required to transmit the messages.

C.4.1 Fault Model and General Assumptions

Each replica is assumed to exhibit fail-silence failure semantics, which is guaranteed by the fail-silent mechanism developed in [24]. This way, hardware and software faults are covered and masked by the fail-silent behaviour of the RSU replica. Byzantine faults, notably intrusions, are not covered, since these should be also handled at the IT2S Gateway level (figure C.3), the unit that interconnects RSUs among each others. When the active RSU fails, it is expected that the backup replica is working and able to replace the operation of the failed unit. Thus, common failure modes should be avoided between the primary and backup nodes. For that purpose, design diversity could be employed to reduce the risk that both units fail at the same time and to give enough time for a failed replica to be recovered or fully replaced. In this paper however, identical replicas were utilized to validate the proposed replication scheme, since developing similar units using different hardware and software implementations consumes significant time and resources. There is one aspect though, that can lead to a common failure, being that the replica location. In order to successfully decode the same packets and cover the same network radio range, both the primary and the backup replicas should be co-located or at least placed very close to each other, due to the multiple propagation effects in the wireless channel. However, if some adverse event has an impact in that specific site (e.g., vehicle crash), it is probable that both replicas are affected.

Clock synchronization among individual replicas, different RSUs, and also OBUs, is ensured by a GPS receiver located at each one of the nodes. The accuracy provided by this system is typically very high, in the order of few nanoseconds, which is sufficiently good for the operation of the proposed mechanism. Moreover, in RSUs the availability of GPS signal is usually guaranteed, since there are no mobility effects and less obstacle influences. Under normal circumstances, the quality of the received signal can only be affected by adverse atmospheric conditions. However, these effects are commonly not strong enough to degrade the performance of the system, i.e. it can be considered that RSUs are always synchronized in time.

Obviously, it is also assumed in this redundancy scheme that the backup replica is always able to detect the signal emitted by the active node. In other words, it is assumed that the clear channel assessment (CCA) mechanism in the backup replicas is a reliable failure detector of the primary fail-silent nodes. This is based on the fact that the backup and the primary replicas are co-located or at least placed very closed to each other. In this situation, the received signal strength indication (RSSI) level at the backup node is inevitably high, even if the active node is transmitting with the lowest power value. Hence, the primary unit's transmissions can be reliably detected by the backup RSU, except if a fault happens in the receiver path of the backup node. However, the probability of a fault to occur in the receiving part of the backup unit is much lower than the probability of the primary node to fail in a silent way, since this last scenario involves much more sources of possible faults ranging from the higher to the lower layers of the protocol stack.

Additionally, if a backup replica overlaps the transmission of an active one, due to an incorrect sensing caused by some fault in the receiver chain, the consequences are in general less problematic than the case when a primary node fails and there is no backup to transmit the message. Let's compare both situations. In the first case, the message corruption can undoubtedly have a negative impact in the vehicular system's operation, specially if its a trigger message with the network scheduling and there is no overlap of the RSUs' coverage areas in the safety zone. But in case of failure of the primary RSU and without a backup, there is an opportunity for an *alien* node (non-enabled V-FTT unit) to transmit, jeopardizing the whole TDMA-scheduling in the current EC. In conclusion, the implementation of the proposed redundancy scheme brings clear advantages and dependability improvements to the operation of the road-side infrastructure and consequently to the whole vehicular communications network.

C.4.2 IT2S Platform

The replication strategy proposed in this work takes advantage of a flexible and reconfigurable vehicular communications system, named IT2S platform [37], developed in collaboration between Instituto de Telecomunicações - Aveiro and BRISA, the main motorway operator in Portugal. This research platform was designed and deployed in the scope of two projects: HEADWAY (Highway Environment ADvanced WArning sYstem) [38], a national project with BRISA Innovation, and ICSI (Intelligent Cooperative Sensing for Improved traffic efficiency) [39], a European Union's FP7 project. The IT2S platform is able to operate according to both IEEE WAVE and ETSI ITS-G5 protocol stacks and includes two radio devices, allowing simultaneous multi-channel operation in both safety and infotainment wireless channels.

Figure C.4 depicts the internal blocks of the IT2S platform. It is constituted by the IT2S board, which is responsible for implementing the lower layers of the protocol stack (the IEEE 802.11 standard), and by a Single Board Computer (SBC), where the higher layers together with the ITS services are executed. If the system is used as an OBU, a third component - the Smartphone - can be connected to the SBC, in order to provide a graphical user interface to the vehicles' drivers and passengers. Furthermore, some other safety services can be added to the system's operation by using the smartphone. e.g. the eCall service can be integrated and possibly include the additional information provided by means of vehicular communications [40].

As already mentioned, the IT2S board implements most of the IEEE 802.11 standard, by performing the tasks related to both the analog and digital domains of the physical layer and the most time critical functionalities of the MAC layer (LowerMAC). This corresponds to all signal processing, message transmission and reception between the antennas and the FPGA. It also includes a GPS receiver for location and time synchronization purposes. The medium access control for message transmission is controlled by a module in the FPGA that implements the standard CSMA/CA mechanism. However, given the white-box access to all system's implementation details, a variety of possible extensions and improvements to the standard operation can be developed. For instance, in order to guarantee the timeliness

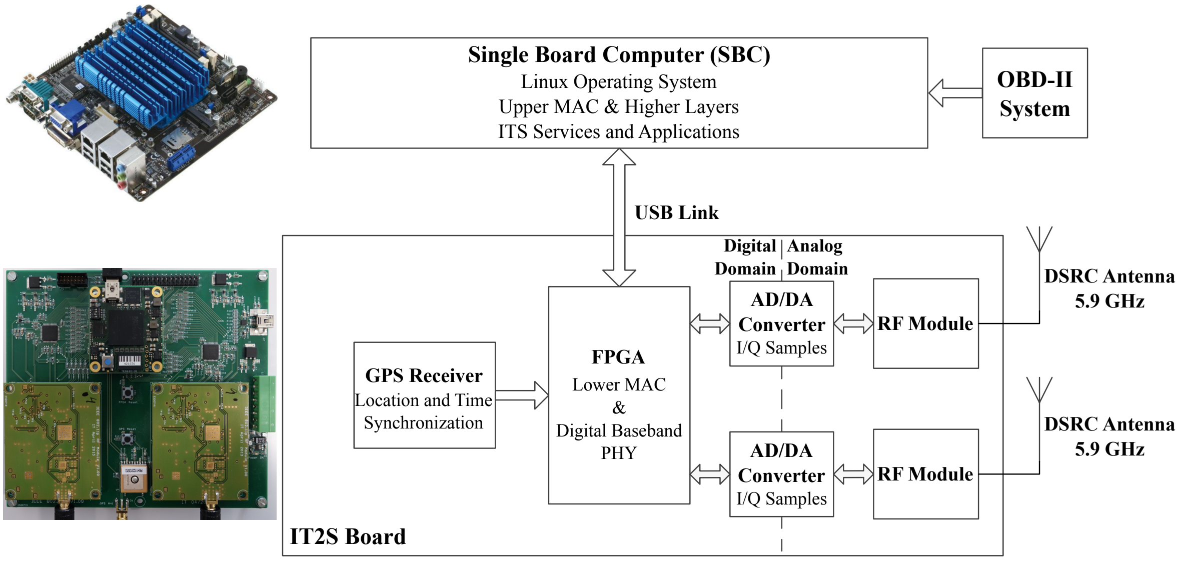


Figure C.4: The IT2S platform (adapted from [37]).

properties of V-FTT protocol, some additional mechanisms needed to be included. One of such mechanisms is the time triggered transmission mode, used to implement the TDMA scheme of V-FTT [41].

C.4.3 Time triggered transmission mode

Nodes of a real-time vehicular communications network, such as one ruled by V-FTT protocol, are required to transmit packets in a timely fashion and with disregard for the state of the wireless medium, resembling the single shot transmission mode present in some fieldbus protocols. For that purpose, the nodes should be capable to disable any carrier sensing mechanism, such as the standard CSMA/CA method. Notwithstanding the fact that this could create some collisions in the wireless medium in case of incorrect protocol design or due to the presence of *alien* nodes (not compliant with the real-time protocol), this type of behaviour is necessary to perform strict TDMA transmissions.

These time sensitive mechanisms must be implemented in hardware at the lower layers of the communications stack, in order to provide low jitter transmissions in the corresponding time slots assigned by the TDMA scheme. This time synchronization at the lower levels can be achieved through the clock signal retrieved from the GPS receiver. Figure C.5 depicts the architectural blocks of the LMAC sublayer, where the described mechanisms were deployed [41]. As it can be seen, there is a *Frame Dispatcher* module that controls the time instants when the messages are transmitted. Its operation can rely on the information provided by the *CSMA/CA Mechanism* block, which corresponds to the IEEE 802.11 standard behaviour, or it can act according to a GPS-based time triggered approach, thus implementing the desired TDMA scheduling policy.

In order to isolate the time critical transmission operation from the jitter introduced in software by the application, the operating system and the device driver, the packets need to

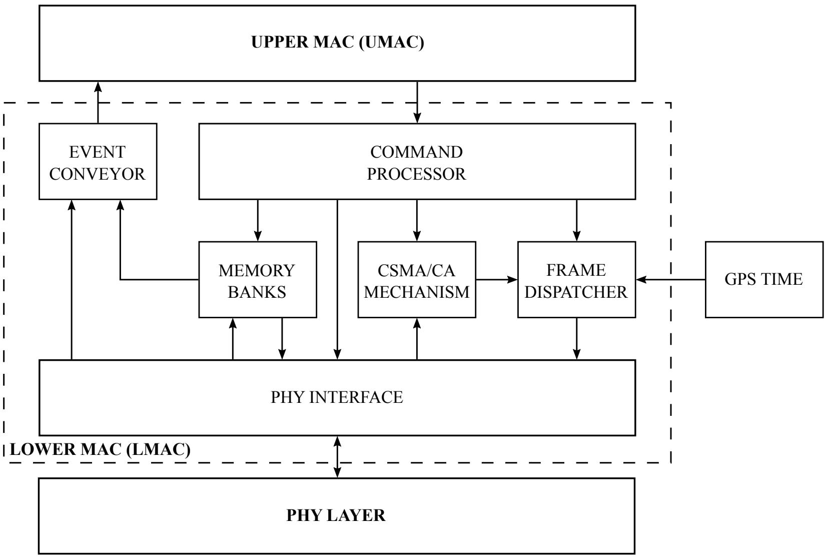


Figure C.5: Block diagram of Lower MAC (adapted from [37]).

be sent to the LMAC well in advance together with a timestamp indicating the moment in which they should be transmitted. These packets are temporarily stored in a buffer (*Memory Banks*), waiting for their respective transmission instant, which will be signalled by the *Frame Dispatcher* based on the GPS time.

Besides low-jitter transmission, these extensions to the standard MAC protocol also guarantee deterministic communications, since by disabling the backoff and enhanced distributed channel access (EDCA) procedures of IEEE 802.11, the nodes have the possibility to violate the standard IFS. This is an essential requirement for the timely operation of the TDMA scheme, given the fact that nodes not compliant with the real-time protocol can be present in the vehicular scenario, and since they are not aware of the assigned scheduling, they may transmit a message in a time slot allocated to a TDMA-enabled node. If all nodes operating according to the deterministic protocol violate the standard IFS, non-compliant devices would continuously sense the wireless medium as busy during the collision free window and would only be able transmit during the free period. This way, the integrity of the TDMA scheduling is preserved and no packet transmissions are corrupted by interfering nodes.

The standard IFS value defined in IEEE 802.11 (10 MHz channels) is 58 μs, thus corresponding to the minimum time before two consecutive transmissions. This is the waiting time necessary for a node to correctly sense the state of the wireless medium, before initiating a packet transmission according to the CSMA/CA mechanism. In the single-shot transmission mode, where the frames are sent regardless the state of the medium and with no re-transmissions, this IFS value can be strongly reduced. Experimental results obtained with the IT2S platform [21] have shown that the minimum IFS can be shortened up to 17 μs.

C.4.4 Backup replica operation

To implement the replication scheme described before, small enhancements need to be deployed in the IT2S platform. Despite the fact that the operation of the backup RSUs is very similar to the primary ones, some modifications are required to produce the desired behaviour. First of all, the timestamp values of the packets sent to the transmission buffer need to be increased by some microseconds, giving enough time for the backup node to detect the failure of a primary unit.

Furthermore, while the primary RSUs transmit their packets in a time triggered way by disregarding the state of the wireless channel, the backup nodes should sense the medium to understand if the primary replica has failed or not. Given the fail silence behaviour enforced in all RSUs and the deterministic operation of V-FTT in the time domain, if the backup replica detects the channel busy in the corresponding time slot, it means that the active RSU is working properly. On the other hand, if no signal is detected by the backup node, it can conclude that the primary RSU has failed. Thus, the backup node should not only take into consideration the state of the medium when transmitting, but also rely its decision on that result.

Based on this reasoning, a slightly modified time triggered transmission mode was implemented in the *Frame Dispatcher* module of the LMAC, allowing the correct operation of the backup RSUs. The resulting decision tree for the transmission of a general packet is presented in figure C.6. This diagram reflects the two paradigms available in the IT2S platform: the standard CSMA-based transmission and the time triggered approach. In the first case, the details of the sensing mechanism and the backoff procedure are hidden, since those are implemented in the *CSMA/CA Mechanism* module (figure C.5). Therefore, when the transmission of a frame following the CSMA/CA method is executed by the *Frame Dispatcher*, all the standard IFS and backoff timings have already elapsed and the CCA value is positive, according to the information provided by the *CSMA/CA Mechanism* block. As a result, as soon as the indication to transmit arrives, the packet is sent to the PHY layer without further verification.

In the case of a time triggered transmission, the *Frame Dispatcher* module takes into account if the node is a primary or a backup replica. In the first scenario, the packet is immediately forwarded to the PHY layer for transmission and its memory slot is released. If the device is a backup, the *Frame Dispatcher* analyses the CCA information to understand if the medium is occupied or not. If the channel is free, it means that the active RSU has failed and consequently the packet will be transmitted. Additionally, the LMAC will signal the higher layers that the primary RSU failed and the node itself is now the active one. On the other hand, if the CCA value is zero, that indicates the primary replica is working and

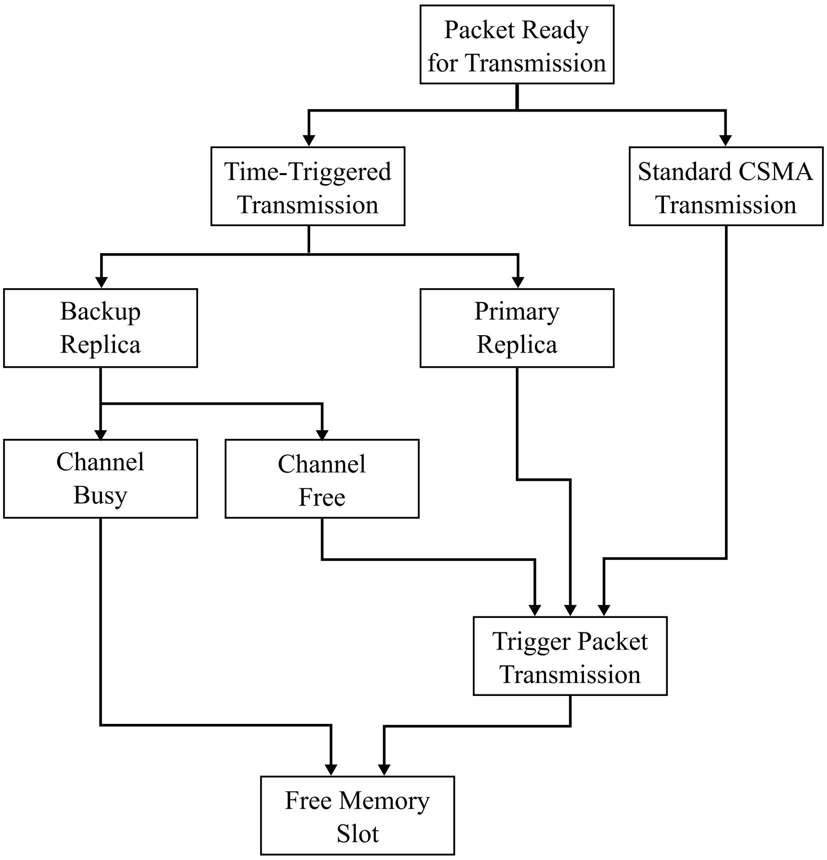

Packet Ready for Transmission
Time-Triggered Transmission
Standard CSMA Transmission
Backup Replica
Primary Replica
Channel Busy
Channel Free
Trigger Packet Transmission
Free Memory Slot

Figure C.6: Decision tree for the transmission of a packet in the LMAC.

therefore, the corresponding packet slot in the *Memory Banks* will be freed without being transmitted.

The configuration of a node as a primary or backup replica is initiated in software at the SBC. Whenever this configuration is altered, a command is issued to the LMAC in the FPGA requiring the modification in the role played by the platform (either active or backup). Then this command is handled by the *Command Processor* module (figure C.5) and as a result, an hardware flag that stores this information is modified accordingly. After that, the *Frame Dispatcher* block only needs to verify the status of this flag to decide which branch of the diagram presented in figure C.6 should be taken. This extension to the LMAC sublayer was seamlessly integrated in the RSUs' operation, allowing the introduction of a redundancy scheme of the master nodes in a transparent way to the mobile units of the network. In order to validate the implementation of the described technique, an experimental setup was devised, being presented together with the obtained results in the next section.

C.5 Experimental Setup and Results

The performance of the proposed RSU replication scheme was evaluated in the experimental setup depicted in figure C.7. Three IT2S platforms were employed, one playing the role of an active RSU, another working as a backup replica and the third one acting as a sniffer node. The tests were carried out in a laboratory environment, with both RSUs co-located (the two antennas were separated by less than 5 cm) and the sniffer unit placed approximately 4 meters apart. All devices were tuned in the same wireless channel with a center frequency of 5.86 GHz, corresponding to channel 172 in the United States and to the service channel number 4 in Europe. The sniffer node was configured to capture the baseband in-phase/quadrature (I/Q) samples of the IEEE 802.11 OFDM frames sent by the RSU nodes. Given the 10-bit ADCs used in the IT2S board, the I/Q values of the captured samples vary between -512 and 511. These samples were post-processed by a MATLAB® script, in order to analyse the transmission behaviour of the RSU replicas.

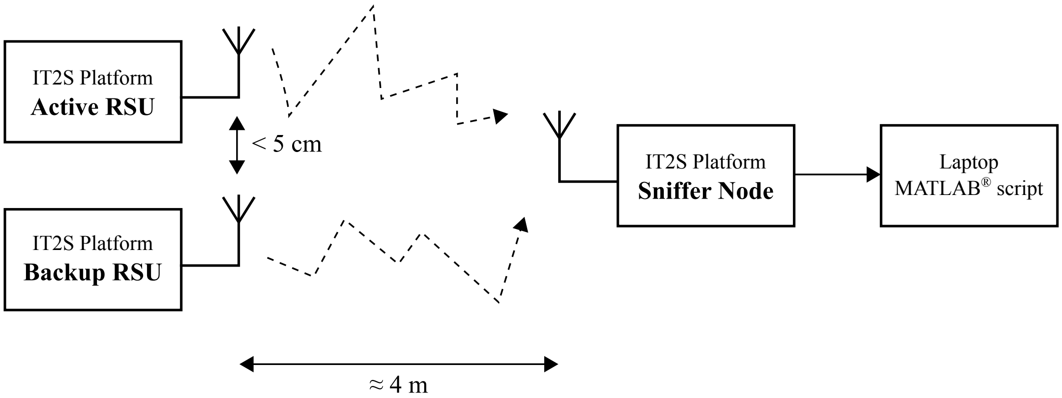


Figure C.7: Experimental setup for the validation of the implemented RSU replication strategy.

C.5.1 Disabling the Clear Channel Assessment Mechanism

As a first experiment, a simple test to validate the single shot transmission mode in the primary RSU was performed. In this mode, the packet transmission follows a time triggered approach and the clear channel assessment (CCA) mechanism is disabled. In other words, the messages are transmitted in the predefined time instants, being the state of the wireless medium completely ignored by the dispatcher module. To prove the correct operation of this transmission mode in the IT2S platform, one forced the channel to be occupied at the moment when the primary RSU's transmission was supposed to occur. For that purpose, the backup RSU acted as an *alien* node not compliant with V-FTT protocol, triggering a packet transmission some μs before the primary node starts transmitting its message. In order to better visualize the effect, the transmit power level used at the primary RSU was much higher than the one utilized in the backup node. The transmitted packets were 30 bytes long in BPSK modulation with coding rate 1/2, corresponding to a 128 μs frame duration.

Figure C.8 plots the 10-bit in-phase samples captured at the sniffer node over time. As it can be observed, the backup RSU (or interfering node) starts to send an IEEE 802.11 packet and less than 100 μs after, i.e. before this first transmission ends, the primary node initiates its transmission by completely disregarding the state of the wireless medium. This result validates the single shot transmission mode described before, providing timeliness guarantees for the execution of V-FTT and similar real-time protocols. In addition, it enables the implementation of the RSU replication scheme proposed in this paper, by guaranteeing that only the backup replica takes into account the CCA value. In the scenario presented in figure C.8 and despite the higher transmit power level, probably the primary RSU's transmission would not be correctly decoded by the majority of nodes listening, due to the interfering signal coming from the *alien* node. However, in this way the scheduling is kept unchanged and the RSU can then control the communications in the wireless channel by violating the IFS in the subsequent transmissions.

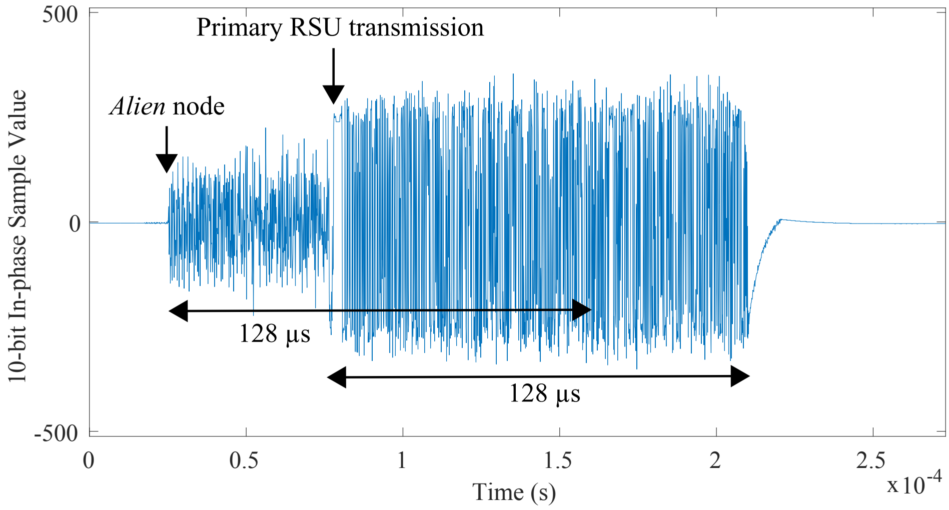


Figure C.8: Time triggered transmission with CCA mechanism disabled.

C.5.2 RSU Replication Scheme

After validating the single shot transmission mode in the IT2S platform, the operation of the implemented RSU replication strategy was analysed under different scenarios. In the first case, both replicas were configured to transmit the same 30 bytes frame but with an offset of 25 μs, i.e. to the transmission timestamp in the backup RSU was added a delay of 25 μs relatively to the primary node. Additionally and in order to give a brief view of how this mechanism can be seamlessly integrated in the TDMA-scheduling of V-FTT protocol, the backup replica was also configured to send two extra frames, one before and another after the transmission under analysis. The minimum IFS between consecutive transmissions was defined as 20 μs. With these timings and as will be demonstrated, the total IFS value (minimum IFS + replica switching time) is always smaller than the standard one (53 μs), ensuring that non-compliant units continuously sense the channel busy thereby keeping the protocol's properties from the previous scheme without replication.

Figure C.9 presents the results obtained in the sniffer node under the described conditions. The primary RSU's transmission was successful, while the backup replica remained silent, not sending the message with the offset of 25 μs. This corresponds to the expected replication behaviour, according to what was defined during the design phase (section C.4). In this experiment, the backup RSU had enough time to sense the transmission of the active node and therefore it has assumed that the primary RSU was working well and there was no need to transmit the delayed backup message. With the parameters specified above (20 μs of minimum IFS and 25 μs of backup replica offset), the idle time between the previous frame and the primary RSU transmission is 20 μs - the minimum IFS value - and between this last one and the next frame is 45 μs - the minimum IFS plus the backup replica offset. The reason for this is the need to guarantee that the minimum IFS value is respected even if the primary replica fails and the backup transmits its delayed message.

This is the scenario presented in figure C.10 where the primary node transmissions were

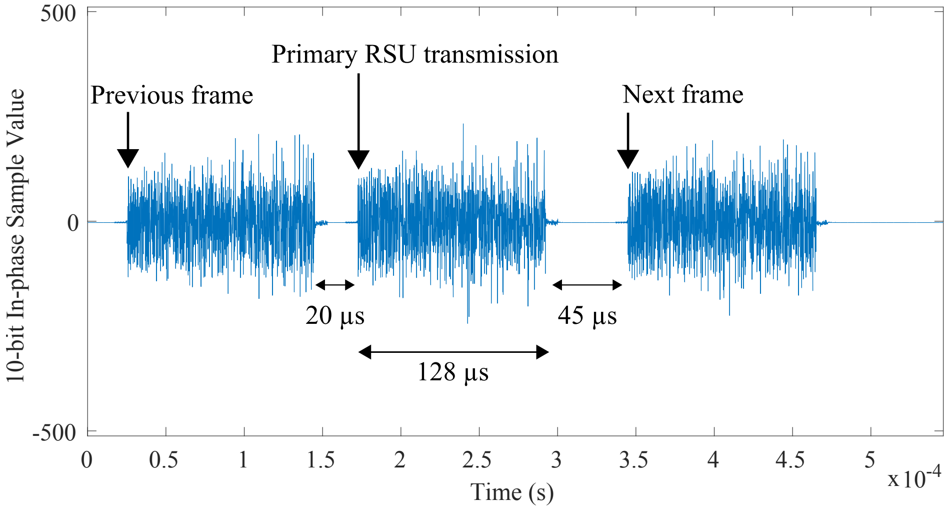


Figure C.9: Primary RSU transmission with a backup replica offset of 25 μs.

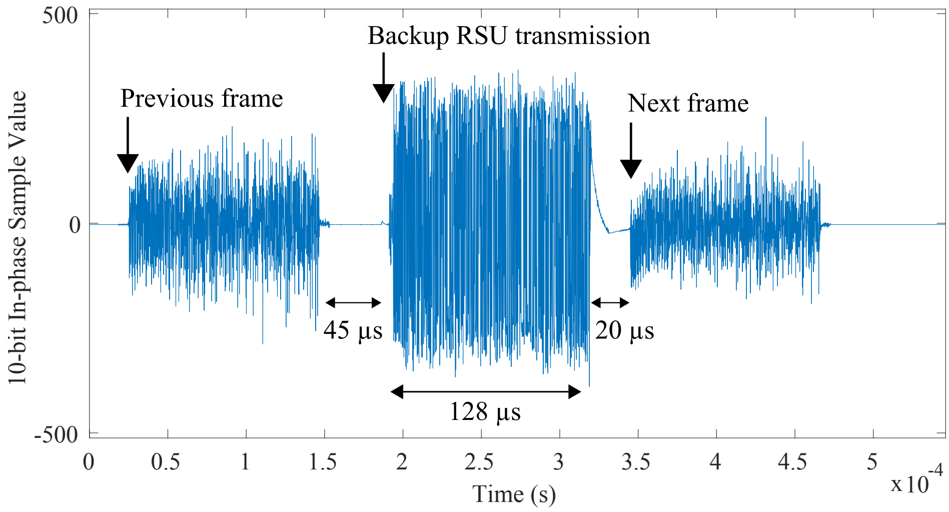


Figure C.10: Backup RSU transmission with the primary replica disabled and a backup replica offset of 25 μs.

disabled in order to simulate a failure event. Since fail-silent behaviour was previously enforced, from the network perspective active RSUs can only fail by not sending any message, thus their single failure mode can be reproduced by stopping all transmissions. In this case, only the backup replica sends the frame, since it realizes that the active unit has failed and stopped transmitting messages. To highlight this result, the transmit power level employed in the backup RSU transmission was higher than the one used in the primary node and in the transmission of the other frames. The beginning of the backup RSU transmission takes place 25 μs after the time instant when the primary node was supposed to start the transmission of its message. As a consequence, the idle time between the previous frame and the backup RSU transmission is 45 μs and between this and the next frame is 20 μs. This way, a minimum IFS value of 20 μs is always ensured, independently of the replica (active or backup) that is transmitting in a certain moment.

Finally, the implemented replication strategy was analysed under the following scenario. Both the primary and the backup RSUs were enabled and ready to transmit, however the backup replica offset was reduced to 12 μs. The obtained result is presented in figure C.11. In this situation, the backup RSU has not enough time to sense the wireless medium and to notice the transmission initiated by the primary node, since the offset in the packets' timestamps between the replicas is too small. Therefore, both platforms send their messages and a collision occurs in the wireless channel. Obviously, this is an undesirable outcome for the protocol's operation, since the information transmitted would not probably be decoded by any node listening.

In order to better understand what is a safe value for the time offset between the primary and backup RSUs' transmissions, a simple experiment was carried out to measure the packet error rate as a function of this time difference. Both the active and backup replicas were configured to transmit the exact same frames in BPSK 1/2 modulation, with a length of

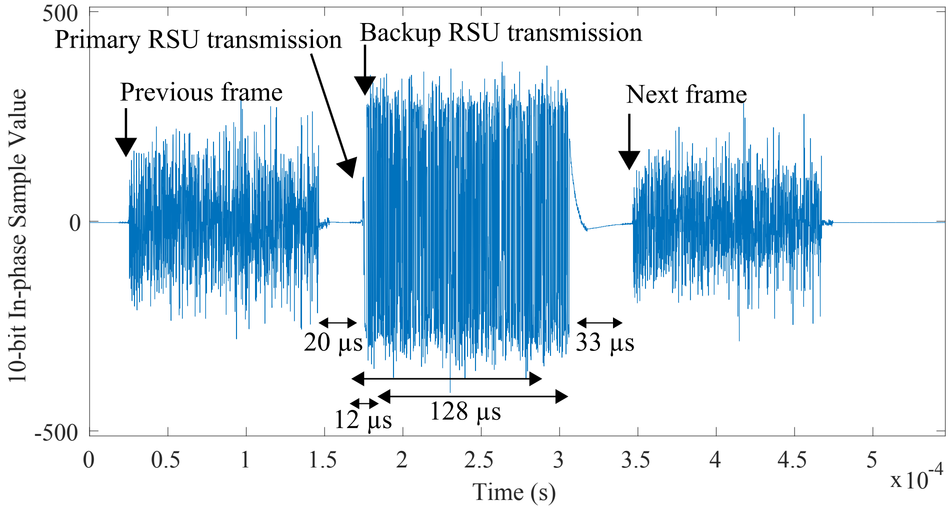


Figure C.11: Overlapped primary and backup RSUs' transmissions for a backup replica offset of 12 μs.

30-bytes and a transmit power level of 0 dBm. Table C.1 summarizes the configuration parameters used in this experiment. The time offset between the primary and the backup transmission timestamps was varied between 0 μs and 25 μs. For each offset value, 10000 transmissions were executed and the number of collisions in the wireless channel was analysed by measuring the packet error rate of the received messages in the sniffer node.

Figure C.12 shows the results obtained in this experimental test. As expected, for small time offsets the packet error rate (PER) is close to 100%, and then gradually it approaches the error free transmission situation (PER = 0 %) with the increase of the offset value. It can be observed that for values higher than 15 μs, the PER value is residual and for completely reliable operation, values above 20 μs can be considered. Hence, it can be concluded that the proposed RSU replication scheme is valid and can be employed to improve dependability in the network's operation. One just needs to ensure that the time offsets between the primary and backup transmissions' timestamps are larger than the safe value derived from figure C.12. As a result, if the active RSU fails, the backup node will replace its operation in a transparent

Table C.1: Configuration parameters for the packet error rate analysis as a function of backup replica offset.

Channel Number	172
Central Frequency	5.86 GHz
Frame Length	30 bytes
Modulation	BPSK
Coding Rate	1/2
Frame Duration	128 μs
Transmit Power Level	0 dBm
Primary-Backup RSUs distance	$<$ 5 cm
RSUs-Sniffer distance	$\approx$ 4 m

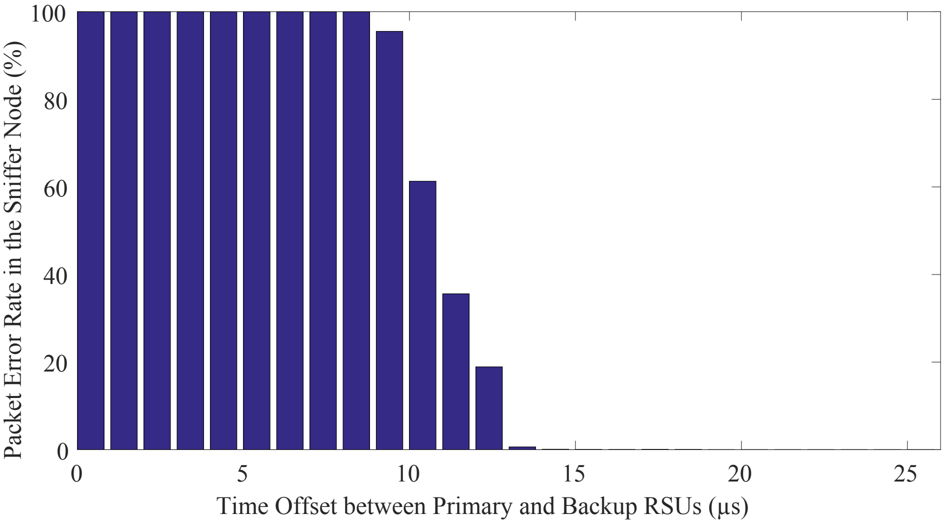


Figure C.12: Packet error rate analysis in the sniffer node as a function of backup replica offset.

way, only with a slight delay (few μs) relatively to the previous primary node's transmissions.

This small delay can be easily accommodated in the resulting IFS intervals, with no impact in the timing properties of the deterministic communications protocol. In the scenarios depicted above, the maximum IFS duration is equal to 45 μs, a value that can still be used in the time-triggered transmissions to protect the scheduled packets against *alien* nodes, by violating the standard IFS value of 58 μs. Without this replication strategy, the trigger messages with the network scheduling would be lost in case of RSU failure, and consequently the vehicles would not be able to transmit according to the real-time TDMA protocol. Now, by using this master's replication scheme, this information can be still be delivered on time to the mobile nodes by the backup unit.

C.6 Conclusions

In this paper, an RSU replication scheme has been proposed to enhance the dependability attributes of infrastructure-based vehicular communication networks. The devised mechanism relies in an active replication strategy that in case of failure of the primary node, continues to provide the expected service without any discontinuity of the real-time TDMA-based protocol scheduling. For that purpose, a backup replica is employed to replace the active RSU's operation when a fail-silent failure is detected. This backup unit is continuously sensing the wireless medium and when it notices an absent RSU transmission, it immediately comes into the foreground and transmits the planned message.

The obtained experimental results have shown the validity of this replication scheme, being only required that the backup node's transmissions are delayed by more than a safe value ($\approx$ 25 μs) relatively to the primary replica. This is required in order to allow the backup RSU to correctly identify a failure in the active node, otherwise it could not have enough time to sense the transmission already initiated by the active RSU. The implementation of the proposed strategy took advantage of a custom vehicular communications device (the IT2S platform), in which non-standard real-time primitives are available, such as disabling the clear channel assessment mechanism and the time-triggered transmission mode. Nevertheless, these functionalities can be easily deployed in any wireless communications module, given access to a common time reference, e.g. provided by a GPS receiver.

As future work, a mechanism to guarantee replica consistency with respect to the vehicle registration's database will be developed. This is an essential feature for the operation of the real-time protocol, since in order to produce the same trigger message in each elementary cycle, the contents of these databases in the different replicas need to be equal. Such inconsistency at the database level is likely to occur, given the fact that in the wireless domain, it is not uncommon to have a packet successfully received by a node and not well decoded by another, even in the case where they are co-located.

Acknowledgements

This work is funded by Fundação para a Ciência e Tecnologia - FCT/MEC through national funds under the PhD scholarship ref. SFRH/BD/52591/2014, by FEDER – PT2020 partnership agreement under the project UID/EEA/50008/2013 and by the European Union's Seventh Framework Programme (FP7) under grant agreement n. 3176711.

References

[1] F. Dressler, F. Kargl, J. Ott, O. Tonguz, and L. Wischhof, "Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl Seminar", *Communications Magazine, IEEE*, vol. 49, no. 5, pp. 158–164, May 2011, ISSN: 0163-6804.

[2] S. Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard", in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, Sep. 2007, pp. 2199–2203. DOI: 10.1109/VETECF.2007.461.

[3] ETSI TR 102 862 V1.1.1, *Intelligent Transport Systems (ITS); Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part*, Dec. 2011.

[4] O. Tonguz and W. Viriyasitavat, "Cars as roadside units: a self-organizing network solution", *Communications Magazine, IEEE*, vol. 51, no. 12, pp. 112–120, Dec. 2013, ISSN: 0163-6804. DOI: 10.1109/MCOM.2013.6685766.

[5] A. Böhm and M. Jonsson, "Real Time Communications Support for Cooperative, Infrastructure-Based Traffic Safety Applications", *International Journal of Vehicular Technology*, 2011. DOI: 10.1155/2011/541903.

[6] T. Meireles, J. Fonseca, and J. Ferreira, “The Case for Wireless Vehicular Communications Supported by Roadside Infrastructure”, in *Intelligent Transportation Systems Technologies and Applications*, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, Eds., John Wiley & Sons, Ltd, 2015, pp. 57–82, ISBN: 9781118894774. DOI: 10.1002/9781118894774.ch4. [Online]. Available: http://dx.doi.org/10.1002/9781118894774.ch4.

[7] G. Chandrasekaran, *VANETs: The Networking Platform for Future Vehicular Applications*, http://www.cs.rutgers.edu/~rmartin/teaching/fall08/cs552/position-papers/006-01.pdf, Accessed 6 November 2015, 2008.

[8] B. Fleming, “Advances in Automotive Electronics [Automotive Electronics]”, *Vehicular Technology Magazine, IEEE*, vol. 10, no. 3, pp. 4–11, Sep. 2015, ISSN: 1556-6072. DOI: 10.1109/MVT.2015.2446446.

[9] B. Rebsamen, T. Bandyopadhyay, T. Wongpiromsarn, S. Kim, Z. Chong, B. Qin, M. Ang, E. Frazzoli, and D. Rus, “Utilizing the infrastructure to assist autonomous vehicles in a mobility on demand context”, in *TENCON 2012 - 2012 IEEE Region 10 Conference*, Nov. 2012, pp. 1–5. DOI: 10.1109/TENCON.2012.6412285.

[10] M.-K. Jiau, S.-C. Huang, J.-N. Hwang, and A. Vasilakos, “Multimedia Services in Cloud-Based Vehicular Networks”, *Intelligent Transportation Systems Magazine, IEEE*, vol. 7, no. 3, pp. 62–79, Fall 2015, ISSN: 1939-1390. DOI: 10.1109/MITS.2015.2417974.

[11] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds”, in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, Mar. 2014, pp. 241–246. DOI: 10.1109/WF-IoT.2014.6803166.

[12] E. Comission, *Statistics - accidents data*, http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm, Accessed 21 March 2016, 2016.

[13] P. Veríssimo, “Uncertainty and predictability: Can they be reconciled?”, in *Future Directions in Distributed Computing*, Springer-Verlag LNCS 2584, May 2003.

[14] L. Ben Othmane, A. Al-Fuqaha, E. Ben Hamida, and M. van den Brand, “Towards extended safety in connected vehicles”, in *Intelligent Transportation Systems - (ITSC), 2013 16th International IEEE Conference on*, Oct. 2013, pp. 652–657. DOI: 10.1109/ITSC.2013.6728305.

[15] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz, “Inter-vehicle communication: Quo vadis”, *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 170–177, Jun. 2014, ISSN: 0163-6804. DOI: 10.1109/MCOM.2014.6829960.

[16] A. Bondavalli, O. Hamouda, M. Kaâniche, P. Lollini, I. Majzik, and H.-P. Schwefel, “The HIDENETS Holistic Approach for the Analysis of Large Critical Mobile Systems”, *Mobile Computing, IEEE Transactions on*, vol. 10, no. 6, pp. 783–796, Jun. 2011, ISSN: 1536-1233. DOI: 10.1109/TMC.2010.222.

[17] L. Marques, A. Casimiro, and M. Calha, “Design and development of a proof-of-concept platooning application using the HIDENETS architecture”, in *Dependable Systems Networks, 2009. DSN ’09. IEEE/IFIP International Conference on*, Jun. 2009, pp. 223–228. DOI: `10.1109/DSN.2009.5270334`.

[18] E. van Nunen, J. Ploeg, A. Medina, and H. Nijmeijer, “Fault tolerancy in Cooperative Adaptive Cruise Control”, in *Intelligent Transportation Systems - (ITSC), 2013 16th International IEEE Conference on*, Oct. 2013, pp. 1184–1189. DOI: `10.1109/ITSC.2013.6728393`.

[19] S. Worrall, G. Agamennoni, J. Ward, and E. Nebot, “Fault Detection for Vehicular Ad Hoc Wireless Networks”, *Intelligent Transportation Systems Magazine, IEEE*, vol. 6, no. 2, pp. 34–44, Summer 2014, ISSN: 1939-1390. DOI: `10.1109/MITS.2014.2304974`.

[20] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Fault Tolerant Architecture for Infrastructure based Vehicular Networks”, in *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira, and J. Fonseca, Eds., Cham: Springer International Publishing, 2016, ch. 8, pp. 169–194, ISBN: 978-3-319-28183-4. DOI: `10.1007/978-3-319-28183-4_8`.

[21] A. Khan, J. Almeida, B. Fernandes, M. Alam, P. Pedreiras, and J. Ferreira, “Towards Reliable Wireless Vehicular Communications”, in *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, Sep. 2015, pp. 167–172. DOI: `10.1109/ITSC.2015.36`.

[22] L. Silva, P. Pedreiras, and J. Alam Muhammad Ferreira, “STDMA-based Scheduling Algorithm for Infrastructured Vehicular Networks”, in *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira, and J. Fonseca, Eds., Cham: Springer International Publishing, 2016, ch. 4, pp. 81–105, ISBN: 978-3-319-28183-4. DOI: `10.1007/978-3-319-28183-4_4`.

[23] J. Almeida, M. Alam, B. Fernandes, M. Awais Khan, A. Oliveira, and J. Ferreira, “Reliable Delivery of Safety Messages in Infrastructure Based Vehicular Networks”, in *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, Sep. 2015, pp. 244–249. DOI: `10.1109/ITSC.2015.49`.

[24] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Fail Silence Mechanism for Dependable Vehicular Communications”, *International Journal of High Performance Computing and Networking (IJHPCN)*, vol. 10, no. 6, pp. 534–545, 2017. DOI: `10.1504/IJHPCN.2017.10008241`.

[25] C. Temple, “Avoiding the babbling-idiot failure in a time-triggered communication system”, in *Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on*, Jun. 1998, pp. 218–227. DOI: `10.1109/FTCS.1998.689473`.

[26] L. Lamport, “Time, Clocks, and the Ordering of Events in a Distributed System”, *Commun. ACM*, vol. 21, no. 7, pp. 558–565, Jul. 1978, ISSN: 0001-0782. DOI: `10.1145/359545.359563`.

[27] F. B. Schneider, “Implementing Fault-tolerant Services Using the State Machine Approach: A Tutorial”, *ACM Computing Surveys*, vol. 22, no. 4, pp. 299–319, Dec. 1990.

[28] M. Wiesmann, F. Pedone, A. Schiper, B. Kemme, and G. Alonso, “Understanding replication in databases and distributed systems”, in *Distributed Computing Systems, 2000. Proceedings. 20th International Conference on*, 2000, pp. 464–474.

[29] N. Budhiraja, K. Marzullo, F. B. Schneider, and S. Toueg, “Distributed Systems (2nd Ed.)”, in, S. Mullender, Ed., New York, NY, USA: ACM Press/Addison-Wesley Publishing Co., 1993, ch. The Primary-backup Approach, pp. 199–216.

[30] D. Powell, I. Bey, and J. Leuridan, Eds., *Delta Four: A Generic Architecture for Dependable Distributed Computing*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1991, ISBN: 0387549854.

[31] X. Défago, A. Schiper, and N. Sergent, “Semi-Passive Replication”, in *Proceedings of the The 17th IEEE Symposium on Reliable Distributed Systems*, ser. SRDS ’98, Washington, DC, USA: IEEE Computer Society, 1998, pp. 43–50.

[32] X. Défago and A. Schiper, “Semi-passive Replication and Lazy Consensus”, *J. Parallel Distrib. Comput.*, vol. 64, no. 12, pp. 1380–1398, Dec. 2004, ISSN: 0743-7315. DOI: `10.1016/j.jpdc.2004.08.006`.

[33] H. Kopetz and G. Grunsteidl, “TTP-a protocol for fault-tolerant real-time systems”, *Computer*, vol. 27, no. 1, pp. 14–23, Jan. 1994.

[34] A. Mehra, J. Rexford, and F. Jahanian, “Design and evaluation of a window-consistent replication service”, *Computers, IEEE Transactions on*, vol. 46, no. 9, pp. 986–996, Sep. 1997.

[35] H. Zou and F. Jahanian, “A real-time primary-backup replication service”, *Parallel and Distributed Systems, IEEE Transactions on*, vol. 10, no. 6, pp. 533–548, Jun. 1999.

[36] S. Poledna, A. Burns, A. Wellings, and P. Barrett, “Replica Determinism and Flexible Scheduling in Hard Real-Time Dependable Systems”, *IEEE Trans. Comput.*, vol. 49, no. 2, pp. 100–111, Feb. 2000, ISSN: 0018-9340. DOI: `10.1109/12.833107`.

[37] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Development of an ITS-G5 station, from the physical to the MAC layer”, in *Intelligent Transport Systems: from Good Practice to Standards*, P. Pagano, Ed., CRC Press, Taylor and Francis Group, 2016, ch. 1, pp. 1–37. DOI: `10.1201/9781315370866-2`.

[38] B. Innovation, *HEADWAY - Connecting vehicles and highways*, `http://www.brisainovacao.pt/en/innovation/projects/headway`, Accessed 28 February 2016, 2012.

[39] ICSI Consortium, *ICSI - Intelligent Cooperative Sensing for Improved traffic efficiency*, `http://www.ict-icsi.eu/`, Accessed 28 February 2016, 2015.

[40] B. Fernandes, M. Alam, V. Gomes, J. Ferreira, and A. Oliveira, "Automatic accident detection with multi-modal alert system implementation for ITS", *Vehicular Communications*, vol. 3, pp. 1–11, 2016, ISSN: 2214-2096. DOI: `http://dx.doi.org/10.1016/j.vehcom.2015.11.001`.

[41] C. Cruz, J. Ferreira, and A. Oliveira, "Supporting Deterministic Medium Access Control in Wireless Vehicular Communications", in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*, Sep. 2015. DOI: `10.1109/VTCFall.2015.7391160`.

Paper D

Timing Analysis of an Active Replication Scheme for the Road Side Units of Vehicular Networks

João Almeida, Muhammad Alam, Joaquim Ferreira and Arnaldo S. R. Oliveira

in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, pp. 4719-4724, 2016

The format has been revised.

Timing Analysis of an Active Replication Scheme for the Road Side Units of Vehicular Networks

João Almeida, Muhammad Alam, Joaquim Ferreira and Arnaldo S. R. Oliveira

Abstract

This paper presents a timing analysis of an active replication scheme previously developed for the road-side units (RSUs) of infrastructure-based vehicular networks. This replication strategy aims to increase fault-tolerance and reliability of RSUs, which are the master nodes of real-time vehicular communications protocols, e.g. V-FTT. Nevertheless, the proposed solution is protocol independent and can be applied to other wireless communications domains. The obtained results show that this replication scheme introduces low delay in the recovery procedure of failed RSU nodes and a small overhead in the protocol communications. However, under specific circumstances it can allow nodes non-compliant with the deterministic protocol to interfere with the scheduled packet transmission. In order to avoid this, some alternative solutions are briefly discussed at the end of the paper.

D.1 Introduction

Vehicular communications support cooperative applications that aim to improve vehicle and road safety, passenger's comfort and efficiency of traffic management. Some of these applications are safety critical and have tight timeliness and throughput requirements. Despite the obvious potential benefits of vehicular communications, the design of dependable vehicular networks is a research challenge, due to the high speed mobility and the open nature of these environments [1]. One of the major problems is the scalability of the standard medium access control (MAC) mechanism (based on the Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA method from IEEE 802.11 [2]) under congested traffic scenarios [3]. As a result, real-time MAC protocols have been developed for controlling channel access in vehicular networks. Some of the proposals rely on a completely ad-hoc framework, while others depend on the support provided by the road-side infrastructure, e.g. the Vehicular Flexible Time-Triggered (V-FTT) protocol [4].

The presence of RSUs connected through a backhauling network provides a global vision of the road traffic situation, which enhances the determinism of collision-free MAC protocols and ensures the existence of a trustworthy entity that is able to cross-validate traffic events, e.g. by using cameras or radars. In this scheme, the RSUs behave as master nodes of the vehicular network, scheduling all the transmissions from the on-board units (OBUs) placed inside the vehicles. However and given the importance of the road-side infrastructure in this scenario, a dependable network architecture focusing on the key role played by the RSUs, should be carefully designed [5]. For that purpose, fault-tolerance mechanisms need to be included in the network operation, as recently identified by the research community in inter-vehicular communications [6].

This work focuses on the timing analysis of an active replication scheme that was previously proposed for the RSUs of infrastracture-based vehicular networks [7]. Despite targeting vehicular communications, this replication strategy is protocol independent and can be employed in other wireless communication domains, particularly for applications in which very precise time-triggered transmissions and real-time guarantees are essential requisites. Therefore, this analysis becomes valid for a broader range of application scenarios, e.g. safety-critical control systems based on industrial wireless communications. Similar timing analysis are commonly found in distributed real-time systems based on fieldbus technologies. For instance in [8], the temporal requirements of a reliable communications protocol for CAN networks are examined by taking into consideration the presence of replicated components and messages. In the wireless domain, few research works are available, but some studies [9] already started to evaluate the impact of replication strategies (e.g. channel redundancy) in the operation of real-time applications.

The rest of the paper is as follows. Section D.2 describes the main properties of V-FTT protocol, while section D.3 presents the dependable network architecture proposed for vehicular networks. Then, in section D.4 the timing analysis of the RSU replication scheme is performed, being the results discussed in section D.5. Finally, section D.6 summarizes the main conclusions.

D.2 Deterministic Vehicular Communications

D.2.1 V-FTT Protocol

V-FTT is a multi-master multi-slave vehicular communications protocol based on a spatial TDMA scheme [4]. The RSUs are the master nodes of the network, which are connected through a backbone link (e.g. fiber optics), thus sharing a common view of the traffic situation. These masters define all network communications and admission control policies, transmitting periodic messages with the scheduling information of OBUs' transmissions - the slave nodes. This way, it is possible to avoid packet collisions in the wireless medium, optimize performance and provide real-time guarantees. Figure D.1 depicts the operation of V-FTT protocol, in which time is divided into periodic Elementary Cycles (ECs) of 50 ms duration. Each EC comprises three different phases. It starts with the Infrastructure Window, where the RSUs covering a certain road segment, transmit the scheduling information (trigger messages) to the OBU nodes, as well as warning messages regarding hazard events. There could be a single RSU covering that particular radio area or the radio ranges of multiple RSUs may partially overlap, which increases system redundancy. Then there is contention-based phase, named Free Period, where nodes non-compliant with the V-FTT protocol can communicate. At the end of the EC, OBUs use the assigned time slots to send vehicle's information (e.g. location, speed, accident) - Synchronous OBU Window. Both the Infrastructure Window and the Synchronous OBU Window are contention-free periods based on a TDMA scheme, in which nodes perform time-triggered transmissions equally spaced by short inter-frame space durations.

D.2.2 Time-Triggered Transmission Mode

The implementation of the time-triggered transmission mode is only possible due to a tight synchronization at the lower layers of the protocol stack, provided by the GPS receivers available in all vehicular nodes. However, some modifications are required at the MAC layer in order to allow this non-standard behaviour [11]. For instance, the CSMA/CA mechanism needs to be disabled and transmission timestamps must be included in the buffers used to

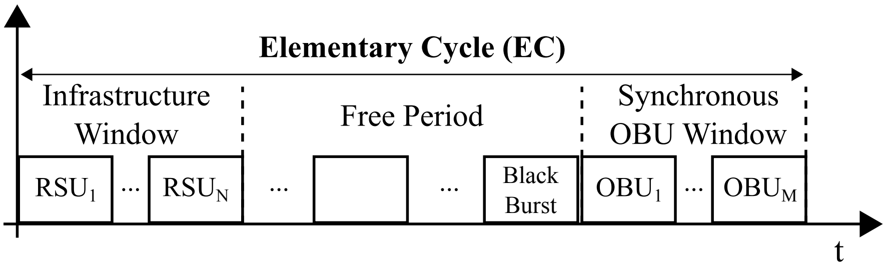


Figure D.1: V-FTT protocol (adapted from [10]).

store packets before transmission. These mechanisms have successfully been developed in a custom and flexible vehicular communications system, named IT2S platform [12].

In the time-triggered transmission mode, the packet is sent to the channel at a predefined time instant regardless the state of the wireless medium, i.e. even if there is an ongoing transmission in the same channel. This way, it is possible to implement the bandjacking technique described in [10], which guarantees that the channel is not occupied at the exact moment the contention-free period begins. For that purpose, a black burst frame is transmitted, keeping the channel busy prior to the beginning of the Synchronous OBU Window, as shown in figure D.1. Then, one just needs to employ a short inter-frame space value between the subsequent transmissions, in order to ensure that non-compliant nodes perceive the channel as busy until the beginning of the next Free Period.

D.2.3 Violating the Standard Inter-Frame Space

An important property of V-FTT is the protection it offers against nodes non-compliant with the protocol (*alien* nodes), either acting according to the standard or other alternative protocols, such as the ones proposed in [3] and [13]. This property is attained by employing an inter-frame space (IFS) value small enough to guarantee that all *alien* nodes have no opportunity to transmit during the whole contention-free period. Assuming that all *alien* nodes follow the Distributed Coordination Function (DCF) of IEEE 802.11 [2], then they are all ruled by the CSMA/CA method. In this scheme and according to the standard, the minimum IFS value for broadcast transmissions is equal to 58 μs, corresponding to the case when the random backoff period is equal to zero. This value is named Distributed (coordination function) Inter-Frame Space (DIFS) and its derived from the parameters presented in equation D.1 for OFDM signals with 10 MHz channel bandwidth (the ones defined for vehicular communications use in the 5.9 GHz frequency band).

$$\begin{aligned} &DIFS = aSIFSTime + 2 \times aSlotTime = \\ &32\mu s + 2 \times 13\mu s = 58\mu s \end{aligned} \tag{D.1}$$

In this equation, *aSIFSTime* (from Short Inter-Frame Space) represents the time that a IEEE 802.11 station has to respond with an acknowledgement frame to a polling by the special channel access method named Point Coordinating Function (PCF). Since V-FTT does not make use of these polling frames, no station will answer within this short IFS. The other parameter - *aSlotTime* - corresponds to the duration of a backoff slot, which is basically the time needed for the Clear Channel Assessment (CCA) mechanism to sense the medium, determine whether the channel is busy or idle and if it is the case to change from receiving to transmitting mode. As a consequence, in order to violate the standard IFS and make sure that no *alien* node will get access to the channel, an IFS value lower than or equal to the one given by equation D.2 should be utilized. This way, if an *alien* node is intended to transmit immediately after the DIFS value, it will have enough time (*aSlotTime*) to sense the wireless medium and to find it already occupied by a V-FTT node.

$$\begin{aligned} &IFS \leq DIFS - aSlotTime = \\ &aSIFSTime + 2 \times aSlotTime - aSlotTime = \\ &aSIFSTime + aSlotTime = 32\mu s + 13\mu s = 45\mu s \end{aligned} \tag{D.2}$$

This value (45 μs) is exactly equal to the one used by the PCF method, with the same goal of guaranteeing a contention-free interval. In that case, the value is named Point (coordination function) Inter-Frame Space (PIFS). In V-FTT protocol, since all messages transmitted during the contention-free period follow a time-triggered approach without sensing the wireless medium, it is possible to strongly reduce this IFS value. Experimental results have shown that the IFS can be shortened up to 17 μs [10], however a safe margin must be given and typically an IFS value of 20 μs is employed in the operation of V-FTT protocol.

D.3 Dependable Network Architecture

D.3.1 Fault-Tolerant Infrastructure-based Vehicular Network

As already explained in section D.1, safety-critical systems such as vehicular networks require a high degree of determinism and dependability. Thus, the different parts of the network should provide reliable service even in the presence of faults. With that goal in mind, a fault-tolerant architecture has been proposed [5], as presented in figure D.2. This dependable framework encompasses three major mechanisms. On the RSU side, a fail silence enforcement entity ensures that the node can only fail by not sending any message to the network [14]. This avoids incorrect messages or packets transmitted out of time. The fail silence mechanism

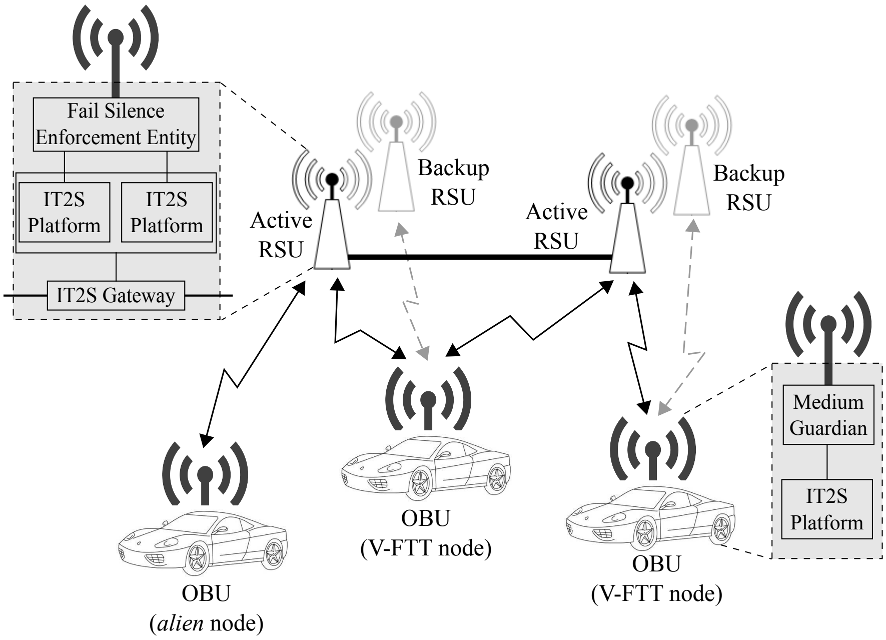


Figure D.2: Fault-tolerant vehicular network architecture [7].

is based on an internal redundancy scheme that compares the messages produced by two IT2S platforms. If there is an agreement both in value and time domains, the message is forwarded to the physical layer for transmission. Otherwise, nothing is send and the RSU node remains silent trying to recover from the failure.

The fail silence failure mode facilitates the design of replication strategies for the nodes of a network. In [7], an RSU replication scheme was proposed in order to increase the reliability of these master units. Since this is the mechanism under analysis in this work, a more detailed description is provided below. On the OBU nodes, medium guardians were devised in order to ensure that slave nodes only transmit during the time slots specifically allocated to them. This way, even if an OBU is faulty, one guarantees that it will not interfere with the messages transmitted by the other vehicles. This medium guardian should belong to a different fault confinement region and must process the scheduling information in an independent way to avoid common mode failures. It should be noticed that these mechanisms, despite targeting the integration with the operation of V-FTT protocol, can be employed in other real-time wireless communications scenarios.

D.3.2 RSU Replication Scheme

The RSU replication scheme proposed in [7] follows an active or state-machine approach [15], where a backup RSU immediately replaces the operation of an active node in case of failure. This active strategy only takes a small fraction of time, in the order of few μs, to identify the failure in the primary RSU and to restore the scheduled activities, i.e. packet transmissions. As a result, this recovery procedure is transparent to the other nodes of the network and avoids any discontinuity of the traffic scheduling in the real-time communications protocol. For this scheme to be effective, the information shared among all RSU replicas need to be consistent and the systems need to be time synchronized, in this case through individual GPS receivers.

The detailed operation of this active replication strategy is as follows. Both the primary and backup replicas are configured to transmit the exact same messages but with a very small time offset (some μs). The packet transmission in the backup RSU is slightly delayed, giving enough time for it to understand if the active node failed or not. If the active RSU fails to transmit the intended message, the backup replica will perceive the wireless medium as free, through its CCA mechanism, and will send the desired packet, replacing the operation of the active node. On the other hand, if the primary RSU is able to transmit the planned message in the predefined instant, the backup will sense the channel as busy, and will deduce that the primary replica is free of error, since the nodes are fail-silent. This way, the road-side infrastructure presents a fault-tolerant behaviour, being all messages still transmitted on time, with just a small delay introduced at the beginning of the packet transmission. This delay can be accommodated by the subsequent IFS, between the current and the next frame, and consequently all the following transmission instants of the remaining RSUs' and OBUs' messages can be kept unchanged.

In order to implement this replication scheme, some additional mechanisms are required at the lower layers of the protocol stack, namely at the MAC sublayer. A new transmission mode was developed that allows the backup replicas to transmit in a time-triggered fashion but only if the channel is free. Otherwise, the packet is discarded and the corresponding memory slot is released. Additionally, it is also necessary to increase the transmission timestamp values of the packets that are stored in the transmission buffer of the backup RSU. From the results presented in [7], one can conclude that a safe replica offset value that still minimizes the delay introduced by this recovery procedure, is equal to 25 μs.

D.4 Timing Analysis of the Replication Scheme

In this work, a detailed analysis is performed regarding the timing behaviour of V-FTT protocol in the presence of the active replication scheme previously described. More exactly, an evaluation is presented with respect to the possible impacts on the real-time guarantees provided by the deterministic vehicular communications protocol. As already mentioned, in case of failure in the primary RSU, a small delay is introduced at the beginning of the packet transmission. Therefore, it is necessary to assess if this delay has some impact in the scheduling of the time-triggered messages or in the properties of the real-time protocol, namely the protection it offers against transmissions from *alien* nodes.

Essentially, there are two distinct scenarios that need to be carefully analysed. The first scenario is the case where there is a single RSU communicating with the vehicles inside its coverage area, which means that inside each EC, there is only one message transmitted by an RSU. Therefore, there can be only one primary RSU replica failing, leading to a simple situation where the RSU transmission, either from the primary or from the backup, only has impact on the previous and subsequent IFS durations. The second scenario occurs when there are multiple RSUs communicating with the same vehicles, i.e. their radio coverage areas are partially overlapped, as envisaged by V-FTT protocol for more critical road segments (e.g. blackspots). In this situation, if all RSUs are replicated, a combination of different conditions will define the IFS values, depending on which RSUs have failed.

In this analysis, it is assumed that the default IFS value (named $shortIFS$) used in the operation of V-FTT protocol without replication is equal to 20 μs and that the backup replica offset ($replicaOffset$) is equivalent to 25 μs. These values follow from the discussion above and are based on the results presented in previous works [10] [7].

D.4.1 Single RSU Scenario

In the scenario with a single RSU, there are two resulting IFS values that must be analysed. One is the IFS duration before the RSU transmission ($IFS_{precedent}$), either from the primary or from the backup replica transmissions, while the other is the IFS value after the RSU transmission ($IFS_{subsequent}$). When the system is operating without failures and the primary RSU is transmitting the packets, the wireless channel is occupied according to the time diagram depicted in figure D.3. In this case, the $IFS_{precedent}$ is equal to the $shortIFS$ (20 μs), since there is no delay at the beginning of the RSU transmission, and the $IFS_{subsequent}$ is derived from the sum of the $replicaOffset$ value, since the backup replica did not transmit, plus the $shortIFS$ previous to the next frame. These results are summarized in equation D.3.

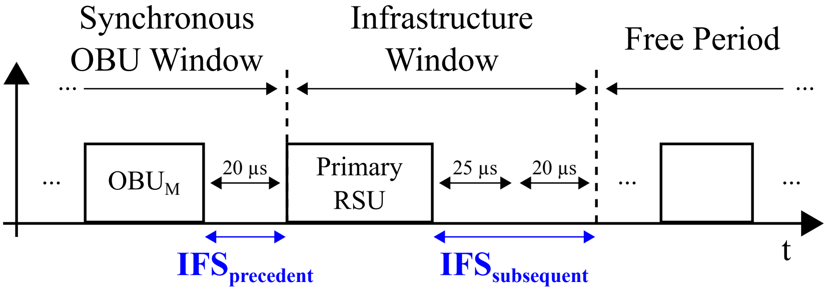


Figure D.3: Time diagram of the primary transmission for the single RSU scenario.

$$\begin{aligned} &IFS_{precedent} = shortIFS = 20\mu s \\ &IFS_{subsequent} = replicaOffset + shortIFS = \\ &25\mu s + 20\mu s = 45\mu s \end{aligned} \tag{D.3}$$

On the other hand, if the primary replica fails and the backup needs to come into the foreground to transmit the planned packet, the time occupancy of the medium is as depicted in figure D.4. In this situation, the value of $IFS_{precedent}$ is equal to the $shortIFS$ duration plus the $replicaOffset$, due to the failure in the active node and the corresponding delay introduced by the recovery procedure. Regarding the $IFS_{subsequent}$, its value corresponds solely to the $shortIFS$ previous to the next Free Period, since the backup RSU transmission ends closer to the end of the Infrastructure Window, when compared to the case of figure D.3. The resulting values are expressed in equation D.4 and as expected, they are opposite to the ones obtained in equation D.3.

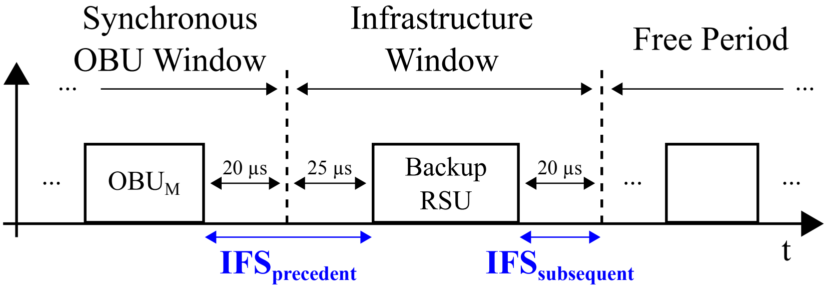


Figure D.4: Time diagram of the backup transmission for the single RSU scenario.

$$\begin{aligned} &IFS_{precedent} = shortIFS + replicaOffset = 45\mu s \\ &IFS_{subsequent} = shortIFS = 20\mu s \end{aligned} \tag{D.4}$$

D.4.2 The Case of Multiple RSUs

In the scenario with multiples RSUs, the analysis is a little more complex, however it can be reduced to the case of only two RSUs covering an overlapped radio area, since the results are identical to the situation with three or more units. In this case, there are three IFS values of interest. Besides the IFS duration between the end of the previous EC and the beginning of RSUs' transmissions ($IFS_{precedent}$) and between the end of RSUs' transmissions and the next Free Period ($IFS_{subsequent}$), it is also important to analyse the IFS value between consecutive RSU messages (IFS_{middle}).

Starting with the example in which all primary RSUs are working properly and the system is free of errors, figure D.5 depicts he time diagram that includes the transmissions of both the primary RSU_1 and the primary RSU_2. This situation is similar to the one presented in figure D.3 for the single RSU scenario. In this case, the $IFS_{precedent}$ remains the same (equal to $shortIFS$) and the IFS_{middle} and $IFS_{subsequent}$ are equivalent to the sum of the $shortIFS$ plus the $replicaOffset$ value. These results are summarized in equation D.5.

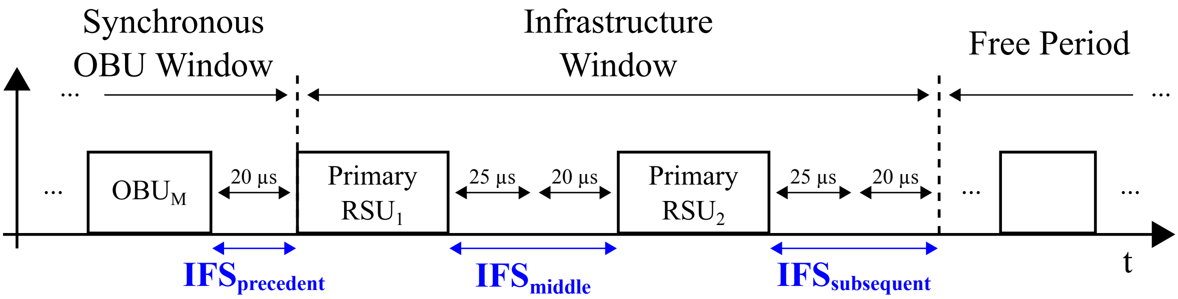


Figure D.5: Time diagram of the primary RSU_1 + primary RSU_2 transmissions for the multiple RSUs scenario.

$$\begin{aligned}
IFS_{precedent} &= shortIFS = 20\mu s \\
IFS_{middle} &= shortIFS + replicaOffset = 45\mu s \\
IFS_{subsequent} &= shortIFS + replicaOffset = 45\mu s
\end{aligned} \tag{D.5}$$

Now, let's consider the case where the primary RSU_1 is transmitting but in RSU_2, the active node has failed and the messages are being sent by the backup unit (figure D.6). Under these circumstances, the IFS_{middle} duration assumes its maximum value, since it is the result of summing two $replicaOffset$ values plus one $shortIFS$ (equation D.6).

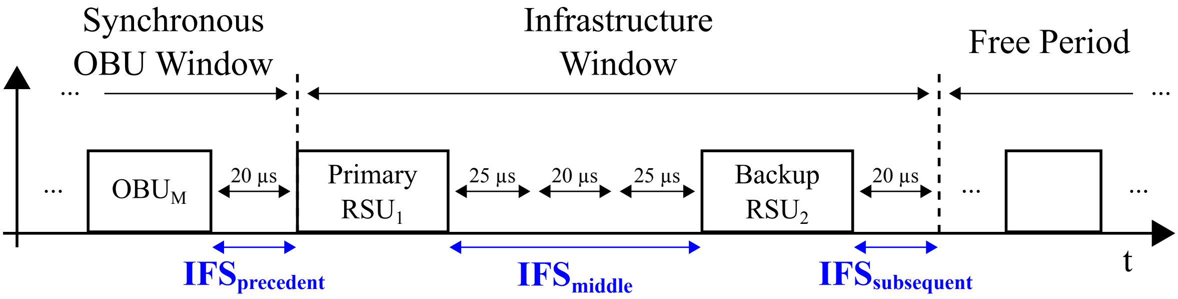


Figure D.6: Time diagram of the primary RSU_1 + backup RSU_2 transmissions for the multiple RSUs scenario.

$$
\begin{aligned}
&IFS_{precedent} = shortIFS = 20\mu s \\
&IFS_{middle} = shortIFS + 2 \times replicaOffset = \\
&20\mu s + 2 \times 25\mu s = 70\mu s \\
&IFS_{subsequent} = shortIFS = 20\mu s
\end{aligned}
\tag{D.6}
$$

Figure D.7 illustrates the scenario in which the primary RSU$_1$ has failed and thus the backup RSU$_1$ is transmitting together with primary RSU$_2$. The IFS_{middle} duration is the shortest possible, being equal to the $shortIFS$ value, as presented in equation D.7.

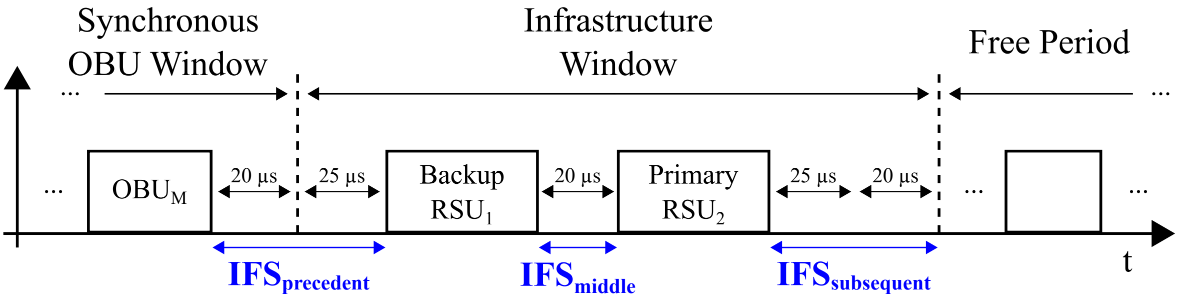


Figure D.7: Time diagram of the backup RSU$_1$ + primary RSU$_2$ transmissions for the multiple RSUs scenario.

$$
\begin{aligned}
&IFS_{precedent} = shortIFS + replicaOffset = 45\mu s \\
&IFS_{middle} = shortIFS = 20\mu s \\
&IFS_{subsequent} = shortIFS + replicaOffset = 45\mu s
\end{aligned}
\tag{D.7}
$$

Finally and despite being a very unlikely situation, it can also happen that both primary nodes fail. The resulting diagram is similar to the one presented in figure D.4 for the single RSU operation. In this case, both backup RSUs are sending the protocol messages as shown in figure D.8. The resulting IFS values are computed in equation D.8.

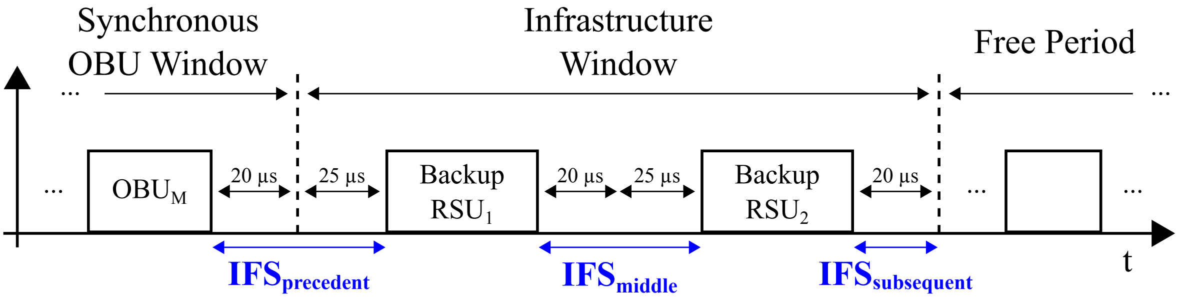


Figure D.8: Time diagram of the backup RSU$_1$ + backup RSU$_2$ transmissions for the multiple RSUs scenario.

$$\begin{aligned}
IFS_{precedent} &= shortIFS + replicaOffset = 45\mu s \\
IFS_{middle} &= shortIFS + replicaOffset = 45\mu s \\
IFS_{subsequent} &= shortIFS = 20\mu s
\end{aligned} \tag{D.8}$$

D.5 Discussion and Possible Solutions

From the previous analysis, one can conclude that the proposed replication scheme provides a low-delay recovery procedure for the RSUs of a vehicular network. When a primary replica fails, the backup one replaces its operation within a small time interval. This duration depends on the scenario (single or multiple RSUs) and on the combination of which specific RSUs have failed, as summarized in table D.1. The delay introduced by the active replication scheme can be easily accommodated in the operation of the real-time protocol, by including these specific IFS values in the RSUs' packet transmissions. This way, the scheduling is not affected, being only required to slightly enlarge the duration of the Infrastructure Window. The resulting overhead when compared to the case with no replication (with regular IFS values equal to $shortIFS = 20\mu s$), can be considered as negligible.

However, there is an important feature of V-FTT protocol that can be compromised by directly employing this replication scheme. In section D.2, it was shown that, in order to protect real-time communications against nodes non-compliant with the deterministic protocol, the maximum IFS value should be lower or equal to 45 μs. As it can observed in table D.1, this is not a problem for the single RSU scenario in which the largest duration is equivalent to 45 μs, but for a specific case involving multiple RSUs, the total IFS_{middle} value is equal to 70 μs, becoming larger than the limit of 45 μs. This situation occurs when the primary RSU$_1$ is working properly and the backup RSU$_2$ has replaced the operation of the primary replica.

		$IFS_{precedent}$	IFS_{middle}	$IFS_{subsequent}$	Violation of standard IFS?
Single RSU	Primary RSU	20 μs	-	45 μs	Yes
	Backup RSU	45 μs	-	20 μs	Yes
Multiple RSUs	Primary RSU_1 + Primary RSU_2	20 μs	45 μs	45 μs	Yes
	Primary RSU_1 + Backup RSU_2	20 μs	70 μs	20 μs	No
	Backup RSU_1 + Primary RSU_2	45 μs	20 μs	45 μs	Yes
	Backup RSU_1 + Backup RSU_2	45 μs	45 μs	20 μs	Yes

Table D.1: Timing Analysis of the Active Replication Scheme.

As a result, the deterministic protocol can not violate the standard IFS value under these specific circumstances, and therefore an *alien* node has a small but existing window of opportunity to interfere with the real-time operation of the vehicular network. This problem can only be avoided if the different RSUs' transmissions are not consecutive. One of the possible solutions is to interleave the Infrastructure Window with the Synchronous OBU Window, allowing the distinct RSUs' messages to be distributed along the OBUs' packets. This way, there would be no consecutive RSUs' transmissions, since at least one OBU's message would be sent in between. Nevertheless, this strategy has some drawbacks, since the size of the Synchronous OBU Window is very dynamic and at a certain moment, there could be not enough number of OBUs in radio range to separate the RSUs' packets.

Another possibility is to reutilize the bandjacking mechanism previously described in section D.2, to transmit a black burst with the smallest duration available before each RSU transmission. In this situation, the RSUs' packets would be equally spaced by small frames transmitted always at predefined instants and independently of replica failures. In order to guarantee this condition, these black burst frames could be transmitted simultaneously by all RSUs and by all the replicas. However again, there are some disadvantages, e.g. the overhead introduced by all these black burst transmissions. This overhead strongly depends on which layer the bandjacking mechanism is implemented. For instance, if these black bursts are requested at the MAC layer, the minimum frame duration is obtained from the transmission of a single byte packet at the maximum rate (64-QAM with coding rate 3/4), which is equal to 48 μs. Alternatively, if this mechanism is developed at the physical layer, it is possible to generate a signal to occupy the wireless medium for a even shorter period of time (the minimum value being determined by the *aSlotTime* duration, which is equal to 13 μs).

D.6 Conclusions

In this paper, a timing analysis was performed regarding the operation of an RSU replication scheme for infrastructure-based vehicular networks. The obtained results have shown that the recovery procedure has low-latency, but still can have some impact in the real-time properties of the deterministic communications protocol. For the case of multiple RSUs with overlapping radio coverage areas and under certain circumstances, the IFS value can be greater than the maximum required to guarantee protection against nodes non-compliant with the protocol. Some possible solutions are briefly discussed in this work and further research is necessary to evaluate the best strategy to solve this problem.

Acknowledgements

This work is funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia under the PhD scholarship ref. SFRH/BD/52591/2014 and the project PEst-OE/EEI/LA0008/2013.

References

[1] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks", *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun. 2008, ISSN: 0163-6804. DOI: 10.1109/MCOM.2008.4539481.

[2] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, Mar. 2012.

[3] K. Bilstrup, E. Uhlemann, E. Ström, and U. Bilstrup, "On the Ability of the 802.11p MAC Method and STDMA to Support Real-Time Vehicle-to-Vehicle Communication", *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–13, 2009, ISSN: 1687-1499. DOI: 10.1155/2009/902414. [Online]. Available: http://dx.doi.org/10.1155/2009/902414.

[4] T. Meireles, J. Fonseca, and J. Ferreira, "The Case for Wireless Vehicular Communications Supported by Roadside Infrastructure", in *Intelligent Transportation Systems Technologies and Applications*, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, Eds., John Wiley & Sons, Ltd, 2015, pp. 57–82, ISBN: 9781118894774. DOI: 10.1002/9781118894774.ch4. [Online]. Available: http://dx.doi.org/10.1002/9781118894774.ch4.

[5] J. Almeida, J. Ferreira, and A. S. R. Oliveira, "Fault Tolerant Architecture for Infrastructure based Vehicular Networks", in *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira, and J. Fonseca, Eds., Cham: Springer International Publishing, 2016, ch. 8, pp. 169–194, ISBN: 978-3-319-28183-4. DOI: 10.1007/978-3-319-28183-4_8.

[6] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz, "Inter-vehicle communication: Quo vadis", *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 170–177, Jun. 2014, ISSN: 0163-6804. DOI: 10.1109/MCOM.2014.6829960.

[7] J. Almeida, J. Ferreira, and A. S. R. Oliveira, "An RSU Replication Scheme for Dependable Wireless Vehicular Networks", in *2016 12th European Dependable Computing Conference (EDCC)*, Sep. 2016, pp. 229–240. DOI: 10.1109/EDCC.2016.11.

[8] L. M. Pinho and F. Vasques, "Timing analysis of reliable real-time communication in CAN networks", in *Real-Time Systems, 13th Euromicro Conference on, 2001.*, 2001, pp. 103–114. DOI: 10.1109/EMRTS.2001.934010.

[9] G. Cena, S. Scanzio, L. Seno, A. Valenzano, and C. Zunino, "Combining reliability and timeliness in industrial wireless networks: An experimental assessment", in *2016 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2016, pp. 1–4. DOI: 10.1109/WFCS.2016.7496505.

[10] A. Khan, J. Almeida, B. Fernandes, M. Alam, P. Pedreiras, and J. Ferreira, “Towards Reliable Wireless Vehicular Communications”, in *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, Sep. 2015, pp. 167–172. DOI: 10.1109/ITSC.2015.36.

[11] C. Cruz, J. Ferreira, and A. Oliveira, “Supporting Deterministic Medium Access Control in Wireless Vehicular Communications”, in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*, Sep. 2015. DOI: 10.1109/VTCFall.2015.7391160.

[12] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Development of an ITS-G5 station, from the physical to the MAC layer”, in *Intelligent Transport Systems: from Good Practice to Standards*, P. Pagano, Ed., CRC Press, Taylor and Francis Group, 2016, ch. 1, pp. 1–37. DOI: 10.1201/9781315370866-2.

[13] R. Scopigno and H. A. Cozzetti, “Mobile Slotted Aloha for Vanets”, in *Vehicular Technology Conference (VTC 2009 Fall), 2009 IEEE 70th*, Sep. 2009, pp. 1–5. DOI: 10.1109/VETECF.2009.5378792.

[14] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Fail Silence Mechanism for Dependable Vehicular Communications”, *International Journal of High Performance Computing and Networking (IJHPCN)*, vol. 10, no. 6, pp. 534–545, 2017. DOI: 10.1504/IJHPCN.2017.10008241.

[15] F. B. Schneider, “Implementing Fault-tolerant Services Using the State Machine Approach: A Tutorial”, *ACM Computing Surveys*, vol. 22, no. 4, pp. 299–319, Dec. 1990.

Paper E

A Medium Guardian for Enhanced Dependability in Safety-Critical Wireless Systems

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

in ***IEEE Transactions on Intelligent Transportation Systems***, **vol. 19, no. 3, pp. 965-976, 2018**

The format has been revised.

A Medium Guardian for Enhanced Dependability in Safety-Critical Wireless Systems

João Almeida, Joaquim Ferreira and Arnaldo S. R. Oliveira

Abstract

According to the recent perspectives for the next generation of mobile networks (5G), future wireless communications will be able to support the operation of safety-critical systems, such as remote surgery or vehicle platooning. For that purpose, high reliability and availability values ($> 99.999\%$) as well as low end-to-end delay (< 1 ms) are included in the requirements specification. In order to achieve these goals, novel solutions will need to be introduced both at the communications devices and at the network protocols. Fault tolerance mechanisms are good candidates to attain such dependability attributes. In this paper, a medium guardian concept is proposed to guarantee fail-silent behaviour, both in time and value domains, for the nodes of a wireless network. After a generic description of the wireless medium guardian concept, its application to the case of ETSI ITS-G5 based vehicular communications is demonstrated. In this way, the design and practical implementation of a medium guardian for real-time vehicular communications is reported, together with the experimental evaluation of this first prototype. The obtained results demonstrate the low latency of the fault detection mechanism and the effectiveness of the guardian in preventing error propagation to other nodes of the network.

E.1 Introduction

The forthcoming fifth generation (5G) of mobile communications systems will bring disruptive changes to a variety of different markets and fields of human activity. The novel wireless technologies and network architectures will certainly have an impact on future industrial automation, health care, transportation systems, grid management, agriculture, among many others. These various application domains pose distinct requirements namely in terms of throughput, latency, number of connected devices or energy efficiency [1] [2]. The Internet of Things (IoT), in which billions of devices are expected to be connected to the Internet, will play a crucial role in this next generation of mobile networks, since the demands for low power consumption and large number of links will give origin to new radio units, communications protocols and network infrastructures. However, the most challenging requirements probably arise from the services involving real-time interaction with a remote or surrounding environment, frequently described as the Tactile Internet concept [3]. This real-time cyber-physical control involves extremely low latencies, with end-to-end delays lower than 1 millisecond, and high levels of availability, reliability and security. Some of these applications are related to safety-critical systems, such as telesurgery, cooperative driverless vehicles or industrial robotics. In such scenarios, a failure in the wireless communications sub-system may lead to catastrophic consequences in the operating environment.

For the case of cooperative automotive intelligent transport systems (ITS), dependable wireless vehicular communications will improve road safety, transportation efficiency and passenger comfort. Cooperative applications running in clusters of vehicles, in some cases with the support of roadside infrastructures, expand drivers' situational awareness from a few meters to some hundred meters, disseminating warnings to the drivers, and may even support closed-loop automatic control of the vehicles, e.g., platooning or intersection control. Despite their obvious benefits, these safety ITS applications pose a difficult challenge to the communications layer of the system, since it is necessary to guarantee that all nodes respect the communications policy and do not interfere with the remaining transmissions taking place in the wireless channel.

In order to attain the strict reliability and availability requirements ($> 99.999\%$), while maintaining low latency values, innovative mechanisms will need to be developed, both at the node and at the network level. These solutions will need to tackle several sources of faults in wireless networks, like, for instance, changing channel conditions [4], spectrum interference, security attacks [5] or dynamic network topologies. Fault-tolerant mechanisms are traditionally used to prevent the occurrence of failures in real-time distributed systems [6] [7], being employed in various wired LAN and fieldbus technologies, such as CAN, Flexray or Ethernet. Similar techniques can be applied in future wireless systems and there is already some work focusing on the provision of redundant links for 5G networks [8] [9], thus allowing fast recovery in case of failure. However, such strategies assume that when a node fails, it presents a fail-silent behaviour, i.e. the node permanently stops emitting any signal to the wireless channel. In certain situations, that may not be the case and several types of faults could arise either from the software component of the node or from the digital or analogue hardware parts. For example, the analogue components of wireless transceivers represent a critical source of faults that may lead only to partial degradation of the radio performance [10]. Under these circumstances, the operation of the network communications protocol can be unpredictable, causing large delay values and low reliability in packet transmission, i.e. high number of messages not correctly received.

In this work, the medium guardian concept is proposed with the aim of providing fail-silent behaviour to the nodes of a wireless network. This idea was briefly presented in [11] and consists in the adaptation of the bus guardian concept to wireless communications systems. The bus guardian is a behavioural error detection technique commonly used to provide fail-silence operation in fieldbuses technologies. In the case of the wireless domain, a faulty node whose operation is being monitored by a medium guardian, will not interfere with the remaining communications taking place in the medium. After describing the operation of a generic medium guardian, this paper demonstrates its application in the ITS context, providing a practical implementation to the use case scenario of real-time vehicular communications. This mechanism is part of a broader strategy targeting the design of a fault-tolerant architecture to improve the dependability attributes of wireless vehicular networks [12].

This work contributes to advance the state-of-the-art in fault-tolerant wireless communications by introducing a new concept, the medium guardian, that is capable of guaranteeing fail-silence behaviour to the nodes of a network. As a use case scenario, the medium guardian is designed and validated for vehicular networks, a field of ITS that poses hard real-time and dependability requirements. The rest of the paper is organized as follows. Section E.2 presents a brief overview of the different contributions and proposed architectures for bus guardians. Then, in section E.3 the medium guardian concept is generically described, while section E.4 details the design and implementation of a medium guardian device for wireless vehicular communications. Section E.5 reports the experimental tests together with the obtained results. Finally, section E.6 summarizes the conclusions and future work.

E.2 Related Work

As stated before, a malicious or malfunctioning node may compromise the operation of an entire safety-critical system. Therefore, it is necessary to devise a fail-safe strategy that prevents a fault occurring in a node to propagate to the rest of the network. In cabled networks, this is typically achieved by guaranteeing that all nodes exhibit a single type of failure: the fail silent failure mode. In this mode, the results produced by one node, when observed by the remaining units, are always correct or are simply not delivered. A node can be fail-silent in the value domain only, i.e. all generated messages contain valid values, in the time domain only, i.e. packets are transmitted just at the right instants, or in both of them. With fail-silent behaviour and assuming that omissions are properly handled, a fault inside a node cannot affect others and thus each node becomes a different fault confinement region. Generically, there are two main groups of techniques used to enforce fail-silent behaviour: the ones based on adding redundancy and the ones that rely on behavioural error detection techniques. The first set of methods is typically more expensive, given the fact that resource replication is employed. Behavioural error detection mechanisms are usually cheaper but may lead to an higher error detection latency. Bus guardians belong to this class of mechanisms and they act as failure mode converters, i.e. the failure modes of the node are replaced by the failure modes of the guardian. In order to be effective, the operation of the guardian must reside in a distinct fault containment region (e.g. separate clock, hardware, power supply, etc.), so it can fail independently from the node it monitors. However, a trade-off is usually made between fault coverage, the final cost of the system and the probability of common mode failures.

The bus guardian concept was first introduced in the architecture of a fault-tolerant multiprocessor for aircraft (FTMP) [13], in which guardian units are described as independent devices responsible for governing the status of their associated modules (e.g. processor, memory and I/O access unit). In this context, each bus guardian is able to receive commands instructing the isolation and the switch of the corresponding malfunctioning module to a silent state. To achieve an even higher level of reliability, redundant guardians can be employed in each component and the decisions of establishing power-on state and enabling bus transmissions are only taken after reaching agreement among all guardians. In [14], bus guardians are utilized to protect a time-triggered communication system from the babbling idiot failure mode, which occurs when a faulty node of a distributed system sends unsolicited messages at arbitrary points in time without respecting the medium access rules. For that purpose, each node of the network is equipped with a bus guardian holding a-priori knowledge of the TDMA scheduling established during design time. If a guardian detects a temporal violation in the predefined time slot allocation, it will automatic and permanently disable the transmission path of the node. The same strategy can be adapted to prevent babbling idiot failures in event-triggered communications, as suggested in [15]. In this case, messages are transmitted at arbitrary points in time, which makes more difficult the fault detection task and the design of the guardian. Nevertheless, the effect of undetected faults can be bounded to a small value, as long as the guardian is configured with the minimum inter-arrival time required between the transmission of two consecutive messages by the node being monitored. Consequently, by including this worst case response time in the analysis of the system, one can prevent timing failures caused by babbling idiot units.

In order to enable flexibility in more dynamic networks, the bus guardian configuration parameters, such as time slot allocation or inter-arrival time, can be updated during run-time and possibly every communications cycle [16]. This is not the case for static scheduling techniques where these parameters are established during the protocol design phase or eventually during network startup. Another aspect is related with the distinct architectures available for implementing a bus guardian based on the level of independence from the node it is monitoring [15] (Fig. E.1). The closely or tightly coupled guardian usually achieves the smallest error detection latency, while the independent guardian can provide complete isolation from the node. A compromise between these two solutions can be attained with a loosely coupled guardian, where transmissions are only allowed under the control of the guardian.

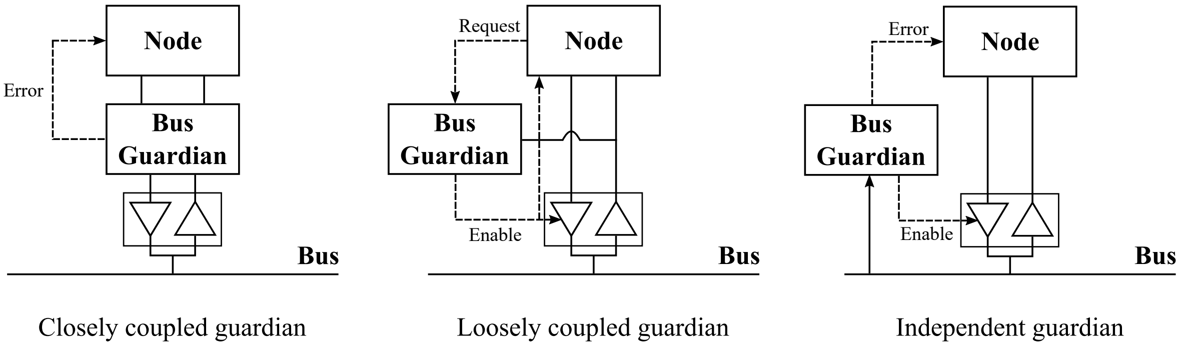


Figure E.1: Possible bus guardian architectures (adapted from [15]).

If the network can be organized in a star topology, the individual guardians governing each node can be replaced by a single central guardian per network channel [17]. In this scenario, the use of an independent guardian architecture brings clear advantages.

E.3 The Medium Guardian Concept

The key idea of this work is to adapt the bus guardian concept to wireless communications systems. As in wired networks, the main goal is to protect the shared medium from faults arising in a node, thus creating distinct fault containment regions. In order to govern the operation of each wireless node, a special device called medium guardian is associated to that unit, being responsible for monitoring the information transmitted to the wireless medium (Fig. E.2).

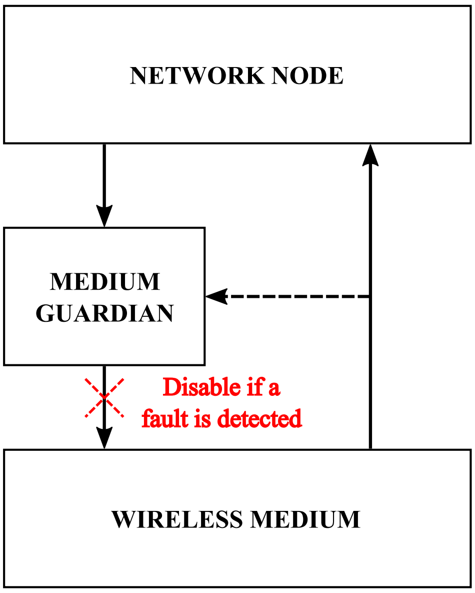


Figure E.2: The medium guardian concept.

E.3.1 Policing Parameters

The medium guardian can be statically configured with the transmission parameters of the node, either defined at design time or acquired during network startup. Another possibility consists in dynamically configuring the guardian by receiving instructions from other nodes of the network, either masters or peers. Let's consider for example a single-master, multiple-slave architecture, in which the master node periodically disseminates the TDMA scheduling for the slave units. In this case, the guardian must be able to decode the time slot allocated to the node under its supervision and only authorize a transmission inside the corresponding time window. Eventually, these configuration parameters could also be autonomously derived by the guardian from the state of the network, as it happens in self organizing networks, e.g. the ones based on the self-organizing time division multiple access (STDMA) protocol [18]. This last approach may be particularly useful for the future networks relying on full-duplex wireless systems [19] or cognitive radio strategies [20]. In these scenarios, the medium guardian should be capable of sensing the wireless medium and understand when the node is allowed to transmit, e.g. by identifying the presence of primary network users within radio range. For the full-duplex case, it may even be necessary to equip the guardian with a full duplex radio, so it can cancel the self-interference signal, thus being able to isolate the messages transmitted by the other nodes.

E.3.2 Monitoring Value, Time and Frequency Domains

Moreover, with the recent protocols and waveforms that are being proposed for the next generation of mobile networks, it becomes evident that a medium guardian may have to validate the operation of the node it is monitoring in three different domains. Besides value and timing aspects, which are traditionally under the supervision of bus guardian devices, the frequency domain becomes extremely important in wireless systems. As a matter of fact, resource allocation both at the channel level and at the different subcarriers inside the same channel, already plays an essential role in current wireless communications and it will have an even more significant impact in future technologies. Opportunistic spectrum access techniques are being developed [21], in order to cope with the large data rate (10 Gb/s) and low latency (< 1 ms) requirements, as well as with the massive number of radio units expected in the next generation of mobile networks. The 5G candidate waveforms, such as Generalized Frequency Division Multiplexing (GFDM) [22] or Non-Contiguous OFDM (NC-OFDM) [23], target flexible and dynamic resource allocation in networks with services and nodes holding distinct communications requirements. Typically these protocols support non-continuous subcarrier allocation, which requires a sensing mechanism able to identify the utilization of each subcarrier individually. Therefore, a medium guardian operating in this type of environments should be also capable to assess channel occupancy in a subcarrier basis and validate node's transmissions accordingly. This could be achieved by plotting the frequency representation of the signal the node is transmitting and verifying its compliance with the medium access rules previously established.

E.3.3 Fault Coverage vs. Error Detection Latency

The validation in the value, time or frequency domains performed by the medium guardian can take place prior to, during or after actual message transmission and can be executed in the digital or analogue worlds. These decisions depend on the fault coverage and error detection latency requirements and have a direct influence on the complexity and architecture of the guardian. For instance, if the medium guardian is monitoring the digital signal produced by the node before digital-to-analogue and radiofrequency (RF) conversion, a small detection latency can be attained. This value could even go to zero, if the behaviour of the node can be slightly modified in order to produce results in advance, so that the message is entirely analysed before start being transmitted. However in this case, the correct operation of the analogue part can not be assured and if one of these components fails, a fault may be propagated to the wireless medium [10]. On the other hand, by examining the output RF signal at the air interface, a medium guardian can completely cover all possible sources of faults in the node, including the analogue components from the DAC up to the antenna. The main drawback of this approach resides in the fact that the contents of the message (value domain) can only be validated after the whole frame has been transmitted to the wireless medium. The reason for this lies in the modern modulation schemes, forward error correction codes and encryption techniques. As a result, the medium guardian would be only able to analyse any message field after receiving and digitally processing the entire packet, thus increasing the total error detection latency. In comparison with the traditional areas of application of bus guardians, this is typically not an issue since in fieldbus protocols it is possible to immediately evaluate the correctness of each individual bit upon arrival.

E.3.4 Security Benefits

From a security perspective, the utilization of medium guardians may be very beneficial since it could possibly protect the rest of the network from malicious attacks occurring in a node. In certain scenarios, it can be desirable to deploy an infrastructure that allows remote access and remote updates of the software version running in its units. In some technologies, this may even include upgrades to the reconfigurable hardware that controls the radio communications systems of the nodes. Let's consider that a hacker gains access to one of these nodes and succeeds at modifying its transmission behaviour with the main goal of corrupting communications taking place in the wireless medium. In this case, a well-designed guardian can prevent this attack from being successful. This can be attained by designing the medium guardian as a completely independent device with the ability to permanently shutdown the operation of the node it is attached to, e.g. by controlling the power supply status of the node. Such guardian should not be remotely accessible, making it impossible for a hacker to modify its *modus operandi*. This way, a medium guardian can detect and protect against malicious faults, securing the correct state of the communications channel.

E.4 Use Case Scenario

After this generic description, the design and application of the medium guardian concept to a specific use case scenario is presented. This first prototype of a medium guardian device was developed in the scope of real-time vehicular networks.

E.4.1 Dependable Vehicular Networks

The essential aim of vehicular communications is to enhance road safety by exchanging information among road users (vehicles, bicycles and pedestrians) and the road-side infrastructure. In order to be effective, vehicular networks must exhibit dependable and real-time properties, so that safety-critical messages can arrive at their destination before the required deadline with deterministic guarantees. A fault-tolerant architecture was proposed in [12] to improve the dependability attributes of infrastructure-based vehicular networks (Fig. E.3). In this framework, the road-side units (RSUs) behave as masters of the network, being responsible for coordinating all communications and admission control policies. Given their central role in the system, some fault-tolerant techniques are employed to overcome the fact that RSUs constitute single point of failures in the network. Firstly, a fail-silence mechanism is introduced in these nodes to ensure that they only send correct messages at the right instants. The method used to provide fail-silent behaviour to the RSU nodes relies on adding redundancy, and comparing the output messages produced by both modules. After that, an active replication scheme is included to allow a low-latency recovery of faulty RSUs. Thus, when an active RSU silently fails, it is automatically and almost instantaneously replaced by a backup one [24]. The same strategy could have been followed to attain fail-silent behaviour in the on-board units (OBUs) placed inside the cars. However, for these nodes a less expensive solution should be considered and therefore, the inclusion of a medium guardian in each OBU is proposed, being the focus

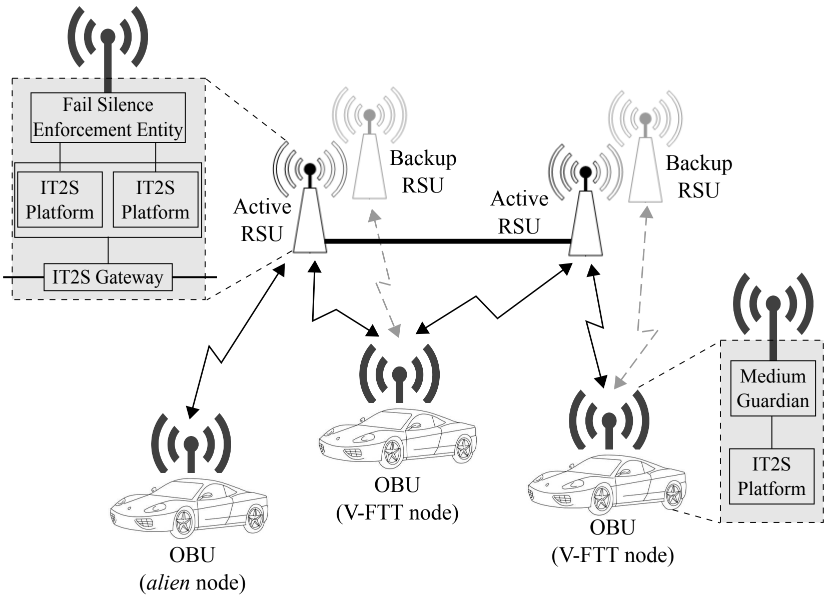


Figure E.3: Fault-tolerance mechanisms in V-FTT network (adapted from [12]).

of this work.

A deterministic medium access scheme, named Vehicular Flexible Time-Triggered (V-FTT) [25], is used to provide real-time behaviour to the nodes of the network. This protocol is based on spatial Time Division Multiple Access (TDMA), with slot reuse along the road. In this scenario (Fig. E.4), the RSUs periodically broadcast scheduling messages with the slot allocation for every Elementary Cycle (EC). Then, after a free period for asynchronous traffic, the OBUs transmit their frames in the time slots assigned to each one of them. The utilization of a medium guardian in this context can be extremely useful, since it can validate the OBUs' transmissions and prevent them from occupying the wireless medium outside the allocated time intervals. The typical EC duration is 100 ms, in order to match the maximum refresh rate (10 Hz) of Cooperative Awareness Messages (CAM) from ETSI ITS-G5 standards [26].

E.4.2 Principle of Operation

The primary objective of this medium guardian is to guarantee the compliance of the node it is monitoring with the transmission schedule. As a consequence, the validation in the temporal domain is of uttermost importance in this case. Hence, it is possible to avoid the babbling idiot failure and to assure that even a faulty OBU will not interfere with the packets transmitted in the remaining time slots by the other nodes. In vehicular networks, clock synchronization is ensured by requiring that all nodes are equipped with a GPS module. Therefore, the medium guardian must also keep time synchronization using an independent GPS device. Then, by comparing its local time with the time window assigned to the OBU, it could identify a violation of the communications scheduling and consequently disable the transmission interface of the node. The guardian also has the task of verifying the contents of the messages sent by the node, namely the most important fields, such as the frame header containing the node ID or MAC address or other critical information like vehicle's position and speed. This last data related to the localization of the vehicle and its dynamics can also be independently obtained from the GPS module included in the guardian. The verification of node's identification in the frame header is particularly important to prevent masquerading while the validation of GPS data can avoid a malicious node from disseminating erroneous information that may lead to road safety events, due for instance to false location coordinates.

The operating scenario of the medium guardian for real-time vehicular networks is depicted

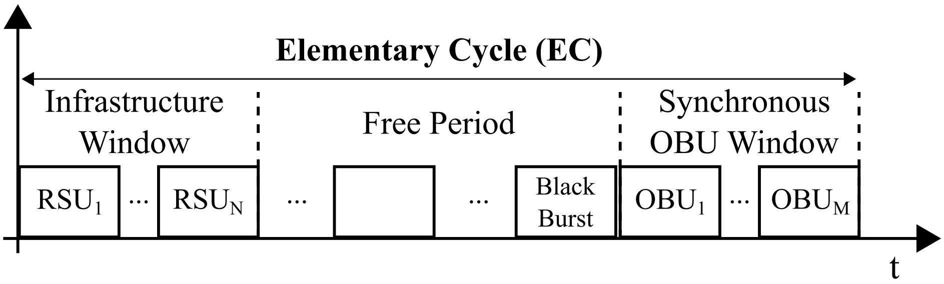


Figure E.4: Elementary Cycle of V-FTT protocol (adapted from [25]).

in Fig. E.5. Both the guardian and the associated OBU receive and process the periodic scheduling messages from the RSU nodes. These messages are transmitted in the control channel (CCH) for vehicular communications in Europe (ITS-G5) with a centre frequency of 5.9 GHz. Given the fact that vehicular communications platforms are dual-radio devices, as required by the European standards, the other radio unit of RSUs and OBUs nodes can be tuned in a service channel (SCH) to exchange infotainment data. From the scheduling messages, both the guardian and the OBU retrieve the slot allocation for the current EC, thus knowing exactly which time slot was assigned to that specific node. Then, when the local clock of the guardian meets the start of the time window corresponding to the granted slot, a control signal - *EnableTransmission* - is enabled through a wired connection to the OBU. This signal corresponds to an output pin of the guardian and is kept in high state until the end of the slot interval. The OBU uses this reference signal to understand if its intent to transmit is taking place at the right moment. If not, it will cancel the transmission and wait for the next opportunity to send a message. Even with the presence of this control signal, the OBU may be able to ignore its information (malicious attacks) or it can happen that faults arise in the analogue part of the transmitter, being unaffected by the control signals in the digital domain. Therefore, an additional signal - *ShutdownOBU* - is required to completely shutdown the transmission interface of the OBU in case of misbehaviour. This signal is activated as soon as the guardian detects a violation of the time window established by the *EnableTransmission* indication. As a result, the operation of the OBU is halted, by disabling the RF module or the whole power supply of the node through a hardwired connection.

In order to cover the maximum number of fault sources possible, the medium guardian was designed based on an independent architecture (Fig. E.1), that is capable of monitoring

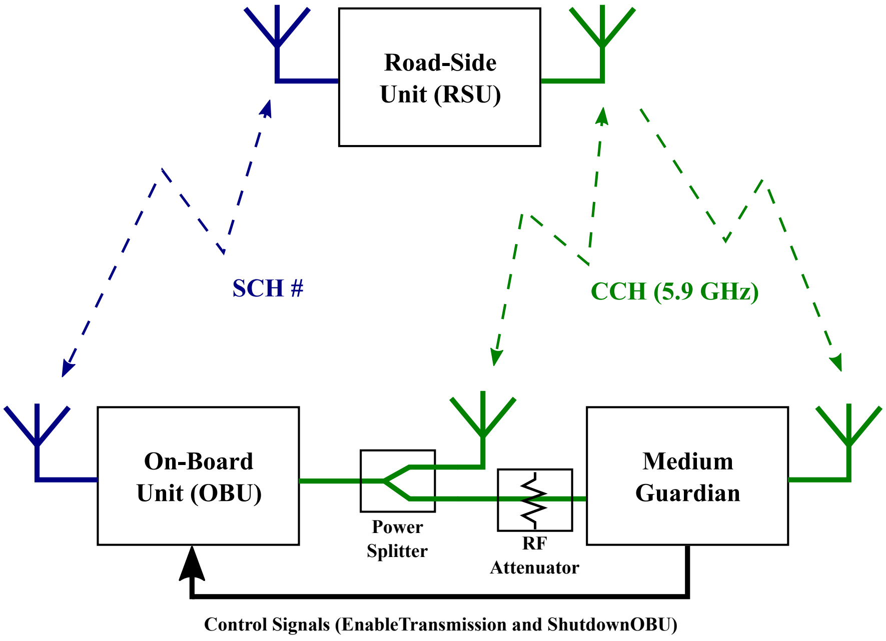


Figure E.5: Medium guardian for real-time vehicular communications.

the RF signal emitted to the wireless medium by the OBU. As it can be observed in Fig. E.5, the OBU signal is divided, by means of a power splitter, into the OBU antenna and the input of the RF front-end in the medium guardian. To prevent the saturation of the guardian's front-end, an RF attenuator of 60 dB is employed, reducing the signal power level. By using this scheme, only the antenna component is excluded from the guardian's validation process. Ideally the OBU antenna should also be included in this analysis, however that is not possible to achieve without allowing the RF signal to be mixed with other transmissions that may occur in the channel. In this architecture, the guardian is also a dual-radio device, being one radio responsible for decoding the RSU scheduling messages and the other focused on the validation of OBU transmissions. Nevertheless, the radio listening to the RSU packets, which is directly connected to the air interface through its antenna, can also capture the wireless signal whenever the OBU is transmitting. Due to possible limitations (e.g. the saturation of the analogue front-end) of such method, this possibility was not incorporated in the initial design of the medium guardian. However, it can be added seamlessly in the future, in order to include the antenna component in the system's fault coverage.

E.4.3 Fault Hypothesis

The fault hypothesis for the developed medium guardian operation comprehends the following types of faults:

- **Node faults** - In the proposed scheme, the medium guardian device belongs to a fault containment region that is assumed independent of the one constituted by the OBU node. The covered faults within each node include hardware faults, both transient and permanent, and software faults. However and as already referred, faults in the OBU antenna are not considered. Byzantine faults are partially covered, since the medium guardian operation can not be reconfigured over the air, making it impossible to modify its behaviour without physical access. Nevertheless, some other types of security attacks may still happen in the case when an adversary node masquerades as an RSU and starts transmitting erroneous scheduling messages. A possible way to prevent this from happening is by including encryption and authentication in the exchanged messages, which would also increase the guardian's complexity.
- **Channel transient faults** - Vehicular communications are regularly affected by transient faults, since the wireless channel conditions may vary a lot, depending on atmospheric and traffic conditions. These effects may cause packet losses that in case of the scheduling messages, would prevent the OBU nodes from transmitting. Even when the OBU correctly receives the communications schedule, if the guardian does not decode the same RSU packet, it will not allow the OBU's transmission. It will also not signal this transmission attempt as a fault, but the node will be prevented from sending its packet. A way to circumvent the higher packet error rate is by introducing time and spatial redundancy in the scheduling dissemination by the RSUs. This can be achieved by deploying a more dense RSU distribution along the road, leading to a partial overlap of the RSUs' radio coverage areas. This way, a single OBU transmission

can be scheduled by a configurable number of adjacent RSUs for the same transmission slot, reducing the risk of missing the communications schedule for a particular EC, both by OBU node and by the medium guardian.

- **Channel permanent faults** - The communications channel constitutes a single point of failure for wireless vehicular networks. Permanent faults may occur due for instance to unregulated interference, which can be considered as a malicious fault. This type of faults are not addressed in this work, but a possible solution may rely in adding redundancy, by detecting the interference signal and changing the operation of the communications protocol to another wireless channel not affected by the same disturbance.
- **Synchrony assumptions** - Time synchronization among RSUs, OBUs and medium guardians is ensured by a GPS receiver located at each one of these units. Typically, the accuracy provided by this system is good enough to meet the requirements of the real-time vehicular communications protocol, but in some specific situations the quality of the GPS signal may drop, e.g. in tunnels or some dense urban scenarios with tall buildings. In these cases, an alternative strategy may be employed, by utilizing the scheduling message transmitted at the beginning of each EC as a synchronization mark. As a result, the RSU nodes would also become time masters, periodically refreshing the time reference (typically 100 ms) to all the other network clocks. In order to provide strict real-time guarantees, this possibility needs to be seriously considered in the development of a real-world implementation of the system, since GPS availability can not be taken for granted and a fall-back mechanism must be readily available in such scenario.

E.4.4 Medium Guardian Architecture

The structural building blocks of the medium guardian are presented in Fig. E.6. It is composed by an FPGA, a GPS module and two radio units, each one with a RF front-end and a Analogue-to-Digital/Digital-to-Analogue (AD/DA) converter. One of the radios is connected to the OBU through an RF cable and attenuator, while the other one is attached to a 5.9 GHz antenna for vehicular communications. A GPS module is utilized to keep time synchronization by means of a high precision signal called Pulse Per Second (PPS). The FPGA is responsible for decoding all the messages received in both radio units and for implementing all the functional logic of the guardian. This logic was translated into digital hardware blocks using standard VHDL language.

The radio connected to the air interface through the RF antenna holds the task of listening to the messages exchanged in the control channel with the aim of receiving the scheduling frames from the RSU nodes. These packets are decoded in the OFDM reception chain (*Rx Chain*) inside the FPGA and are then identified as scheduling messages in the *Time Slot Calculation* block, where the time slot assigned to the associated OBU is extracted. After that, when the GPS clock meets the start of the time window allocated to that node, the *Enable Transmission* block asserts the corresponding output pin to the OBU. This same signal is used to perform the *Time Domain Validation*, by comparing it with the result of

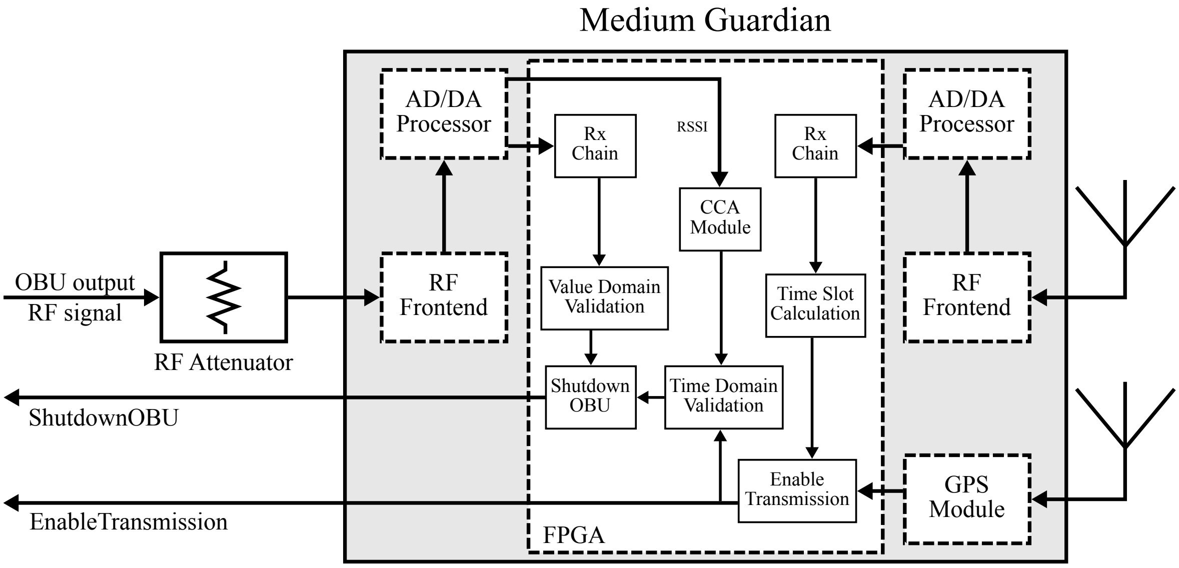


Figure E.6: Structural blocks of the medium guardian device.

the Clear Channel Assessment (*CCA Module*) of the radio directly connected to the OBU. During proper operation, the Received Signal Strength Indication (RSSI) on this radio should only rise above the predefined threshold used to trigger a positive CCA value, when the *EnableTransmission* signal is asserted, meaning that the OBU transmission is taking place within the correct time interval. The packets transmitted by the OBU are decoded by another *Rx Chain* unit, being then analysed in the *Value Domain Validation* block, which verifies some of the message fields. If at least one of the validation blocks (value or time domains) detects a violation in the transmission pattern of the OBU, the *Shutdown OBU* logic block will produce an output signal that will disable the operation of the node.

The OBU should always verify the state of the *EnableTransmission* signal before transmitting, since it may happen that the medium guardian does not correctly receive any scheduling message during a certain Elementary Cycle. Under these circumstances, the *EnableTransmission* pin will not be put in the logic value '1' during the whole EC by the guardian. In that case, the OBU must respect this indication and hold its transmission, even though it has properly decoded the valid scheduling allocation from the RSU nodes. Otherwise, the guardian will consider this packet transmission as a time violation and will halt node's operation, by activating the *ShutdownOBU* signal.

By exploiting the inherent parallelism of FPGAs, it is possible to execute simultaneously all the operations performed by the building blocks depicted in Fig. E.6, thus reducing the time needed to detect a fault in the OBU node. In the current implementation, only the node ID is being verified by the *Value Domain Validation* module, but in the future other message fields can be analysed. For now, this verification can provide a good estimation of the time required to perform a validation of the message in the value domain. Furthermore, once more packet fields are added to the frame analysis, the elapsed time will not increase substantially and could even stay the same if the associated tasks can be completely parallelised.

Based on the information retrieved from the RSU scheduling messages, the medium guardian computes the time window assigned to the transmission of the associated OBU in each Elementary Cycle. The *Time Slot Calculation* block (Fig. E.6) makes use of equation E.1 to determine the beginning of this time window. This value is obtained by adding the $SOW_{StartTime}$ instant, representing the beginning of the Synchronous OBU Window (Fig. E.4), to the number of the OBU slot ($OBU_{SlotNumber}$) multiplied by the slot duration ($Slot_{Duration}$) plus the interframe space ($IFS_{Duration}$).

$$\begin{aligned} OBU_{StartTime} =& SOW_{StartTime} + OBU_{SlotNumber} \times \\ & (Slot_{Duration} + IFS_{Duration}) \end{aligned} \tag{E.1}$$

The relative $SOW_{StartTime}$ value, in turn, is calculated by subtracting from the Elementary Cycle duration ($EC_{Duration}$) the total Synchronous OBU Window (SOW), which corresponds to the total number of OBUs (N) multiplied by the slot duration plus the interframe space (equation E.2).

$$\begin{aligned} SOW_{StartTime} =& EC_{Duration} - N \times (Slot_{Duration} + \\ & IFS_{Duration}) \end{aligned} \tag{E.2}$$

Finally, the end of the transmission window can be computed by adding to the $OBU_{StartTime}$, the duration of OBU's slot plus a maximum tolerance value ($Max_{Tolerance}$) that accounts for mismatches in clocks synchronization between the guardian and the OBU as well as for the time delay required by the guardian's reception chain to detect the end of OBU's transmission. This $Max_{Tolerance}$ value can be empirically determined based on experimental testing of the hardware platform.

$$\begin{aligned} OBU_{EndTime} =& OBU_{StartTime} + Slot_{Duration} + \\ & Max_{Tolerance} \end{aligned} \tag{E.3}$$

A similar tolerance value should be included at the beginning of the transmission window (equation E.1), advancing the time of $OBU_{StartTime}$ to account for any mismatches in clock timings. However, in this particular implementation, the detection delay of the guardian's reception chain is much larger than the effects of clock synchronization, so the $Max_{Tolerance}$ term can be removed from equation E.1. On the OBU side, the delay of the transmission chain is also larger than any possible clock mismatches, thus the $OBU_{StartTime}$ also happens first than the first bits sent to the digital-to-analogue (DAC) converter in the OBU node.

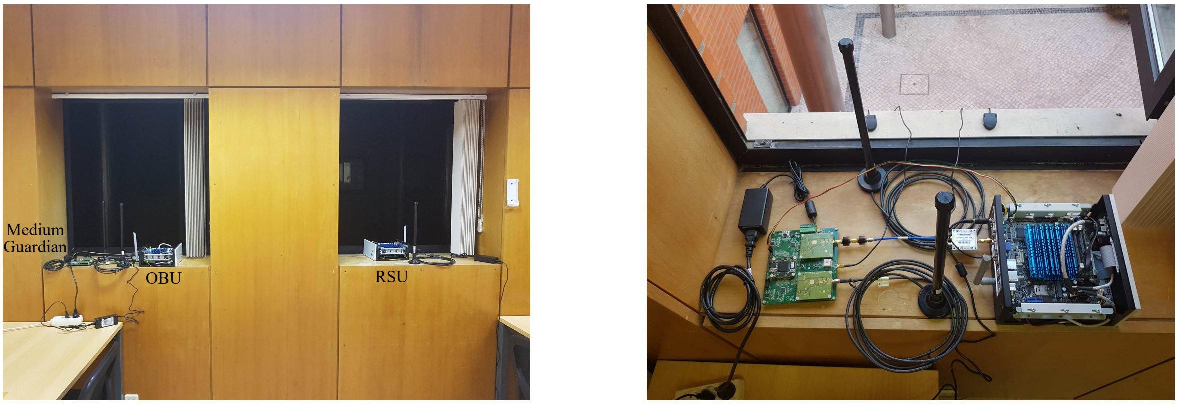
As a result, the *EnableTransmission* signal is put in a high state from the $OBU_{StartTime}$ to the $OBU_{EndTime}$ instants by the medium guardian. This is the time window used both by the OBU to verify if it is transmitting during the correct slot allocation and by the guardian to detect any violation in the communications schedule by the associated node.

E.5 Experimental Tests

The operation of the implemented medium guardian was successfully evaluated in a laboratory environment by utilizing the experimental setup depicted in Fig. E.5. Both the RSU and OBU nodes were implemented in custom vehicular communications platforms with real-time capabilities and able to execute time-triggered transmissions [27]. The guardian monitoring the OBU node was deployed in a dedicated board with independent power supply, according to the architecture presented in Fig. E.6. Despite the fact that the whole experiments were conducted in a laboratory environment, all nodes had GPS signal available from external antennas. Some pictures of the laboratory setup can be observed in Fig. E.7. The main objective of this experimental evaluation was to verify the compliance of the guardian with the behaviour specified in the design phase, both in the case of monitoring a faulty OBU as well as in a fault free scenario. In addition to this, it was particularly important to measure the time required by the guardian to detect a fault in the value or in the time domain. This way, it is possible to evaluate the impact of an invalid transmission in the remaining time slots.

E.5.1 Setup Configuration

During the experiments, two types of packets were exchanged in the control channel: the scheduling messages from the RSU node transmitted at the beginning of the Elementary Cycle and the replies from the OBU in the assigned time slots. The structure of the scheduling messages is presented in Fig. E.8. It starts with the ID number of the RSU (*RSU_ID*), followed by the code of the message type (*MSG_TYPE*) and the size of the packet excluding the frame header (*MSG_SIZE*). After that, there are pairs of values, each pair comprising an *OBU_ID* and an associated *OBU_SLOT* for transmission. Consequently, the total size of the message is variable and depends on the number of OBUs residing in the coverage area of the RSU at each moment. For the tests, a fixed size packet with 6 OBU IDs was employed, one of them belonging to the node being monitored by the guardian.



(a) Laboratory setup.

(b) Medium guardian + OBU.

Figure E.7: Setup configuration for the experimental tests.

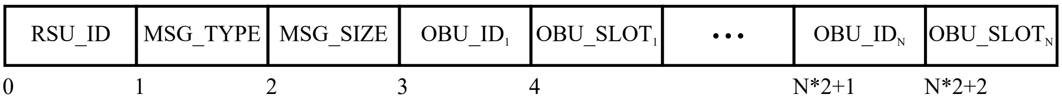


Figure E.8: RSU's scheduling message structure.

The message utilized by the OBU to transmit in the assigned time slot is presented in Fig. E.9. It is composed by the *OBU_ID*, the *MSG_TYPE* and the *MSG_SIZE* fields, followed by the payload of the message where information about e.g. vehicle's position could be included. For a given scenario, the size of the OBUs' messages is static and predefined, allowing the RSU to build the transmission schedule for every communications cycle. In these experiments, the OBU's packet only comprised the frame header, being the payload left unused, i.e. the message had no payload. All the message fields, both in the RSU and OBU packets, are one byte wide. As a result, the total length of the packet in bytes is equal to the number of messages fields, leading to RSU packets of 15 bytes and OBU packets with 3 bytes.

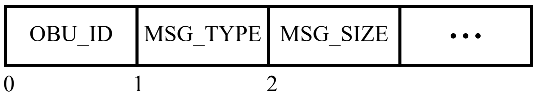


Figure E.9: OBU's message structure.

From the message size, it is then possible to calculate the frame duration in the wireless medium, which constitutes a source of comparison to analyse the timing measurements of the medium guardian's operation. Equations E.4, E.5 and E.6 show how to obtain the transmission time from the number of bytes forming the packet and the configured data rate in Mb/s [28]. As shown in equation E.4, in order to compute the total number of bits in the frame, one needs to multiply by eigth the message length plus 4 bytes from the frame check sequence (FCS) inserted in the MAC layer, and add 6 tailing bits and 16 bits from the SERVICE field.

$$number\_of\_bits = (number\_of\_bytes + 4) * 8 + 16 + 6 \tag{E.4}$$

After that, the number of OFDM symbols composing the frame (eq. E.5) can be calculated by performing the ceiling function to the result of the division between the total number of bits and the number of bits per OFDM symbol for the corresponding modulation. This last value is obtained by multiplying the data rate in Mb/s by eight.

$$number\_of\_symbols = \left\lceil \frac{number\_of\_bits}{data\_rate * 8} \right\rceil \tag{E.5}$$

The resulting frame duration in microseconds (eq. E.6) is equal to the sum of the number of symbols multiplied by the symbol duration (8 μs) together with the time interval of the message preamble (32 μs) plus the SIGNAL field (8 μs).

$$frame\_duration(\mu s) = number\_of\_symbols * 8 + 40 \tag{E.6}$$

With the slowest data rate (3 Mb/s), which corresponds to BPSK modulation with coding rate 1/2, the frame duration of the RSU and OBU packets is 104 μs and 72 μs, respectively. These results are summarized in table E.1 together with the configuration parameters utilized in the experiments.

E.5.2 Timing Measurements

In the experimental tests, timing results were captured for three different situations: 1) fault-free operating scenario, 2) faulty behaviour in the value domain and 3) faulty behaviour in the time domain. A set of 100 trials was executed for each one of these distinct scenarios, each trial constituted by one packet transmission from the RSU (the scheduling message) followed by one packet transmission from the OBU (the reply message). In these experiments, the most relevant FPGA signals were captured both at the guardian and at the OBU, as well as the timing reference provided by the GPS receiver. This way, it was possible to assign globally synchronized timestamps to the signals' events being monitored in both units.

Fig. E.10 exhibits the timing results for the fault-free operating scenario, where the OBU's reply message holds valid values and is transmitted in the correct time slot. The time reference starts with the assertion of the *EnableTransmission* signal from the medium guardian, corresponding to the instant that can be derived from equation E.1. Then, the *obuTransmission=1* event represents the moment when the FPGA in the OBU node starts producing valid digital In-phase/Quadrature (I/Q) samples for transmission by the RF frontend. That packet transmission is detected by the medium guardian approximately 20 μs later, which corresponds to the raise of the CCA value from '0' to '1'. Then after the frame duration has elapsed (72 μs), the OBU stops producing new samples (*obuTransmission=0*), the guardian detects the end of the packet transmission (*guardianCCA=0*) and verifies its contents (*frameVerification=1*), namely the OBU_ID, MSG_TYPE and MSG_SIZE fields in the frame header. Finally, the *EnableTransmission* signal is deasserted at the time instant value that can be derived from equation E.3. A $Max_{Tolerance}$ of 15 μs was used

	RSU	OBU
Central Frequency	5.9 GHz	
Channel Number	180	
Transmission Power	0 dBm	
Channel Bandwidth	10 MHz	
Modulation	BPSK	
Coding Rate	1/2	
Data Rate	3 Mb/s	
Message Size	15 bytes	3 bytes
Frame Duration	104 μs	72 μs
$EC_{Duration}$	100 ms	
$SOW_{StartTime}$	75 ms	
$IFS_{Duration}$	45 μs	
$Max_{Tolerance}$	15 μs	

Table E.1: Setup configuration parameters.

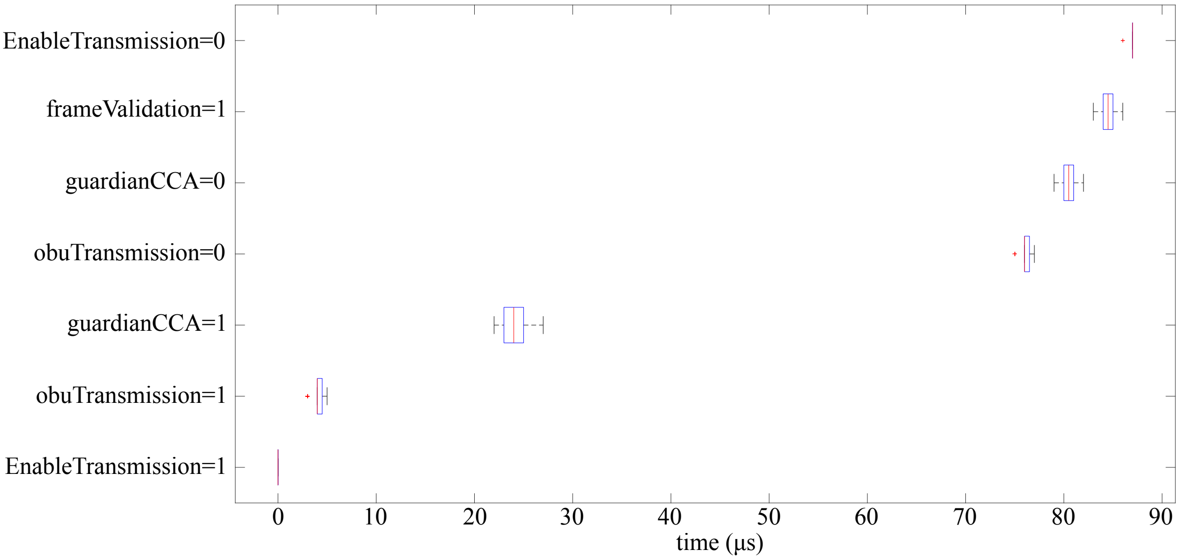


Figure E.10: Timing results in the fault-free scenario.

throughout the experiments, value which will be explained later in more detail.

In the scenario depicted by the results presented in Fig. E.11, faults were injected in the value domain, by modifying the *OBU_ID* field of the OBU's reply message. The sequence of events in this case is very similar to the one displayed in Fig. E.10. However the *frameValidation* flag is not activated but instead the *ShutdownOBU* output pin is raised by the guardian. In this case, the error detection latency, measured from the end of OBU's transmission (*obuTransmission=0*) to the activation of the *ShutdownOBU* pin, is approximately equal to 80 μs (72 μs corresponding to the frame duration plus an effective delay of 8 μs). This verification can only be performed at the end of message's transmission, since the whole frame

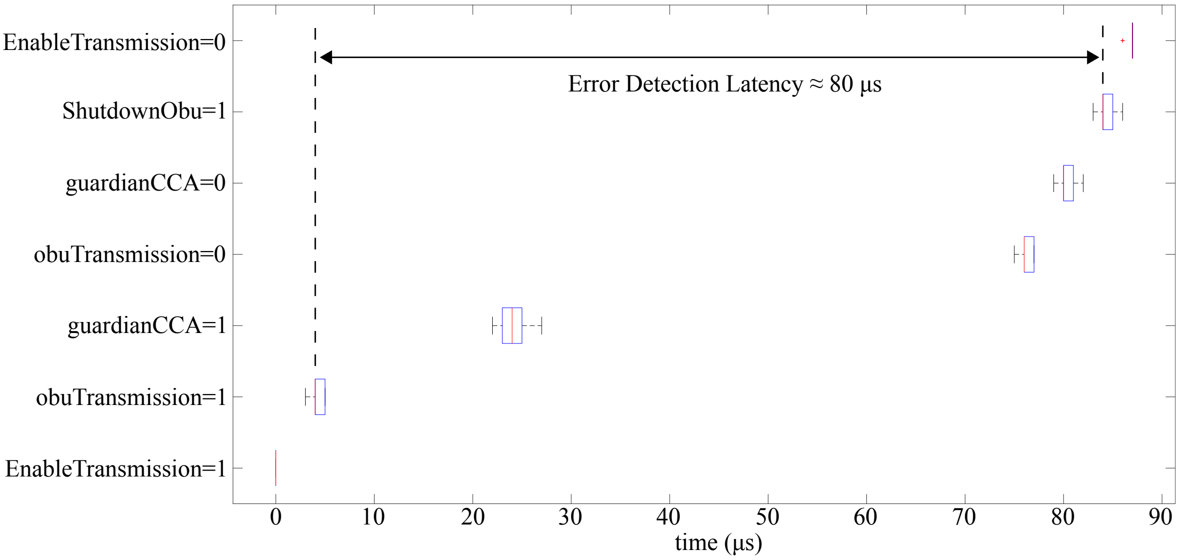


Figure E.11: Timing results with fault injection in the value domain.

and its reception status (including the FCS validation) is only available then.

Finally, Fig. E.12 presents the results obtained for fault injection in the time domain, where the OBU's configuration was modified to transmit in an incorrect interval, in this case in the time slot immediately after the one assigned to it by the RSU's scheduling message. As a result, the time window during which the *EnableTransmission* is enabled, takes place before all the other events in this scenario. After that, the OBU starts transmitting in the subsequent slot, being the frame preamble detected by the guardian (*guardianCCA=1*) and the OBU's operation immediately forced to stop (*ShutdownOBU=1*). The transmission is interrupted, as indicated by the CCA value in the guardian (*guardianCCA=0*), long before the OBU stops producing valid samples (*obuTransmission=0*). This happens because in this specific hardware implementation, the *ShutdownOBU* signal does not completely power off the OBU node, only disables its RF frontend, so that the remaining I/Q samples generated in the FPGA do not reach the OBU's antenna, thus are not transmitted to the wireless medium. The error detection latency in this situation, measured from the beginning of OBU's transmission (*obuTransmission=1*) until the fault detection and corresponding signalling to the OBU node (*ShutdownOBU=1*), is approximately equal to 20 μs.

E.5.3 Results Discussion

The obtained results, which are summarized in table E.2, show that the implemented medium guardian device is capable of correctly detecting and taking action upon faults arising both in the value and time domain. Furthermore, the measured error detection latency is small and with low jitter, thus making the guardian's operation deterministic and useful to employ in real-time wireless communications. It is particularly important to notice that even when the OBU node tries to transmit outside the correct time slot, the guardian's response is so quick (20 μs) that this invalid transmission can not be completed. Therefore, the other nodes of

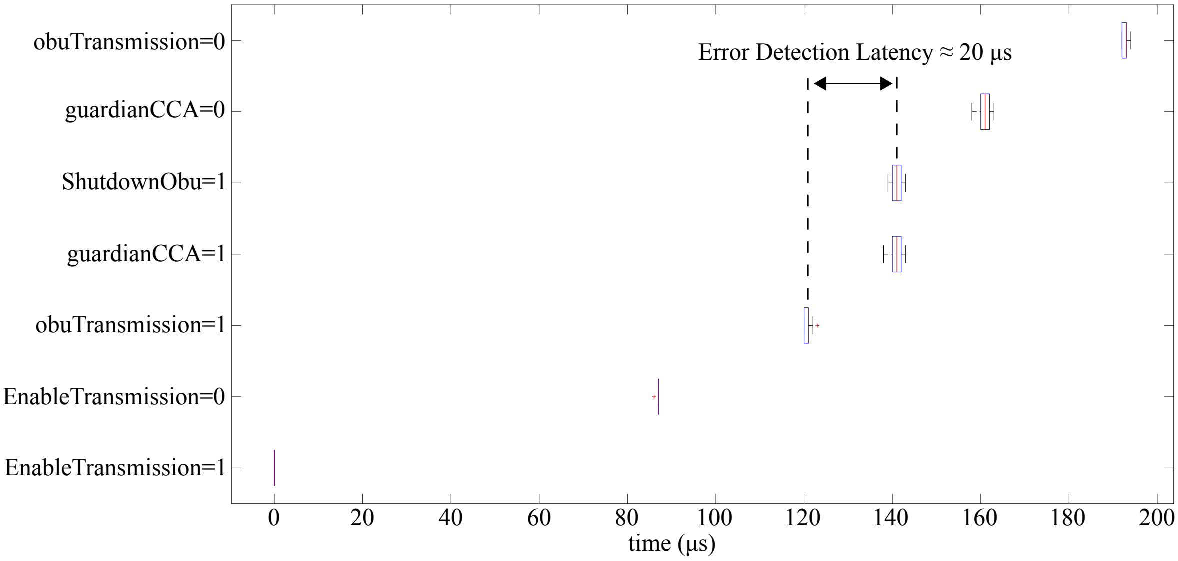


Figure E.12: Timing results with fault injection in the time domain.

Error detection latency	Value domain	Time domain
Mean	80.02μs	19.85μs
Variance	0.02μs	0.57μs

Table E.2: Results summary.

the network are unable to receive and decode this faulty frame, which constitutes a positive aspect of the implemented solution. The reason for this lies in the fact that the shortest valid frame duration that can be obtained according to the standard is equal to 48 μs. This value can be calculated by choosing the smallest frame size (1 byte) and the highest data rate (27 Mbps) and evaluating the results given by equations E.4 - E.6.

A $Max_{Tolerance}$ of 15 μs was chosen based on some preliminary tests showing that after the OBU stops transmitting (*obuTransmission=1*), the CCA value in the medium guardian goes to zero (*guardianCCA=0*) within an interval of approximately 5 μs. Thus, by adding a safety margin of 10 μs, it can be guaranteed that the end of a valid transmission is detected by the guardian, way before the $Max_{Tolerance}$ value has elapsed. By including this 15 μs tolerance in the valid transmission window, the effective $IFS_{Duration}$ is reduced from 45 μs to 30 μs. However, this value is still acceptable for the case of time-triggered transmissions based on TDMA scheduling policies [29].

It should be noticed that the obtained results are generic and can be extended to any packet length or message type. As a result, the experimental assessment of the system covers the different situations that may arise in a real-world scenario, since both value and time faults were carefully analysed. The guardian's operation in the presence of security mechanisms (certificate management and encryption keys) was outside the scope of this work, since it would greatly increase system's complexity and the probability of faults arising during the design and implementation phases. Nevertheless, this could be the subject of future work, given the fact that security features will definitely be present in future wireless vehicular networks.

E.6 Conclusions

In this paper, the medium guardian concept was introduced with the main goal of enhancing the dependability attributes of safety-critical wireless systems. Vehicular communications are among those systems, exhibiting strict real-time requirements that can only be met if the nodes of the network behave in a deterministic and secure way. A practical medium guardian implementation was developed in order to monitor the operation of a mobile node (OBU) inside the vehicular network. The use case scenario under study took advantage of a previously proposed TDMA scheduling protocol, suitable for real-time vehicular communications.

An experimental setup was devised to test the operation of the medium guardian and to evaluate the timing behaviour of the system as a whole. The obtained results proved the effectiveness and good performance of the medium guardian device as a mechanism to detect faults in the value and time domains and to prevent further interference from the faulty node in the wireless medium. The measured error detection latency is small and deterministic, being able to cope with the operation of the real-time MAC protocol.

As future work, the system's performance will be evaluated in the field and more features could be included in the guardian's architecture, e.g. the support for security mechanisms or non-TDMA medium access control schemes. It is expected that nodes' mobility have no effect on the measured results, since these parameters are not affected by vehicle's speed, however this hypothesis needs to be validated under real-world conditions.

Acknowledgements

This work is funded by Fundação para a Ciência e Tecnologia - FCT/MEC through national funds under the PhD scholarship ref. SFRH/BD/52591/2014 and by FEDER – PT2020 partnership agreement under the project UID/EEA/50008/2013.

References

[1] 5GPP, *The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services*, `https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf`, Accessed 28 February 2016.

[2] ITU-R, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, `https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf`, Accessed 28 February 2016.

[3] G. P. Fettweis, "The Tactile Internet: Applications and Challenges", *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 64–70, Mar. 2014, issn: 1556-6072. doi: `10.1109/MVT.2013.2295069`.

[4] D. Qiao, S. Choi, and K. G. Shin, "Goodput analysis and link adaptation for IEEE 802.11a wireless LANs", *IEEE Transactions on Mobile Computing*, vol. 1, no. 4, pp. 278–292, Oct. 2002, issn: 1536-1233. doi: `10.1109/TMC.2002.1175541`.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, issn: 0018-9219. doi: `10.1109/JPROC.2016.2558521`.

[6] F. Cristian, "Understanding Fault-tolerant Distributed Systems", *Communications of the ACM*, vol. 34, no. 2, pp. 56–78, Feb. 1991, issn: 0001-0782. doi: `10.1145/102792.102801`.

[7] S. Poledna, *Fault-Tolerant Real-Time Systems: The Problem of Replica Determinism.* Norwell, MA, USA: Kluwer Academic Publishers, 1996.

[8] T. Omar, Z. Abichar, A. E. Kamal, J. M. Chang, and M. Alnuem, "Fault-Tolerant Small Cells Locations Planning in 4G/5G Heterogeneous Wireless Networks", *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, Oct. 2016, issn: 0018-9545. doi: `10.1109/TVT.2016.2615325`.

[9] A. Ravanshid, P. Rost, D. S. Michalopoulos, V. V. Phan, H. Bakker, D. Aziz, S. Tayade, H. D. Schotten, S. Wong, and O. Holland, "Multi-connectivity functional architectures in 5G", in *2016 IEEE International Conference on Communications Workshops (ICC)*, May 2016, pp. 187–192. DOI: 10.1109/ICCW.2016.7503786.

[10] S. Worrall, G. Agamennoni, J. Ward, and E. Nebot, "Fault Detection for Vehicular Ad Hoc Wireless Networks", *Intelligent Transportation Systems Magazine, IEEE*, vol. 6, no. 2, pp. 34–44, Summer 2014, ISSN: 1939-1390. DOI: 10.1109/MITS.2014.2304974.

[11] J. Almeida, J. Ferreira, and A. S. R. Oliveira, "Poster: Medium Guardian - the Bus Guardian Concept applied to Wireless Communications Systems", in *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*, ser. EWSN '17, Uppsala, Sweden: Junction Publishing, 2017, pp. 194–195, ISBN: 978-0-9949886-1-4.

[12] ——, "Fault Tolerant Architecture for Infrastructure based Vehicular Networks", in *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira, and J. Fonseca, Eds., Cham: Springer International Publishing, 2016, ch. 8, pp. 169–194, ISBN: 978-3-319-28183-4. DOI: 10.1007/978-3-319-28183-4_8.

[13] A. L. Hopkins, T. B. Smith, and J. H. Lala, "FTMP - A highly reliable fault-tolerant multiprocess for aircraft", *Proceedings of the IEEE*, vol. 66, no. 10, pp. 1221–1239, Oct. 1978, ISSN: 0018-9219. DOI: 10.1109/PROC.1978.11113.

[14] C. Temple, "Avoiding the babbling-idiot failure in a time-triggered communication system", in *Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on*, Jun. 1998, pp. 218–227. DOI: 10.1109/FTCS.1998.689473.

[15] I. Broster and A. Burns, "An analysable bus-guardian for event-triggered communication", in *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, Dec. 2003, pp. 410–419. DOI: 10.1109/REAL.2003.1253288.

[16] J. Ferreira, L. Almeida, A. Fonseca, P. Pedreiras, E. Martins, G. Rodriguez-Navas, J. Rigo, and J. Proenza, "Combining operational flexibility and dependability in FTT-CAN", *IEEE Transactions on Industrial Informatics*, vol. 2, no. 2, pp. 95–102, May 2006, ISSN: 1551-3203. DOI: 10.1109/TII.2005.875508.

[17] G. Bauer, H. Kopetz, and W. Steiner, "The central guardian approach to enforce fault isolation in the time-triggered architecture", in *The Sixth International Symposium on Autonomous Decentralized Systems, 2003. ISADS 2003.*, Apr. 2003, pp. 37–44. DOI: 10.1109/ISADS.2003.1193930.

[18] H. Lans, "Position Indicating System", Patent 5 506 587, Apr. 1996.

[19] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond", *IEEE Communications Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014, ISSN: 0163-6804. DOI: 10.1109/MCOM.2014.6736751.

[20] S. Haykin, “Cognitive radio: brain-empowered wireless communications”, *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005, ISSN: 0733-8716. DOI: `10.1109/JSAC.2004.839380`.

[21] G. Wunder, P. Jung, M. Kasparick, T. Wild, F. Schaich, Y. Chen, S. T. Brink, I. Gaspar, N. Michailow, A. Festag, L. Mendes, N. Cassiau, D. Ktenas, M. Dryjanski, S. Pietrzyk, B. Eged, P. Vago, and F. Wiedmann, “5GNOW: non-orthogonal, asynchronous waveforms for future mobile applications”, *IEEE Communications Magazine*, vol. 52, no. 2, pp. 97–105, Feb. 2014, ISSN: 0163-6804. DOI: `10.1109/MCOM.2014.6736749`.

[22] N. Michailow, M. Matthé, I. S. Gaspar, A. N. Caldevilla, L. L. Mendes, A. Festag, and G. Fettweis, “Generalized Frequency Division Multiplexing for 5th Generation Cellular Networks”, *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3045–3061, Sep. 2014, ISSN: 0090-6778. DOI: `10.1109/TCOMM.2014.2345566`.

[23] H. Bogucka, A. M. Wyglinski, S. Pagadarai, and A. Kliks, “Spectrally agile multicarrier waveforms for opportunistic wireless access”, *IEEE Communications Magazine*, vol. 49, no. 6, pp. 108–115, Jun. 2011, ISSN: 0163-6804. DOI: `10.1109/MCOM.2011.5783994`.

[24] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “An RSU Replication Scheme for Dependable Wireless Vehicular Networks”, in *2016 12th European Dependable Computing Conference (EDCC)*, Sep. 2016, pp. 229–240. DOI: `10.1109/EDCC.2016.11`.

[25] T. Meireles, J. Fonseca, and J. Ferreira, “The Case for Wireless Vehicular Communications Supported by Roadside Infrastructure”, in *Intelligent Transportation Systems Technologies and Applications*, A. Perallos, U. Hernandez-Jayo, E. Onieva, and I. J. García-Zuazola, Eds., John Wiley & Sons, Ltd, 2015, pp. 57–82, ISBN: 9781118894774. DOI: `10.1002/9781118894774.ch4`. [Online]. Available: `http://dx.doi.org/10.1002/9781118894774.ch4`.

[26] ETSI, *EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, v.1.3.2*, Nov. 2014.

[27] J. Almeida, J. Ferreira, and A. S. R. Oliveira, “Development of an ITS-G5 station, from the physical to the MAC layer”, in *Intelligent Transport Systems: from Good Practice to Standards*, P. Pagano, Ed., CRC Press, Taylor and Francis Group, 2016, ch. 1, pp. 1–37. DOI: `10.1201/9781315370866-2`.

[28] “IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, Mar. 2012.

[29] A. Khan, J. Almeida, B. Fernandes, M. Alam, P. Pedreiras, and J. Ferreira, "Towards Reliable Wireless Vehicular Communications", in *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on*, Sep. 2015, pp. 167–172. DOI: 10.1109/ITSC.2015.36.

List of Publications

- J. Ferreira, A. Oliveira, **J. Almeida** and C. Cruz, "Fail Silent Road Side Unit for Vehicular Communications", *SAFECOMP 2013 - Workshop ASCoMS (Architecting Safety in Collaborative Mobile Systems) of the 32nd International Conference on Computer Safety, Reliability and Security*, September, 2013, Toulouse, France, pp. 343-354
- A. Khan, **J. Almeida**, B. Fernandes, M. Alam, P. Pedreiras and J. Ferreira, "Towards Reliable Wireless Vehicular Communications", *IEEE 18th International Conference on Intelligent Transportation Systems*, Las Palmas, Spain, 2015, pp. 167-172, doi: 10.1109/ITSC.2015.36
- **J. Almeida**, M. Alam, B. Fernandes, A. Khan, A. Oliveira and J. Ferreira, "Reliable Delivery of Safety Messages in Infrastructure Based Vehicular Networks", *IEEE 18th International Conference on Intelligent Transportation Systems*, Las Palmas, Spain, 2015, pp. 244-249, doi: 10.1109/ITSC.2015.49
- **J. Almeida**, J. Ferreira and A. S. R. Oliveira, "Fault Tolerant Architecture for Infrastructure based Vehicular Networks", *Intelligent Transportation Systems: Dependable Vehicular Communications for Improved Road Safety*, M. Alam, J. Ferreira and J. Fonseca, Eds., Springer International Publishing, 2016, Vol. 52, ch. 8, pp. 169-194, doi: 10.1007/978-3-319-28183-4_8
- **J. Almeida**, M. Alam, J. Ferreira and A. S. R. Oliveira, "Mitigating Adjacent Channel Interference in Vehicular Communication Systems", *Digital Communications and Networks*, Vol. 2, Issue 2, 2016, Pages 57-64, doi: 10.1016/j.dcan.2016.03.001
- **J. Almeida**, J. Ferreira, and A. S. R. Oliveira, "Development of an ITS-G5 Station, from the Physical to the MAC Layer", *Intelligent Transport Systems: from Good Practice to Standards*, P. Pagano, Ed., CRC Press, Taylor and Francis Group, 2016, ch. 1, pp. 1-37, doi: 10.1201/9781315370866-2
- **J. Almeida**, J. Ferreira and A. S. R. Oliveira, "An RSU Replication Scheme for Dependable Wireless Vehicular Networks", *12th European Dependable Computing Conference (EDCC)*, Gothenburg, Sweden, 2016, pp. 229-240, doi: 10.1109/EDCC.2016.11
- **J. Almeida**, J. Ferreira, A. S. R. Oliveira, P. Pedreiras and J. Fonseca, "Enforcing Replica Determinism in the Road Side Units of Fault-Tolerant Vehicular Networks", *The 1st EAI International Conference on Future Intelligent Vehicular Technologies (Future 5V)*, Porto, Portugal, 2016, pp. 3-12, doi: 10.1007/978-3-319-51207-5_1
- N. Cardoso, M. Alam, **J. Almeida**, J. Ferreira and A. S. R. Oliveira, "Performance Evaluation of SIMO Techniques in IEEE 802.11p", *The 1st EAI International Conference*

on Future Intelligent Vehicular Technologies (Future 5V), Porto, Portugal, 2016, pp. 91-100, doi: 10.1007/978-3-319-51207-5_9

- **J. Almeida**, M. Alam, J. Ferreira and A. S. R. Oliveira, "Timing Analysis of an Active Replication Scheme for the Road Side Units of Vehicular Networks", *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, Florence, Italy, 2016, pp. 4719-4724, doi: 10.1109/IECON.2016.7793749
- J. Blancou, **J. Almeida**, B. Fernandes L. Silva, M. Alam, J. Fonseca and J. Ferreira, "eCall++: An Enhanced Emergency Call System for Improved Road Safety", *IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, United States, 2016, pp. 1-8, doi: 10.1109/VNC.2016.7835964
- M. Alam, B. Fernandes, **J. Almeida**, J. Ferreira and J. Fonseca, "Integration of Smart Parking in Distributed ITS Architecture", *International Conference on Open Source Systems & Technologies (ICOSST)*, Lahore, Pakistan, 2016, pp. 84-88, doi: 10.1109/ICOSST.2016.7838582
- **J. Almeida**, J. Ferreira and A. S. R. Oliveira "Poster: Medium Guardian - the Bus Guardian Concept Applied to Wireless Communications Systems", *Proc. International Conference on Embedded Wireless Systems and Networks*, Uppsala, Sweden, 2017, pp. 194-195
- J. Rufino, M. Alam, **J. Almeida** and J. Ferreira, "Software Defined P2P Architecture for Reliable Vehicular Communications", *Pervasive and Mobile Computing*, Vol. 42, 2017, pp. 411-425, doi: 10.1016/j.pmcj.2017.06.014
- **J. Almeida**, J. Ferreira and A. S. R. Oliveira, "Fail Silence Mechanism for Dependable Vehicular Communications", *International Journal of High Performance Computing and Networking*, October, 2017, Vol. 10, No. 6, pp. 534-545, doi: 10.1504/IJHPCN.2017.10008241
- J. Ferreira, J. Fonseca, D. Gomes, J. Barraca, B. Fernandes, J. Rufino, **J. Almeida** and R. Aguiar, "PASMO: An Open Living Lab for Cooperative ITS and Smart Regions", *IEEE International Smart Cities Conference (ISC2)*, Wuxi, China, 2017, pp. 1-6, doi: 10.1109/ISC2.2017.8090866
- **J. Almeida**, J. Ferreira and A. S. R. Oliveira, "A Medium Guardian for Enhanced Dependability in Safety-Critical Wireless Systems", *IEEE Transactions on Intelligent Transportation Systems*, March, 2018, Vol. 19, no. 3, pp. 965-976, doi: 10.1109/TITS.2017.2777909
- J. Ferreira, M. Alam, B. Fernandes, **J. Almeida**, L. Silva, L. Moura, R. Costa, G. Iovino and E. Cordiviola, "Cooperative Sensing for Improved Traffic Efficiency: the Highway Field Trial", *Computer Networks*, October, 2018, Vol. 143, no. 9, pp. 82-97, doi: 10.1016/j.comnet.2018.07.006
- W. Farhat, J. Rufino, B. Fernandes, **J. Almeida**, M. Alam, J. Ferreira and C. Souani, "Towards ITS Vision Assisted Cooperative Perception", *IEEE 87th Vehicular Technology Conference (VTC2018-Spring)*, Porto, Portugal, 2018, pp. 1-4, doi: 10.1109/VTC-Spring.2018.8417862