République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté des Sciences Exactes
Département d'Informatique
Laboratoire d'Informatique MEDicale (LIMED)

THÈSE

EN VUE DE L'OBTENTION DU DIPLOME DE DOCTORAT

Domaine : Mathématiques et Informatique Filière : Informatique
Spécialité : Data Science

Présentée par
Djamila ZAMOUCHE

Thème

Security and Safety of Intelligent Transportation Systems

Soutenue le 02/03/2022 devant le Jury composé de :

Nom et Prénom	Grade		
Mme Louiza BOUALLOUCHE	Professeur	Univ. de Bejaia, Algérie	Présidente
M. Sofiane AISSANI	M.C.A.	Univ. de Bejaia, Algérie	Rapporteur
M. Mawloud OMAR	M.C, HDR	Univ. Gustave-Eiffel, France	Co-rapporteur
Mme Lamia HAMZA	M.C.A.	Univ. de Bejaia, Algérie	Examinatrice
Mme Djamila BOUKREDERA	M.C.A.	Univ. de Bejaia, Algérie	Examinatrice
M. Reda KASMI	M.C.A.	Univ. de Bouira, Algérie	Examinateur
M. Mohamed MOHAMMEDI	M.C.A.	Univ. de Bejaia, Algérie	Invité

Année Universitaire : 2021/2022

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of BEJAIA

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculty of Exact Sciences
Department of Computer Science
Research Laboratory LIMED

Thesis
submitted for the degree of ***Doctor of Philosophy***

In: COMPUTER SCIENCE
Option: DATA SCIENCE

By**: Djamila ZAMOUCHE**

Subject

Security and Safety of Intelligent Transportation Systems

Jury:

Chair:

Prof. Louiza BOUALLOUCHE — University of Bejaia, Algeria

Examiners:

Dr. Lamia HAMZA — University of Bejaia, Algeria
Dr. Djamila BOUKREDERA — University of Bejaia, Algeria
Dr. Reda KASMI — University of Bouira, Algeria

Supervisors:

Dr. Sofiane AISSANI — University of Bejaia, Algeria
Dr. Mawloud OMAR — University Gustave-Eiffel, France

Guest:

Dr. Mohamed MOHAMMEDI — University of Bejaia, Algeria

2021-2022

Abstract

Over the last decades, advancements in computing, electronics, and mechanical systems have been resulting in the development of transportation all over the world, which has been providing a lot of benefits for many aspects of human life. Intelligent Transportation Systems (ITSs) are advanced applications that aim to make the transportation infrastructures safer, more convenient, and smarter by using information that is shared among vehicles such as crash warning, sudden-brake warning, lane-change warning, and so on. Thus, such systems provide a wide variety of services including, but not limited to, traffic control, traffic management, passenger and road safety, and remote region connectivity. However, several challenges hampering the proper operation of these systems, such as extreme disturbances and they rely on several kinds of devices that can cause malfunctions. Moreover, vehicular communications are expected to be subject to severe breaches that affect the reliability of the exchanged information. Seeking to improve the safety and protect human life, in this thesis, we address these problems by providing improvements to the existing STIs. In particular, we have proposed an *enhanced train-centric communication-based train control system* for railway transportation that allows improving the quality and enhancing reliability of the train control. Moreover, we have proposed our second contribution that manifests itself in the proposition of a *discordant safety messages detection strategy in connected vehicles environment* that provides the vehicles with the ability to quickly and preemptively identify discordant messages and hence dealing against potential disturbances, while ensuring a trade-off between the efficiency and safety. The proposed mechanisms are evaluated through simulations in terms of important metrics. The obtained results highlight the promising performances of our proposals.

Keywords : Intelligent Transportation Systems, Vehicular Networks, Security, Safety, Process Algebra, Anomaly Detection.

Acknowledgements

Trust in the God with all your heart, in all your ways acknowledge Him, and He shall direct your paths.

First, my thanks and gratitude should be expressed to Almighty Allah who has granted me with a great will and spiritual support in my life.

I would like to express my deepest gratitude and acknowledgement to all the great people who supported me along the way towards completing my Ph.D. studies.

I would like to extend my sincere thanks to my Ph.D. supervisor Dr. Sofiane AISSANI for his invaluable support, endless encouragement, and constant advisement. During these three years, he has always found the time for me to guide and encourage my research activities whenever it was needed. Thank you.

I am sincerely grateful to my Ph.D. co-supervisor Dr. Mawloud OMAR for his consistent motivation, exemplary supervision, great guidance, and unconditional support. Dr. OMAR, you are a humble, dedicated, inspiring, and caring advisor. You are and always be for me, a dedicated teacher and an exemplary supervisor. Thank you.

No volume of words is enough to express my sincere thanks towards Dr. Mohamed MOHAMMEDI. First, I would like to thank him for his patient guiding and inspiring throughout my thesis period. Secondly, I highly appreciate his motivation, encouragement and support in my research work, which helped me build confidence and courage to overcome difficulties.

I gratefully acknowledge my Ph.D. committee members, Prof. Louiza BOUALLOUCHE, Dr. Lamia HAMZA, Dr. Djamila BOUKREDERA, and Dr. Reda KASMI, for their constructive comments and insightful suggestions, which helped me improve the quality of my thesis.

I would like to express my sincere gratitude to my dear parents, sister, and brother for their unconditional support, love and trust. My mother who has always been with me with her prayers, spiritual support and assistance. And my father who has given me everything in my life. Without their unwavering faith in me and their support to

pursue my dreams, I would never have been able to complete my thesis. Words are not enough for expressing all the thanks him.

I would like to thank all my dear family and friends who have provided constant encouragement. The list is too long to be put here. But they have always been of greet help during these three years of Ph.D.

Furthermore, I am greatly thankful to all of my colleagues in the LIMED Laboratory and Research Unit LaMOS for providing me with the warm and friendly atmosphere.

Finally, I would express all my gratitude to all the members of computer science department of University of Bejaia, whether they are teachers or administrators, who saved no effort to ensure that our training and our work ends in good conditions.

I would like to dedicate this thesis
To the memory of my Grand Mother
To my loving parents
To my dear sister and brother
To all people that I love.

Table of contents

Contents v

List of figures viii

List of tables ix

List of acronyms x

1 Introduction 1

1.1 Context of our study . . . 1
1.2 Motivation and objectives . . . 3
1.3 Thesis contributions and outline . . . 4
1.4 List of publications . . . 5

2 Theoretical Background 7

2.1 Introduction . . . 7
2.2 Intelligent Transportation Systems . . . 7
2.2.1 ITS architecture . . . 8
2.2.2 ITSs applications . . . 9
2.3 Enabling technologies for ITSs . . . 13
2.3.1 Connected and automated vehicles . . . 14
2.3.2 Dedicated Short-Range Communication (DSRC) spectrum . . . 14
2.3.3 Wireless Access in Vehicular Environment (WAVE) protocol . . . 15
2.3.4 Communication infrastructures . . . 16
2.4 ITS environment challenges . . . 18
2.5 Security and Safety aspects in ITSs . . . 20
2.6 Fundamentals of the contributions . . . 21
2.6.1 Formal modeling . . . 21
2.6.2 Process algebra CBPA . . . 22

2.6.3 Formal validation . . . 24
2.6.4 Gaussian distribution approach . . . 25
2.7 Conclusion . . . 25

3 Literature Review of Security and Safety Approaches of Intelligent Transportation Systems 27
3.1 Introduction . . . 27
3.2 Classification . . . 27
3.3 Critical study and overall discussion . . . 31
3.3.1 Railway ITSs . . . 31
3.3.2 Road ITSs . . . 40
3.4 Conclusion . . . 56

4 Ultra-Safe and Reliable Enhanced Train-centric Communication-Based Train Control System 57
4.1 Introduction . . . 57
4.2 Problem statement . . . 58
4.3 Our proposed approach . . . 58
4.3.1 Overview . . . 59
4.3.2 ETcCBTC system architecture . . . 60
4.3.3 Safety monitoring method . . . 61
4.3.4 Safety analysis . . . 66
4.4 Performance study . . . 68
4.4.1 Simulation parameters . . . 68
4.4.2 The obtained results . . . 69
4.5 Conclusion . . . 73

5 Highly Efficient Approach for Discordant BSMs Detection in Connected Vehicles Environment 75
5.1 Introduction . . . 75
5.2 Problem statement . . . 76
5.3 Our proposed approach . . . 78
5.3.1 Overview . . . 78
5.3.2 BSM traffic model . . . 79
5.3.3 Incoherence detection approach . . . 81
5.3.4 Complexity analysis . . . 82
5.4 Performance study . . . 85

5.4.1 Experiment setting 85
5.4.2 The obtained results 90
5.5 Conclusion 94

6 Conclusion and Future Directions **95**
6.1 Conclusion 95
6.2 Future works 97

References **98**

List of figures

2.1 The national ITS architecture. 9
2.2 Illustrative scenario of the exchange of BSMs and emergency messages. 13
2.3 Typical connected and automated vehicle. 15
2.4 DSRC Spectrum allocated by FCC. 16
2.5 Illustration of WAVE protocol stack. 17
2.6 Vehicular communications in ITS. 18
2.7 Gaussian distribution. 26

3.1 Taxonomy of the reviewed approaches. 30

4.1 ETcCBTC system architecture. 61
4.2 Flowchart of the safety supervision of the proposed ETcCBTC system. 63
4.3 Safety policy graph. 64
4.4 Train behaviors graph. 65
4.5 Response time versus trains number. 70
4.6 Transmission load versus train number. 72
4.7 Safe operation rate versus probability of OSPM failure. 73
4.8 Check success and false alarm rates of our safety checking module versus time. 74

5.1 Disruption risk in function of BSM metrics. 77
5.2 Incoherence detection overview. 84
5.3 Traffic simulation area. 86
5.4 Flowchart of the simulation steps. 87
5.5 The Precision / Recall versus the threshold. 91
5.6 The efficiency of the proposed model. 92
5.7 Comparison of the detection efficiency on the generated anomaly dataset. 92
5.8 Execution time versus simulated dataset size. 93

List of tables

2.1 Safety applications with their requirements [20], [77]. 12

3.1 Overall comparison of the reviewed approaches proposed for rail ITSs. . 38
3.2 Overall comparison of the reviewed approaches proposed for the road safety-applications. 54

4.1 Notations 62
4.2 Simulation parameters 69

5.1 Notations 80
5.2 Average execution time of elementary operations. 89
5.3 Performances of the proposed approach. 94

List of acronyms

ATO	**A**utomatic **T**rain **O**peration
ATP	**A**utomatic **T**rain **P**rotection
ATS	**A**utomatic **T**raffic **S**upervision
BDL	**B**ayesian **D**eep **L**earning
BPA	**B**asic **P**rocess **A**lgebra
BSM	**B**asic **S**afety **M**essage
CAN	**C**ontrol **A**rea **N**etwork
CAV	**C**onnected and **A**utomated **V**ehicle
CBPAC	**C**onditional **B**asic **P**rocess **A**lgebra with **C**ommunication
CBPA	**C**onditional **B**asic **P**rocess **A**lgebra
CBTC	**C**ommunication-**B**ased **T**rain **C**ontrol
CDF	**C**umulative **D**istribution **F**unction
CH	**C**luster **H**ead
CLR	**C**ryptographic **L**oss **R**ate
CPS	**C**yber-**P**hysical **S**ystem
CTC	**C**entralized **T**raffic **C**ontrol
CV	**C**onnected **V**ehicle
DSPN	**D**eterministic and **S**tochastic **P**etri **N**ets
DSRC	**D**edicated **S**hort **R**ange **C**ommunication
DWT	**D**iscrete **W**avelet **T**ransform
DoS	**D**enial **o**f **S**ervice
ETCS	**E**uropean **T**rain **C**ontrol **S**ystem
ETcCBTC	**E**nhanced **T**rain-**c**entric **C**ommunication-**B**ased **T**rain **C**ontrol
FCC	**F**ederal **C**ommunications **C**ommission
FTA	**F**ailure **T**ree **A**nalysis
GPS	**G**lobal **P**ositioning **S**ystem
HA	**H**ybrid **A**utomata

ICT	**I**nformation and **C**ommunications **T**echnology
IPEM	**I**terative **P**runing **E**rror **M**inimization
ISDM	**I**ntelligent and **S**afe **D**riving **M**ethods
ITFN	**I**ntuitionistic **T**rapezoidal **F**uzzy **N**umbers
ITS	**I**ntelligent **T**ransportation **S**ystem
IVC	**I**nter-**V**ehicular **C**ommunications
IoT	**I**nternet of **T**hings
LC	**L**evel **C**rossing
LIN	**L**ocal **I**nterconnect **N**etwork
LPN	**L**abeled **P**etri **N**et
LTE	**L**ong **T**erm **E**volution
LiDAR	**Li**ght **D**etection **A**nd **R**anging
MAC	**M**essage **A**uthentication **C**ode
MAL	**M**ovement **A**uthority **L**imit
MA	**M**ovement **A**uthority
MC	**M**arkov **C**hain
MLPQ	**M**ulti-**L**evel **P**riority **Q**ueues
MOST	**M**edia **O**riented **S**ystems **T**ransport
NGTCS	**N**ext **G**eneration **T**rain **C**ontrol **S**ystem
NLOS	**N**on **L**ine **O**f **S**ight
NS	**N**etwork **S**imulator
OBU	**O**n-**B**oard **U**nit
OCU	**O**bject **C**ontrol **U**nit
OSPM	**O**ver **S**peed **P**rotection **M**odule
PNC	**P**hysical-**L**ayer **N**etwork **C**oding
RLNC	**R**andom **N**inear **N**etwork **C**oding
RSSI	**R**eceived **S**ignal **S**trength **I**ndicator
RSU	**R**oad **S**ide **U**nit
SFS	**S**egment-based **F**orwarder **S**election
SUMO	**S**imulation of **U**rban **MO**bility
TOBC	**T**rain **O**n-**B**oard **C**ontroller
TSC	**T**raffic **S**upervision **C**enter
TSSN	**T**rain **S**afety **S**ensor **N**etwork
TcCBTC	**T**rain-**c**entric **C**ommunication-**B**ased **T**rain **C**ontrol
US DoT	**U**nited **S**tates **D**epartment of **T**ransportation
V2I	**V**ehicle-to-**I**nfrastructure

V2V	**V**ehicle-to-**V**ehicle
VANET	**V**ehicular **A**d hoc **NET**work
VOBC	**V**ehicle **O**n-**B**oard **C**ontroller
WAVE	**W**ireless **A**ccess in **V**ehicular **E**nvironments
WHO	**W**orld **H**ealth **O**rganization
WSMP	**W**AVE **S**hort **M**essage **P**rotocol
ZC	**Z**one **C**ontroller

Chapter 1

Introduction

"The beginning of knowledge is the discovery of something we do not understand."
Frank Herbert

1.1 Context of our study

The Internet of Things (IoT) is an emerging concept that bring forward new promising solutions in all areas of everyday life [30], [47]. The IoT is a giant network of connected *things* or *objects*, which have identities, physical attributes, use intelligent interfaces, and are seamlessly integrated into the information network [26], [57]. As a result, the IoT paradigm is envisioned as an enabler for a new generation of systems known as *Cyber-Physical Systems* (CPSs). CPSs refer to the next generation of engineered systems focusing on integration of Information and Communications Technology (ICT) systems (sensing, actuating, computing, communicating, and so on) to provide users with a wide range of innovative applications and services [36], [74]. CPSs have made evolutionary changes in large-scale systems from mechanical, electrical, chemical to biological systems in various application domains such as energy conservation, industrial and environmental control, healthcare, traffic management and safety, advanced automotive systems, and so on, [80]. Some of these application scenarios are found in the context of *Intelligent Transport Systems* (ITS). Recent years, ITSs attracts a great deal of attention and interest of the researchers' community as it is a new way toward deeply reforming the conventional transportation systems. The United States Department of Transportation (US DoT) defines ITS as *"the electronics, communications or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety and mobility and enhance productivity"* [7]. Also, accordingly

to ITS America, ITSs are defined as *"a broad range of diverse technologies, which holds the answer to many of transportation problems. ITS is comprised of a number of technologies, including information processing, communications, control, and electronics. Joining these technologies to our transportation system will save lives, save time, and save money"* [5]. In simple words, ITSs are a group of technologies that provide guidance throughout the journey to improve road safety, optimize the use of transport infrastructures, and reduce traffic congestion in today's cities. In fact, the wireless communications and Connected and Automated Vehicles (CAVs) technology is the key enabler of ITSs [64], [72], [112], transforming vehicles into smart mobile entities that are able to provide innovative services relating to different modes of transportation. As such, large number of ITSs such as advanced traffic management systems and traffic control systems are developed in recent years to solve the transportation issues.

The wireless communications system is a huge contribution toward the design of fully operational ITSs. Its communication modes including, in particular, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enable real-time information exchange between vehicles and their surroundings such as others vehicles, roadside infrastructures (e.g., traffic light systems and base stations), remote infrastructures in the cloud, and even pedestrians, providing two primary branches of services, namely, *non-safety applications* and *safety applications* [16], [88]. The former category deals with comfort of the drivers and passengers in the journey providing some services like region of interest information, weather forecast, entertainment services such as audio and video streaming and web access service. The latter category, being the most critical objective of ITSs, aims at offering safety-related services like collision avoidance warning, real-time traffic conditions dissemination, and accidents notification. As such, ITSs have the potential to provide a wide variety of services, where they can promote the safety of road users, whether drivers or passengers, reducing the number of deaths and injuries from traffic accidents, reduce human errors, etc. [19], [82]. Moreover, they have significant environmental benefits that are based on the principle that fewer vehicles in operation result in lowering fuel consumption and consequently less carbon emissions [97]. Besides, such system guarantee enormous economic benefits as both carriers and transport users will be able to make more reasonable decisions to reduce passengers and cargo transportation time and to cut transportation expenditures and delays [60]. On other hand, the communication paradigm enables the vehicles to be a valuable source of traffic data that feeds different online safety control systems. Accordingly, such applications and services as well as their associated challenges impose

safety and reliability requirements for that ITSs be successfully designed, especially as any operation's failure of these systems make the road users safety at stake.

1.2 Motivation and objectives

Traffic control systems are, of course, of a great significance in transportation safety. The notable research enthusiasm to establish a revolutionary and efficient traffic control systems is primarily due to their potential benefits as well as their associated challenges. In fact, these systems are faced with novel and unanticipated situations that have not been considered at the design stage [2]. The major challenges hampering the proper operation of control systems are numerous, including: such systems are based in large number and several kinds of devices which can cause malfunction, extreme disturbances, several communication interfaces, and others factors [18]. Given the characteristics of these control systems that are particularly extremely sensitive to delays, all of these challenging aspects will result naturally in a failure in systems' operation, hence, to traffic accidents. To illustrate, in the road, autonomous vehicles will regularly encounter novel situations (e.g., an accident occurs) that require real-time perception, reasoning, and decision making in order to prevent other road hazards from happening, which means that no operation's failure is tolerated. Consequently, this involve designing effective techniques for system's operation monitoring at run time as well, which can handle potential failures. Such challenges and opportunities serve as the background of the widespread interest in control systems. On the other hand, the most safety-related services targeted for the ITSs rely widely on the exchange of information among vehicles. However, vehicular networks incorporate some of characteristics that represent vulnerabilities of the vehicular communications, which make them easy to penetrate by the attacker [84], [91], [95] such as an open communication medium, a highly changeable topology, lack of fixed security infrastructures, etc. The security of these networks is vital as, in the case of malicious behavior involving just one vehicle, the entire system will be paralyzed, which will affect all other vehicles in that particular zone, for example via DoS attacks. Many researches have been carried out to solve the security and safety issue of ITSs. Unfortunately, most of the existing solutions make them even more complex and less efficient, which require revisions or development of new solutions. In this dissertation, we target to deal with challenges facing the ITSs efficiency and ensure the security and reliability of the safety-critical information. Consequently, the main objective of our work is to design new safety and security

approaches taking into account ITSs constraints and meeting their specific needs in terms of reliability and efficiency.

1.3 Thesis contributions and outline

This thesis aims to supplement the existing research efforts towards the development of safe and dependable ITSs. In the scope of this dissertation, we present first a comprehensive overview of the state-of-the-art of efficiency- and reliability-enhancing mechanisms of ITSs in both railway and road transportation, which have been considered relevant and established over the past few years, followed by in-depth analysis of the selection of existing works. Second, we address the design of control mechanism in rail transport to efficiently control rail traffic, as the autonomous train is the most emerging applications of autonomous vehicles. In this context, we propose an *enhanced train-centric communication-based train control system* for railway transport. This system allows improving the quality and enhancing reliability of the train control. To guarantee safe operation of the proposed control system, we implement a new safety-checking approach based on process algebra, which aims to track and correct in real-time the train behavior. In order to demonstrate the effectiveness of our proposal, we analyze its safety level. In addition, we evaluate the performances of proposed mechanism through intensive simulations in terms of important metrics with comparison to conventional systems. We propose in the next part of this thesis, our second contribution that manifests itself in the proposition of *a discordant safety messages detection strategy in connected vehicles environment*. Our solution is a decentralized model-based approach providing the vehicles with the ability to quickly and preemptively identify discordant messages and hence dealing against potential disturbances, while ensuring a trade-off between efficiency and safety. Moreover, among the advantages of this approach are its ability to detect various attacks types, namely, Denial of Service (DoS), dropping, and flooding attacks. The proposed technique is based on data anomaly detection using Gaussian distribution approach. We carry out a formal evaluation to evaluate the effectiveness of our approach regarding important criteria, where the obtained results show that our approach offers effective results. Moreover, we conduct simulations to evaluated the efficiency of the proposed model, where the simulation results demonstrate that the model outperforms the concurrent machine learning-based methods, and achieve a promising performance regarding high precision, accuracy, recall, and f1 score.

The remainder of this thesis is organized as follows. In chapter 2, we provide a broad overview of ITSs. We describe its architecture and main applications. We also introduce some challenges in ITSs environment and the security and safety aspects in ITSs. Chapter 2 also lays out preliminary notions about some fundamentals which our contributions are based on. In chapter 3, we present a literature review of a selection of existing works in the literature that address efficiency- and reliability-enhancing of ITSs. Precisely, we summarize the main operations of each mechanism followed by a critical discussion. Then, we provide a comparison and an in-depth analyze of the reviewed works. Chapter 4 of this thesis is dedicated to a detailed presentation of the train control system proposed for railway transportation. Chapter 5 consists of a description of our second contribution related to a discordant safety messages detection strategy in connected vehicles environment. In chapter 6, we conclude the thesis and highlight a collection of open research directions for future consideration.

1.4 List of publications

Journal papers

1. **D. Zamouche**, M. Mohammedi, S. Aissani, and M.Omar. *Ultra-Safe and Reliable Enhanced Train-centric Communication-Based Train Control System*. Journal of Computing (Springer Publisher), 2021.

2. **D. Zamouche**, M. Omar, M. Mohammedi, and S. Aissani. *Highly Efficient Approach for Discordant BSMs Detection in Connected Vehicles Environment*. Submitted to Journal of Wireless Networks (Springer Publisher), 2021.

3. M. Mohammedi, M.Omar, **D. Zamouche**, K. Louiba, S. Ouared, and K. Hocini. *Energy-Aware Key Management and Access Control For The Internet of Things*. Journal of World Wide Web (Springer Publisher), 2021.

Conference paper

1. **D. Zamouche**, S. Aissani, K. Zizi, L. Bourkeb and M. Omar. *A Behavioral Modeling-based Driver Authentication Approach for the Smart Cars Self-Surveillance*. Submitted to the 13^{th} International Conference on Ubiquitous and Future Networks, Barcelona, Spain, 2022.

Seminar

1. **D. Zamouche**. New Train-Centric Communication-Based Train Control System For Safe Rail Traffic. LIMED laboratory, February 2020.

Chapter 2

Theoretical Background

2.1 Introduction

In the last few decades, a rapid emergence of Intelligent Transportation Systems (ITSs) has been perceived. An increasing interest from governments as well as private entities has led to an attractive diversity of contributions in this wide research area [53]. ITSs are expected to alleviate the problems related to transportation such as roads congestion and fatalities. ITSs applications are widely deployed and used nowadays. In this chapter, we give a background on the area of ITSs. This chapter is organized as follows. In Section 2.2, we provide a broad overview of ITSs and describe its architecture and applications. In section 2.3, we present enabling technologies for ITSs. We discuss in Section 2.4 some challenges in ITSs. In Section 2.5, we discuss the security ans safety aspects in ITS that should be fulfilled. In section 2.6, we present a brief background on the notions that will be used in our contributions, which are process algebra and Gaussian distribution approach. Finally, we conclude this chapter in Section 2.7.

2.2 Intelligent Transportation Systems

In 2016, the worldwide vehicle population has exceeded one billion for the first time in the history according to Ward's research [86]. By some estimates, the total number of vehicles worldwide is expected to double further and reach 2.5 billion by 2050 [102]. Accordingly, road traffic congestion and road fatalities are expected to increase. According to the global status report on road safety, launched by World Health Organization (WHO) in 2018 [3], it is highlighted that the number of annual road

traffic deaths and road traffic injuries have reached, respectively, 1.35 and 50 million. Therefore, such road fatalities call for the development of efficient and reliable solutions, concreted by ITSs. ITSs have emerged as solution for transportation problems to make transport safer, efficient, and more sustainable. The term "*Intelligent Transportation Systems*" means the application of Information and Communication Technologies (ICT) to the transportation domain. The United States Department of Transportation (US DoT) defines ITS as *"the electronics, communications or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety and mobility and enhance productivity"* [7]. Also, accordingly to ITS America, ITSs are defined as *"a broad range of diverse technologies, which holds the answer to many of transportation problems. ITS is comprised of a number of technologies, including information processing, communications, control, and electronics. Joining these technologies to our transportation system will save lives, save time, and save money"* [5]. Hence, ITSs provide innovative services that can be applied in every transportation mode and used by both passenger and freight transport.

2.2.1 ITS architecture

The National ITSs Architecture is introduced in the United States ITS program which was created by Congress in the Intermodal Surface Transportation Efficiency Act of 1991, and is administered by the US DoT [81]. The program uses advanced electronics to improve traffic safety, decrease congestion, facilitate the reduction of air pollution, etc. The National ITSs Architecture provides a common framework for planning, defining, and integrating ITSs [65]. This architecture defines functions that are required for ITS, physical entities or subsystems where these functions reside, and information flows and data flows that connect these functions and physical subsystems. The architecture framework is described in Figure 2.1. It is comprised of three layers including, namely, the Institutional layer and two technical layers which are Transportation layer and Communication layer.

- The Institutional layer includes the institutions, rules, methods, process, and policies that are required for effective implementation, operation, and maintenance of an ITS. This layer is placed at the base because solid institutional support and effective decisions are prerequisite to an effective ITS program. This is where the objectives and requirements for ITSs are established.
- The Transportation layer is where the transportation solutions are defined in terms of the subsystems and interfaces, the underlying functionality, and data

definitions, which are required for each transportation service. This is the core layer of the architecture.

- The Communications layer provides the accurate and timely exchange of information between systems to support the transportation solutions. Hence, vehicular networks belong to this layer.

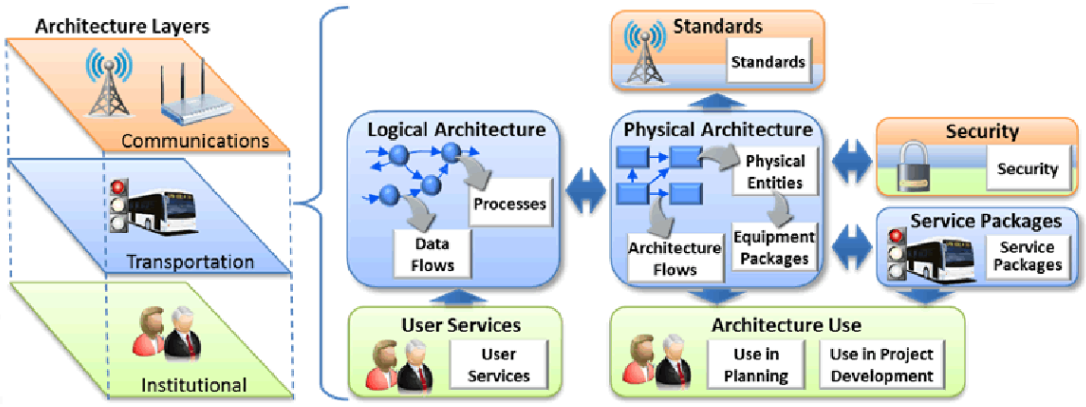

Fig. 2.1: The national ITS architecture.

2.2.2 ITSs applications

ITSs provide two types of applications related to the safety and efficiency of traffic that depend on the exchange of information between vehicles or between vehicles and RoadSide Units (RSUs). For this, computer technology and wireless communication devices are used. According to their usages, this applications can be classified into two types of ITS applications, namely: safety applications and non-safety applications. In what follow, we provide an overview of services provided by each type [40], [20], [77].

2.2.2.1 Safety applications

In particular, safety applications have gained more attention since they are considered as the original motivation behind ITSs. Safety applications are one of the most important applications which decrease significantly the number of road accidents. These applications have a significant role in preserving the life of the driver and passengers as well as the vehicle itself. This type of applications uses information that

vehicles collect from neighboring vehicles to assist a driver to prevent collisions with other vehicles, and they can be useful in many scenarios. In the following, we briefly describe some applications. In Table 2.1, we give a brief summary of communication requirements regarding these safety applications such as transmission mode, allowable latency (ms), and the maximum range (m).

- **Cooperative forward collision warning application:** is intended to aid drivers avoid crash into rear-end of vehicles in front. The message will be sent to all vehicles in surrounding area (single-hop) and over multi-hop distance. Each vehicle receives velocity, position, yaw rate, heading, and acceleration information of all the neighboring vehicles. Then, this data with road map data are used by the vehicle to ascertain a possible rear-end crash with the front vehicle. Vehicle will also resend the beacon including its data to other neighbors. The maximum required range for this application is usually around 150 m with latency less than 100 ms.

- **Lane change warning application:** lane changing maneuvers are prone to be hazardous. This application type helps avoidance of collisions when a driver is in the process of making a risky lane change. Whenever a lane change signals is used, the application will process the information it has and then determine if the space between vehicles is sufficient for the maneuver. In the case where the space is not sufficient, the application will notify the driver about the danger of changing the lane. This application is also included in the list of high priority applications. The maximum required range for covering is usually 150 m with latency less than 100 ms.

- **Blind spot warning application:** this application works in the similar way as the lane change warning application. It is designed to avoid collisions by informing the driver with the existence or nonexistence of vehicles in the blind spot while trying to change the lane. The requirement of this application is similar to lane changing application.

- **Visibility enhancement application:** as the name implies, this application is designed to enhance visibility in different situations e.g. fog, heavy rain, snow storm etc. The system either detects such situations automatically or is triggered manually by the driver. The application uses obtained heading, velocity and position of neighboring vehicles with vehicle's own information taken from Global Positioning Systems (GPS) and map database for enhancing visibility. The range

of cover for this safety application is usually around 300 m with the latency less than 100 ms.

- **Cooperative vehicle-highway automation application (Platoon):** this application enables cooperative vehicle-highway automation system for vehicles on the highway. It makes use of vehicular data and position information along with map data to make vehicle platoon/s which is helpful in improving road service i.e. traffic flow and capacity. The range of cover for this application is around 100 m with the latency less than 20 ms.

- **Highway merging assistance application:** is intended to alerts a driver regarding any merging vehicles. Through its navigation system, the merging vehicle determines if it is on a highway on-ramp. If on an on-ramp, it alerts the other vehicles by broadcasting periodic messages. he effective communication range for this safety application is usually around 250 m and the latency should less than 100 ms.

- **Pre-crash warning application:** if a crash is unavoidable, the vehicle involved will broadcast a pre-crash warning signal to neighboring vehicles, so that nearby drivers have more time to react, which may plausibly avoid a fatal pileup accident. The effective coverage of this application is 50 m with latency of less than 20 ms.

- **Highway/rail collision warning application:** this type of application is designed to provide safety at highway/rail intersections. RSU will be deployed near such intersections that can alert vehicles in the vicinity of approaching train (V2I communication). Alternately, train can send messages to other approaching vehicles (V2V communication). The range of coverage area for this application is around 300 m and the latency should be less than 1000 ms.

Some safety applications require to transmit messages periodically (e.g. every 100 ms), whereas other safety applications transmit messages when an event occurs [101]. Safety applications analyze the incoming messages and provide the necessary action. Therefore, safety messages can be categorized into two groups, namely: (*i*) periodic messages that are transmitted for awareness and (*ii*) event-driving messages that are event messages triggered by unsafe situations. A scenario showing the transmissions of periodic messages and event-driving messages is depicted in Figure 2.2.

1. **Periodic messages:** an important type of periodic messages is *Basic Safety Messages (BSMs)* [61]. The main objective of BSM messages is to inform a

Application	Transmission mode	Allowable latency (ms)	Maximum range (m)
Cooperative forward collision warning	Periodic	100	150
Lane change warning	Periodic	100	150
Blind spot warning	Periodic	100	150
Visibility enhancement	Periodic	100	300
Cooperative vehicle-highway automation (Platoon)	Periodic	20	100
Highway merge assistance	Periodic	100	250
Pre-crash warning	Event-driven	20	50
Highway/rail collision warning	Event-driven	1000	300

Table 2.1: Safety applications with their requirements [20], [77].

certain group of vehicles that are located in interesting region of any unexpected events causing undesirable consequences on the road. This message contains necessary information of vehicles such as position of vehicle, speed, acceleration, heading, wheel angle, etc. Additional information may be added to the messages if desired by the sender. These messages are transmitted periodically in single hop broadcast mode usually in range of 300 m around the vehicle. Vehicle can avoid unsafe situation by processing these messages before it happens.

2. **Event-driving messages:** also called *emergency messages*, are transmit to neighboring vehicles if an incident/unsafe situation has been detected. Upon detection of such typical emergency situation, this category of information are accordingly transferred in multi-hop broadcast. Therefore, if there is no accident occurred, this type of messages will not be generated. Event message has the highest priority for vehicle to process and usually, it contains location, time, and the event type.

2.2.2.2 Non-safety applications

Non-safety applications can also be considered infotainment applications, aim to provide comfort and satisfaction to the passengers and drivers and also make the journey more pleasant. In this type of application, two basic user-related applications are provided, which are Internet connectivity and Peer-to-Peer applications [99]. The goal behind the

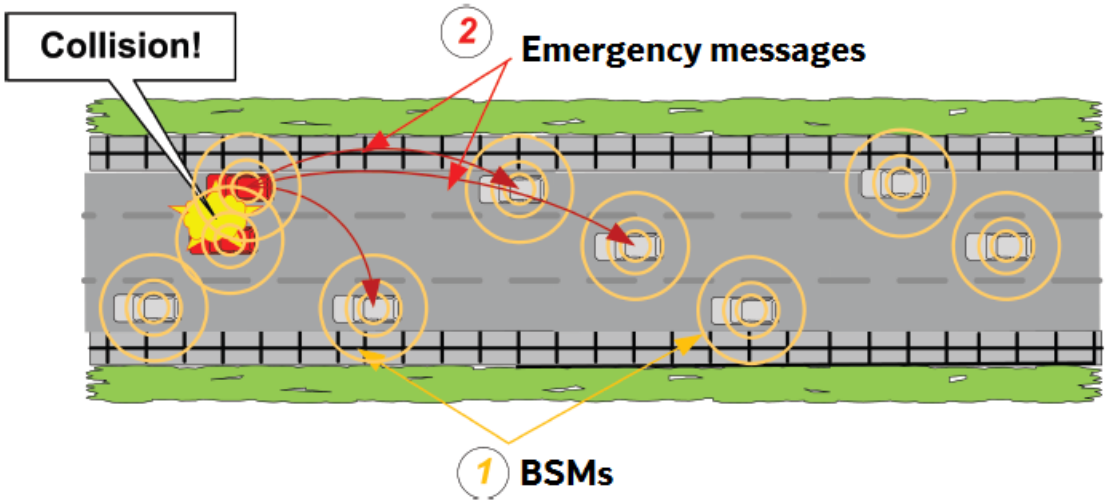

Fig. 2.2: Illustrative scenario of the exchange of BSMs and emergency messages.

first type consists of having a connection that will make all of the Internet applications available such as music and video sharing and downloading, email access, Internet games, and advertisements. The second type is to alleviate boredom during long journey. Drivers and passengers can play games, stream music or movies from special servers during long journeys, and so on. Moreover, drivers traveling together toward the same destination will be able the exchange information about possible changes regarding their itinerary. Telematic applications are also useful for drivers, enabling payment services for parking occupancy, to access distance help from a mechanic service via a wireless diagnosis in case mechanical emergencies. Other location-based applications pertain to find drivers points of interests such as hotels, restaurants, nearby fuel station, touristic places, etc.

2.3 Enabling technologies for ITSs

One of the main priorities of different countries of the world is to improve safety, reliability, and quality of transport services. Consequently, there is a high effort in development of ITSs that can ensure traffic safety and reduce negative effects on environment. Recent information technologies advances and technical development have made possible the creation and usage of integrated intelligent systems [48]. Connected and Automated Vehicles (CAVs) and communications in vehicular networks are the promising technologies that provide significant opportunity to make our transportation

safer, greener, and smarter [11], [66]. Modern vehicles have computing capabilities and support wireless communications to share information among them and with infrastructures thereby increasing vehicles perception of their surroundings.

2.3.1 Connected and automated vehicles

Connected and automated vehicles have been an important point for the ITSs for a while already, based on their ability to support a wide range of ITSs applications [93]. The term "connected and automated vehicle" can refer to a variety of technologies currently being implemented to improve travel and enable a vehicle to assist in the task of driving. Figure 2.3 illustrates a typical CAV. the latter mainly consists of three components, namely, sensors, mapping, and communication system. Vehicles contain of a number of sensors used in the perception of the external environment such as infrared, radar, GPS, accelerometer, gyroscope, LIght Detection And Ranging (LiDAR) and cameras. Infrared sensors are used at night for the detection of animals and other vehicles, while the radar sensors are used for measuring the range and velocity of vehicles. The vehicle's position and changes in the speed as well as the directions are determined, respectively, by GPS, accelerometers and gyroscopes. Finally, LiDAR is one of the most expensive sensors using lasers and photoreceptor to produce a three-dimensional model of the surrounding environment. Mapping, usually use files containing points and lines of the road, photographic images from the streets of satellites, ground pictures from the streets, as well as traffic control devices and obstacles. The mapping may contain the forms of terrain that are obtained by LiDAR. Communication system is a very important component that enable vehicles to exchange relevant traffic information with neighboring vehicles within transmission range.

2.3.2 Dedicated Short-Range Communication (DSRC) spectrum

Dedicated Short Range Communication (DSRC) is considered as short-range wireless communication technology which particularly made for Vehicles to Vehicles (V2V) and Vehicles to Infrastructure (V2I) communications in order to enhance the productivity and safety of the transportation system. Moreover, DSRC enables data transmission in ITSs environment for both safety and non-safety applications. DSRC was originally proposed to work in the 915 MHz band; however, United States Federal Communications Commission (FCC) in the year 1999 allocated 75 MHz of frequency spectrum in the band 5.9 GHz for DSRC within ITSs [1]. The DSRC spectrum is divided into seven

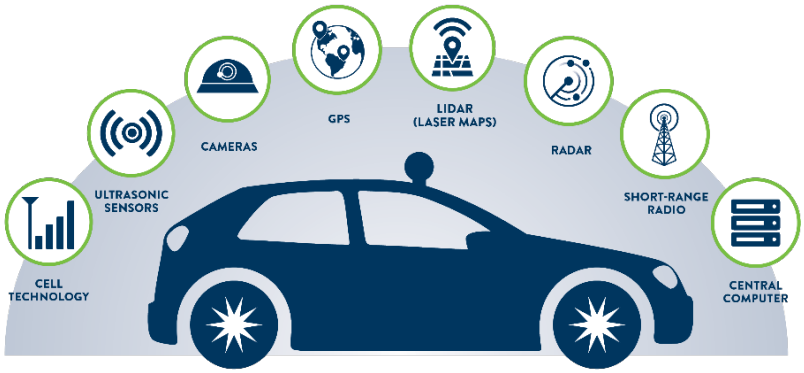

Fig. 2.3: Typical connected and automated vehicle.

10 MHz channels from Channel 172 to 184, including one Control Channel and six Services Channels with a 5-MHz guard band at the low end as illustrated in Figure 2.4. The Control Channel 178 was assigned for carrying high-priority short messages and management information. The FCC in the year 2006 designated Channel 172 for safety applications involving accidents avoidance and mitigation for public safety of life, while Channel 184 is for high-power public safety longer distance communications to be used for public safety applications including intersection collision mitigation. The communication range of DSRC system is up to 1000 meters, where vehicles may be moving at speed up to 140 km/h [25].

2.3.3 Wireless Access in Vehicular Environment (WAVE) protocol

The Wireless Access in Vehicular Environments (WAVE) is a radio-communication system in ITSs that make it possible for vehicles and infrastructures to communicate with each other. In 2004, the IEEE task group TGp developed an amendment to the IEEE 802.11 standard to include vehicular environments [100]. The IEEE 1609.1 standard for WAVE resource management describes an application that allows the interaction of OBUs with limited computing resources and complex processes running outside the OBUs in order to give the impression that the processes are running in the OBUs. The IEEE 1609.2 standard defines secure message formats and the processing

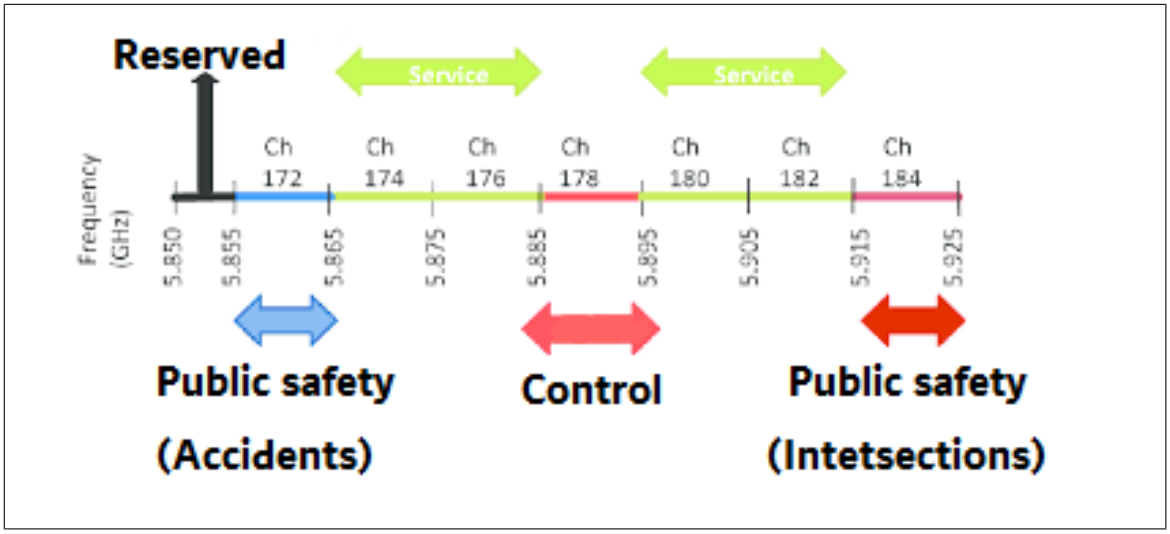

Fig. 2.4: DSRC Spectrum allocated by FCC.

of those secure messages in the WAVE system. It covers methods for securing WAVE management and application messages, with the exception of vehicle-originating safety messages. WAVE Short Message Protocol (WSMP) is used by IEEE 1609.3 networking services in Control CHannel and Service CHannel to enable communications with a maximum payload of 1400 bytes. WSMP allows WAVE-aware devices to directly control physical characteristics (channel number and transmitter power) [51]. Finally, Multi-channel operation IEEE 1601.4 Provides enhancements to the IEEE 802.11p MAC to support multichannel operation. To sum up, IEEE 802.11p WAVE is only a part of a group of standards related to all layers of protocols for DSRC based operations which concerns to physical and MAC layers. Figure 2.5 illustrates the WAVE protocol stack.

2.3.4 Communication infrastructures

The basic concept of ITSs can be designated as the capabilities of sharing particular information among vehicles in order to support a large set of applications intended to enhance transportation quality, more particularly safety. Vehicular communications are the promising tools that can provide facilities for exchanging and sharing information in the wireless vehicular network. In this context, vehicles such as cars, buses, trains, motorcycles, and even pedestrians are equipped with network interfaces. Infrastructures can also cooperate with vehicles and participate in the communication process in order to provide better coverage. At the core of these ITSs, the communication between the

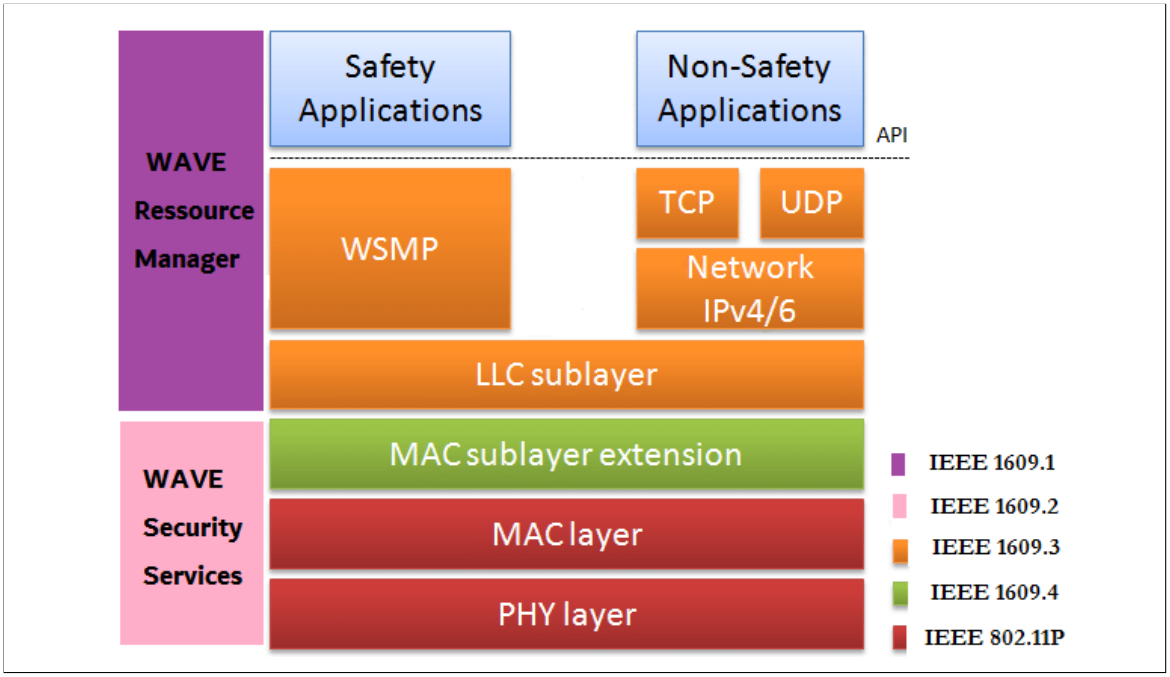

Fig. 2.5: Illustration of WAVE protocol stack.

vehicles will be covered under the Vehicular Ad hoc NETwork (VANET) [103]. VANETs incorporate two types of communication [14], namely: (1) external communications for V2V and V2I communications, and (2) Inter-Vehicular Communications (IVC). Figure 2.6 illustrates ITSs scenarios exploiting vehicular communications.

- **V2V communications:** through V2V communications, vehicles can exchange relevant information with neighboring vehicles within their transmission range without involving fixed infrastructures. Enabling safety-related services is the key application of V2V communications. Vehicles can exchange real-time information among them over a wireless network such as vehicle's speed, length, position, etc., which offer the possibility to prevent critical accidents.

- **V2I communications:** it has been designed to allow the communication of moving vehicles with fixed infrastructures, also defined as RSUs. By deploying RSUs in vehicular networks, V2I communications allow vehicles to access to Internet allowing passengers to browse the web while moving and benefit from various Internet services. V2I support also traffic efficiency as well as safety-related services. For instance, the drivers can receive from RSUs real-time information to a specific road segment in order to prevent from bad weather conditions (e.g. fog, ice, snow and rain).

- **Internal Communications:** embedded electronic components, called electronic controls units, are considered an important part of the modern vehicles' architecture [98]. These electronic controls units monitor and control the different subsystems of a vehicle. They are interconnected through several sub-networks that compose the global internal network of the vehicle. There are five most widely used in-vehicle networks in modern intra-vehicle communication systems [117], namely, LIN (Local Interconnection Network), CAN (Controller Area Network), FlexRay, Ethernet, and MOST (Media Oriented Systems Transport).

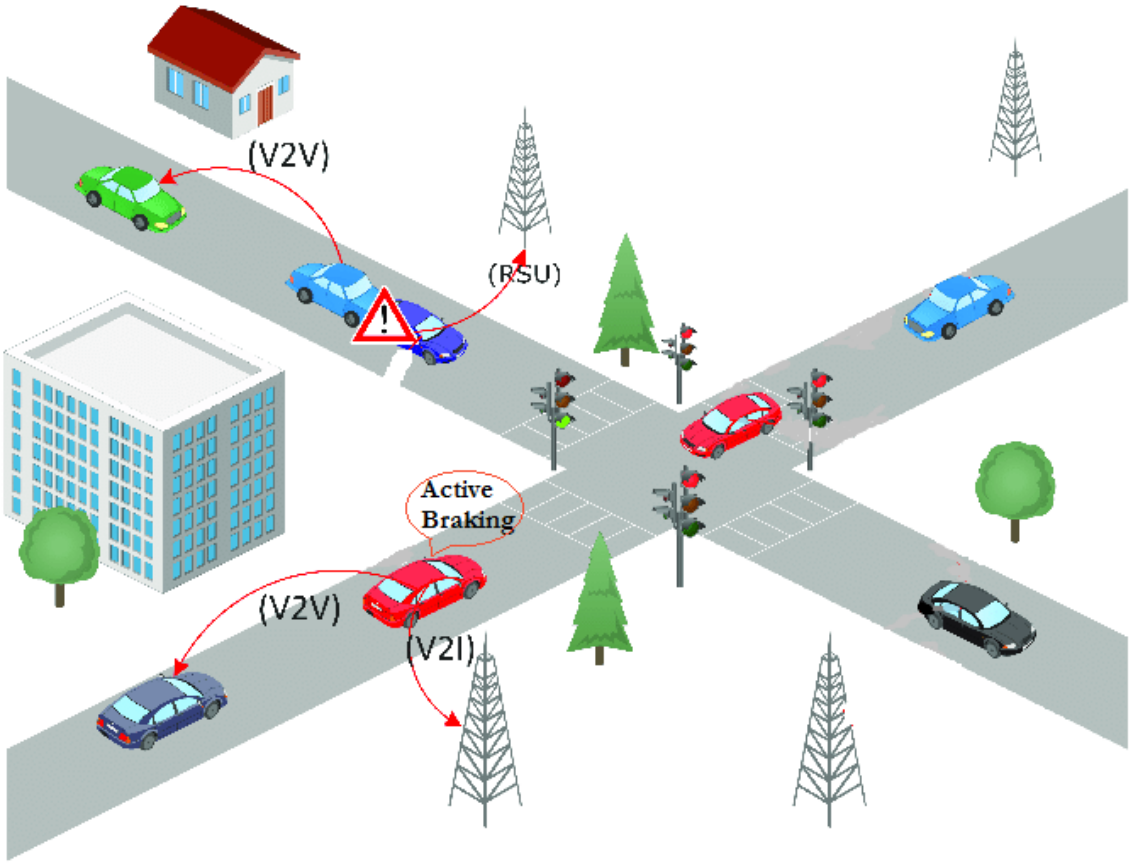

Fig. 2.6: Vehicular communications in ITS.

2.4 ITS environment challenges

The ITSs environment owns several characteristics that require addressing a wide range of challenges for the fast and proper deployment of a system. The core challenges for

ITS deployment in the railway and road transportation are, namely, real-time nature of applications, high mobility of vehicles and dynamic network topology, unbounded and scalable network, intermittent connectivity, security issue, railway circumstances, and road and traffic pattern and conditions. In what follow, we describe each challenge.

- *Real-time nature of applications:* most of the safety-related applications require vehicles to receive real-time data for promptly driving decisions. Therefore, any delay in traffic information delivery may have serious consequences on the road users and the vehicles itself. This hard time constraints are more challenging in case of high traffic density.

- *High mobility of vehicles and dynamic network topology:* the high-speed movement of vehicles makes network topology change dynamically and affects accordingly its spatio-temporal connectivity. Due to the high mobility, the connection duration among vehicles are limited, consequently, the exchanged information is limited. Therefore, vehicular mobility creates great difficulties in designing ITSs applications.

- *Unbounded and scalable network:* the scale of vehicular networks can reach thousands of vehicles particularly in urban areas. Indeed, this creates difficulties in management and also the channel congestion problem due to limited bandwidth while there are a large number of vehicles communicating with high data rate.

- *Unreliable and uncertain nature of connectivity:* the most important problem is the intermittent connectivity among vehicles caused by high mobility and highly network topology change. The high dynamics of vehicles combined with usage of short-range communications make the connectivity among the vehicles very unstable, so even the best effort service cannot be guaranteed. Moreover, vehicles may join and leave the network at any time, which makes the connectivity transient.

- *Security issue:* advancements made in ITS and the new technologies being introduced to roadways and infrastructure bring additional challenges [78]. Increasing integration of loosely secured devices and applications with the transportation systems present opportunities for attackers to exploit these systems. Attacks on ITS have implications within the physical world and can result in damage to infrastructure, delay of emergency response, fatalities, and even threats to national security [49].

- *Railway circumstances:* rail transportation is subject to many and unavoidable challenges. These challenges are due to internal factors such as driving the train, performance of the equipment, failures, temporary restrictions, etc. and external factors such as passengers, weather, vegetation, and so on to the systems. Some of these factors are linked to extraordinary events (for example an insulation fault on a track circuit), others relate to everyday phenomena. Controlling these phenomena is a sure key to improving the performance of a railway line [87].

- *Road and traffic pattern and conditions:* vehicles movements on road and highways generally follow certain pattern governed by streets such as speed limits, traffic lights, etc. Such patterns influence the vehicles propagation and, consequently, the information dissemination. For instance, in urban environment, communications are subject to Non Line Of Sight (NLOS) situations where road obstacles such as cities and buildings, and so on between transmitter and receiver obstruct the radio signal, which degrade the performances of ITSs applications.

2.5 Security and Safety aspects in ITSs

Safety is defined as freedom from unacceptable risk because zero risk is unattainable [9]. Although zero risk is an ideal to pursue, its attainment is likely to be an impossible mission. The realistic expectation is to master the risks and dangers to deal with malfunctions within a system where such malfunction will lead to a dangerous situation. Operation safety is a means for guaranteeing reliability towards specific errors in the entire system (hardware components and software) or as a guaranteed reaction, i.e., reaching a safe state [56]. Operation safety of ITSs can be interpreted as that the vehicles react correctly and at the right time, regardless of the risks that occur. To comply with the operation safety of ITSs, it is a matter of carrying out an improvement or real-time control of the safety systems by development and integration of methods useful for the detection of critical situations affecting the proper operation of vehicles. On the other hand, the most safety-related applications rely on sharing safety-critical and time-constrained information among vehicles. Given their importance, they are particularly highly demanding in terms of security and reliability of information reception. Moreover, they are drastically sensitive to delays. For instance, when an accident occurs, the safety information must be delivered accurately and on time respecting the delay constraint in order to prevent any road hazards from happening. Nevertheless, vehicular communications encounter security threats that can result not only in data losses or network dysfunctions but also in fatal accidents. These problems

can be avoided if security mechanisms account for the main security requirements such as privacy, authentication, integrity, availability, etc. Therefore, security and safety are of the most important in ITSs deployment because accidental risks will be addressed by safety mechanisms and intentional risks will be countered by security mechanisms.

2.6 Fundamentals of the contributions

In this part, we introduce a brief background on the notions that will be used in our contributions, which are process algebra and Gaussian distribution approach.

2.6.1 Formal modeling

Formal Modeling is the process of describing a system (a set of interconnected components performing desired operations) in a well defined formal syntax and semantics language, which can improve the completeness and consistency of the system design [37]. The formal modeling provides a way for logical reasoning about the system's operation and this achieves precise description and allows a stronger design that satisfies the required properties. There are a variety of modelling formalisms that are used such as process algebra, petri nets, finite state machine, temporal logic, etc. These methods can achieve complete exhaustive coverage of the system thus ensuring that undetected failures in behavior are excluded [12]. In what follow, we describe briefly each formalism.

- **Process algebra:** process algebras can be represented as labeled transition systems for specifying the behavior of the system. The most commonly used formalisms are Conditional Basic Process Algebra ($CBPA^{*}_{0,1}$) [44], Calculus of Communicating Systems (CCS) [22], Communicating Sequential Processes (CSP) [52] and Pi-calculus [75]. The probabilistic modeling of the system is mostly performed by enhancing the semantics of process calculus formalisms.

- **Petri nets:** petri nets are used as framework for specifying the concurrent systems with detailed (mathematical and conceptual) basic semantic for their modeling. The petri net model has a powerful capability to model events and states in a distributed system and to capture sequential, concurrency and event-based control [33].

- **Finite state machine:** finite State Machine (also known as finite state automaton) is a predefined state machine with specific transitions. It has a finite set of

states with a start state and accepting states, and a set of state transitions for describing the specific problem [76].

- **Temporal logic:** temporal logics modify traditional modal logics to allow description of when a formula is true. That is, rather than just "necessity" or "possibility", a formula may be true at the next point in time or at some point in the future [63].

Different from the formal methods described above, process algebra provides an intuitive correspondence between formal processes and real processes and is distinguished by their modular aspect which makes it possible to considerably reduce the complexity of the specification of systems. Therefore, our first contribution focuses on formal modeling of train control system's operation and based on CBPA method. We have opted for CBPA formalism because of its ability to specify systems' operation and safety properties. Furthermore, the IEEE standard [90] for the functional exigences of trains control systems, which we have considered, requires a safety policy without communications.

2.6.2 Process algebra CBPA

Process algebra is a mathematical tool used for formally describing the systems behavior [108], which provides a simple use and allowing to study the system behavior. It is based on a non-empty set contains a set of actions of the system, an operator + for alternative composition of processes, and a binary operator . for sequential composition of processes.

Basic Process Algebra ($BPA^*_{0,1}$) [44], which is a framework enriched by two processes 0 and 1. Suppose that α is an action belongs to a finite set of actions and P_1, P_2 two processes belonging to a set of processes. The syntax of $BPA^*_{0,1}$ is defined such as:

$$P_1,\ P_2 ::= 0 \mid 1 \mid \alpha \mid P_1 + P_2 \mid P_1.P_2 \mid P_1^*.P_2 \tag{2.1}$$

where

- 0 indicates a process in a blocked state, where no action is performed.
- 1 indicates a process terminated successfully its execution.
- $P_1 + P_2$ represents the choice between two processes P_1 or P_2, according to the process subordinated by the following actions.

- $P_1.P_2$ represents the sequential composition of two processes P_1 and P_2.
- $P_1^*.P_2$ represents the process which executes the sub-process P_1 zero, one or many times and always ends with the sub-process P_2. $P_1^*.P_2$ is equivalent to $P1.(P_1^*P_2)+P_2$. It is an alternative between P_2, (If P_1 is executed 0 times) and $P1.(P_1^*P_2)$ (if P_1 is executed one time at least).

Conditional Basic Process Algebra ($CBPA_{0,1}^*$) [44] is an extended version of the algebra $BPA_{0,1}^*$, which allows to treat variables and conditions while specifying systems. The syntax of $CBPA_{0,1}^*$ is defined as follows:

$$P ::= 0 \mid 1 \mid c \rhd \alpha \mid P_1 + P_2 \mid P_1.P_2 \mid P_1^*.P_2 \tag{2.2}$$

where

- $c \rhd \alpha$ indicates a process that performs the action α if condition c is satisfied.

Definition 1: Given two processes P and Q, $P \sqcap Q$ represents the greatest common factor between the two processes P and Q, it is the least restrictive process included in both P and Q. If α and β are elementary actions, P, Q and R three processes, 0 the blocked or finished process, we can formally define the operator $\sqcap$ by induction as follows:

- $P \sqcap 0 = 0$.
- $P \sqcap P = P$.
- $\alpha.P \sqcap \alpha.Q = \alpha.(P \sqcap Q)$.
- $\alpha.P \sqcap \beta.Q = 0$.
- $P \sqcap (Q + R) = (P \sqcap Q) + (P \sqcap R)$.

The computation of the $P \sqcap Q$ is done by using the notion of derivatives introduced in [27], which are defined below.

Definition 2: The derivative of a process P with respect to an action α, denoted by $\partial_\alpha(P)$, is the process that remains to be executed after having executed the action α. Thus, the derivative is defined as follows: $\partial_\alpha(P) = \{P' | P \xrightarrow{\alpha} P'\}$.

Definition 3: The function $\delta(P)$ defines the set of actions by which a process P can start its execution. Thus, this function is defined as follows: $\delta(P) = \{\alpha | \exists P' \wedge P \xrightarrow{\alpha} P'\}$.

Axioms: Axioms related to Boolean expressions are given , where false is denoted by $\perp$ and true is denoted by $\top$:

- $\neg\top = \bot$.
- $\neg\bot = \top$.
- $\top \wedge \alpha = \alpha$.
- $\bot \wedge \alpha = \bot$.
- $\top \vee \alpha = \alpha$.
- $\bot \vee \alpha = \alpha$.
- $\alpha \wedge \beta = \beta \wedge \alpha$.
- $\alpha \wedge (\beta \wedge \gamma) = (\alpha \wedge \beta) \wedge \gamma$.
- $\alpha \vee \beta = \beta \vee \alpha$.
- $\alpha \vee (\beta \vee \gamma) = (\alpha \vee \beta) \vee \gamma$.

Where $\{\neg, \vee, \wedge\}$ is connectives: $\neg$: not, $\vee$: or, and $\wedge$: and.

2.6.3 Formal validation

Formal validation is a powerful technique for checking that the operation of a given mechanism is free from errors. It aims at improving the quality of the requirements and increasing the confidence that the categorized requirement fragment and its corresponding formalized counterpart meet the design intent [35]. By exhaustively exercising possible execution scenarios of the systems, formal validation can detect subtle errors that are missed during simulation, where only a small fraction can be checked for correctness [46]. It consists of the definition of a series of validation problems and the analysis of the results given by an automatic validation check. The problems include three main types of checks, namely, checking logical consistency, scenario compatibility, and property entailment [35]:

- *Logical consistency:* to formally verify the absence of logical contradictions in the considered formalized requirement fragments. It is indeed possible that two formalized requirement fragments mandate mutually incompatible behaviors.
- *Scenario compatibility:* to verify whether a scenario is admitted given the constraints imposed by the considered formalized requirement fragments. Intuitively, the check for scenario compatibility can be seen as a form of simulation guided by a set of constraints. The check for scenario compatibility can be reduced to the problem of checking the consistency of the set of considered formalized requirement fragments with the constraint describing the scenario.
- *Property entailment:* to verify whether an expected property is implied by the considered formalized requirement fragments. This check is similar in spirit to model checking, where a property is checked against a model. Here the considered set of formalized requirement fragment plays the role of the model against which

the property must be verified. Property checking can be reduced to the problem of checking the consistency of the considered formalized requirement fragments with the negation of the property.

2.6.4 Gaussian distribution approach

Gaussian distribution (also known as normal distribution) is a bell shaped curve, and it is assumed that during any measurement values will follow a normal distribution with an equal number of measurements above and below the mean value [38]. A Gaussian distribution is shown in Figure 2.7. When measuring a value, the statistical operation that are the mean (μ) and standard deviation (σ) are calculated, and then determine the Probability distribution. The "mean" is the average of all values. The "standard deviation" represents the average deviation of an individual value from the mean value. Mean value is defined as

$$\mu(X) = \frac{x_1 + x_2 + x_3 ... + x_n}{n} \tag{2.3}$$

where, $x_1, x_2, x_3, ..., x_n$ are individual values of X and n is the number of values. After calculation of the mean value, standard deviation is determined using the following formula

$$\sigma = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu) \tag{2.4}$$

Afterwards, the probability distributions is determined as follow

$$P(X) = \sqrt{2\pi\sigma^2}^{-1} \cdot exp^{-(X-\mu)^2/2\sigma^2} \tag{2.5}$$

2.7 Conclusion

In this chapter, we setup the context for ITSs. First, we have introduced the ITSs as well as their architecture and applications. We have then presented the technologies enabling the development of ITSs. Afterwards, we have introduces the main challenges in ITSs environment. In other part of the chapter, we have discussed the main requirements in terms of security and safety aspects. Finally, we have presented a brief background on the notions that will be used in our contributions, which are process algebra and Gaussian distribution approach. The aim of the next chapter is to present a state of the art on security and safety approaches of ITSs proposed in the literature.

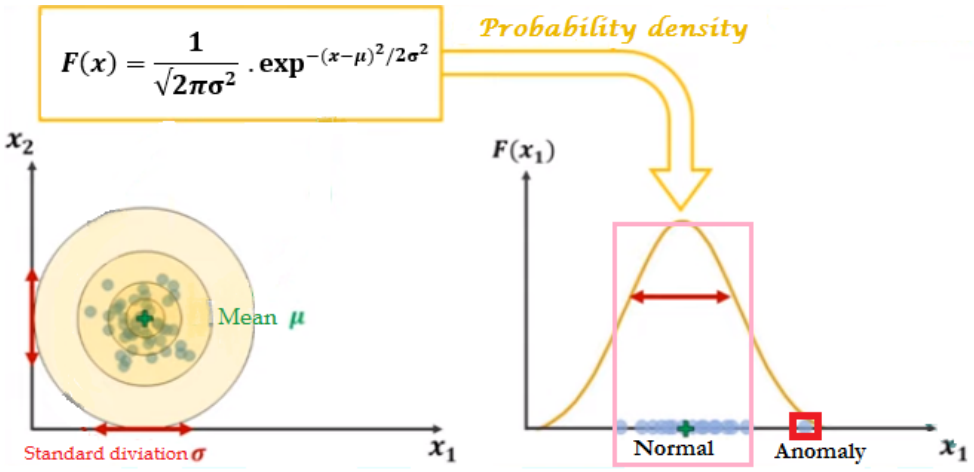

Fig. 2.7: Gaussian distribution.

Chapter 3

Literature Review of Security and Safety Approaches of Intelligent Transportation Systems

3.1 Introduction

Security and safety are an extremely crucial feature in Intelligent Transportation Systems (ITSs). Numerous research papers have been carried out on security and safety of ITSs because of their omnipresence in everyday life and their importance to economic and environment. The purpose of this chapter is to provide a survey of some works judged relevant and recently proposed in the literature for railway and road ITSs. First, we present a taxonomy, which classifies the selected security and safety solutions. Then, we provide a comprehensive literature review in which we summarize the main operations of each work and discuss some advantages and shortcoming, followed by an overall comparison of all the reviewed solutions as well as a synthesis. Finally, we set out the principle of the solutions that we propose by positioning them compared to prior researches.

3.2 Classification

To achieve the security and safety characteristics in ITSs, researchers have proposed some techniques. These security and safety mechanisms play an important role in ensuring safer and reliable ITSs operation. After analyzing the works collected, it appeared to us that a classification was necessary in order to list the different methods

followed. We illustrate in Figure 3.1 our taxonomy of the most relevant and recent works. We have classified the reviewed security and safety approaches into two main categories, namely, approaches for railway ITSs and approaches for road ITSs. In what follow, we detail each category.

1. **Railway ITSs:** the occurrence of railway accidents has seen a sharp increase and constitutes an important issue affecting railway transport safety. Dealing with the occurrence of this scourge is of paramount importance. A great deal of researches have been carried out and is still in progress to address the operation safety requirements in rail traffic. In this chapter, we present an in-depth study of some relevant researches and recently proposed in the literature to satisfy the requirements of smooth operation of intelligent railway systems. Based on the methods followed, we divide the proposed mechanisms for Railway ITSs in two main categories, namely, Safety monitoring-based approaches and Risks assessment-based approaches. In the following section, for each solution, we provide their operations and discussions in terms of advantages and drawbacks.

   (a) **Safety monitoring-based approaches:** safety monitoring is a helpful aspect that is introduced to ensure a reliable and safer operation of a system by making timely malfunctioning maintenance. In this category, some solutions of safety monitoring were proposed for trains control systems aiming at enhance their operation safety, where they differ by the techniques used and the degree of effectiveness of their approaches.

   (b) **Risks assessment-based approaches:** the concept of *risk analysis* was developed as risk assessment tool towards investigating both the potentiality of an undesired event and its consequences. In this type of approaches, the primary goal is selecting and studying of the factors that lead to the occurrence of an accident, and subsequently, propose solutions that could face this occurrence.

2. **Road ITSs:** the effectiveness of road ITSs depends widely on the efficient exchange of data among vehicles. However, due to the inherent characteristic of road ITSs, this information is expected to be subject to severe beaches, which impact its reliable reception. Therefore, extensive research has been conducted toward safety-related applications reliability. In this chapter, we review the most significant and recent approaches from the literature. Based on the methods followed, we divide the the proposed mechanisms for road ITSs in two main

categories, namely, Attacks mitigation-based approaches and Safety messages dissemination quality-based approaches. Likewise, for each solution, we provide their operations and discussions in terms of advantages and drawbacks in the following section.

(a) **Attacks mitigation-based approaches:** the target of the approaches belonging to this category is to mitigate attacks that compromise the reliability and efficiency of vehicular communication network. Depending on the designed solutions, this category is divided into two sub-categories: (*i*) False safety messages detection-based approaches and (*ii*) Safety messages verification prioritization-based approaches. These two sub-categories are as follow.

- **False safety messages detection-based approaches:** this type of approaches aims to guarantee that the transmitted safety messages are anomaly-free. In this context, the vehicular communication network is secured through the detection of false safety messages that are injected by disruptive vehicles to report false congestion information, false situation and location information, bogus events such as traffic accidents, etc.
- **Safety messages verification prioritization-based approaches:** accepting safety messages without signature verification could cause security issues. Hence, the messages are queued up for signature verification. Since vehicles may not be able to verify all received messages, this type of approaches proposes messages verification prioritization to granting authentication of messages in case of invalid messages signature due to malicious data injection attacks, and dealing with messages loss caused by the verification time too long of each message especially in high density traffic.

(b) **safety messages dissemination quality-based approaches:** in this category, the proposed solutions target dissemination issues of safety messages in vehicular network. The primary goal of the mechanisms belonging to this category is to ensure that the vehicles are able to communicate with neighboring vehicles with no transmission delay, low packet loss, and reduced broadcast redundancy by improving the safety messages transfer quality.

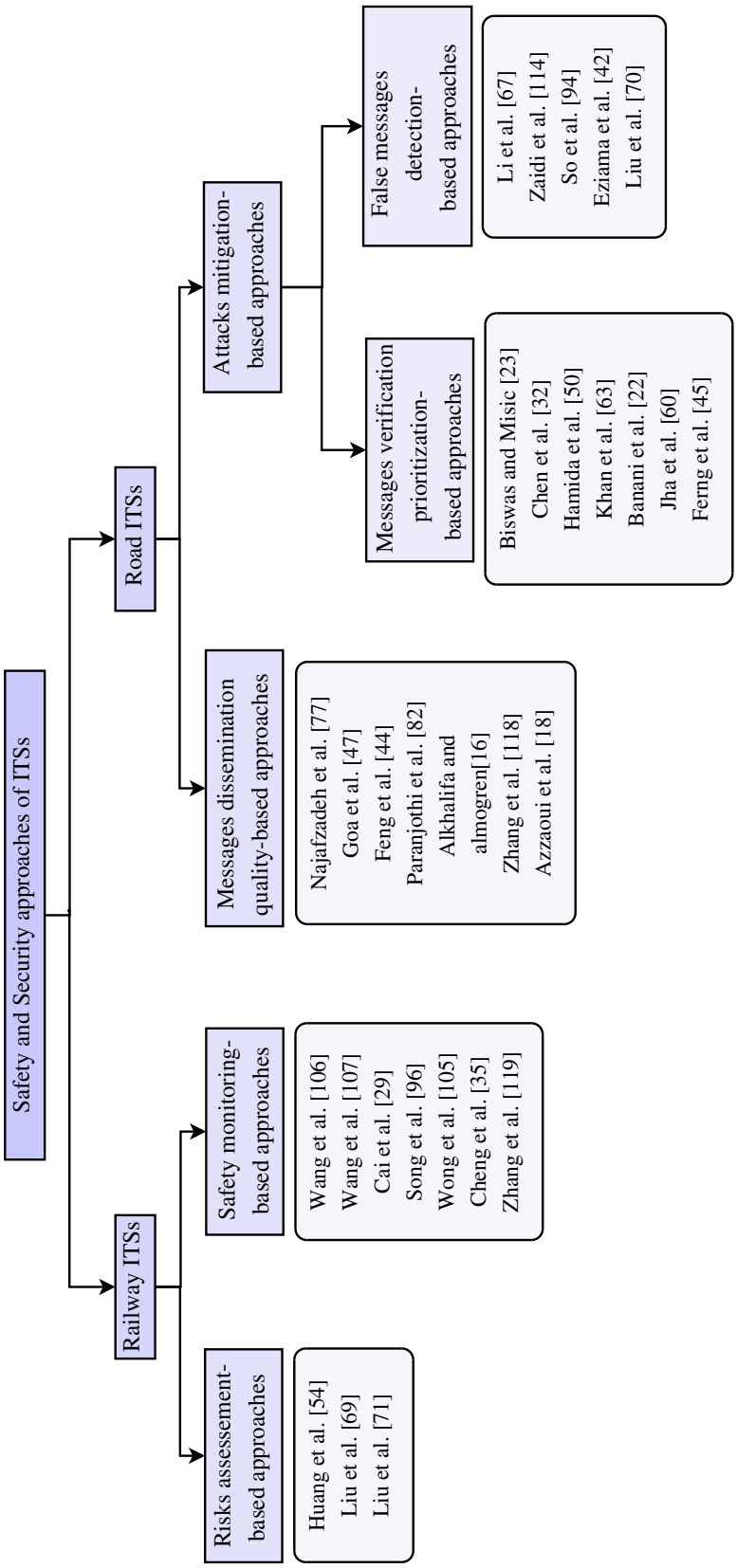

Fig. 3.1: Taxonomy of the reviewed approaches.

3.3 Critical study and overall discussion

In this section, we review from the literature some relevant and recent works, and we provide a brief synthesis of the reviewed works.

3.3.1 Railway ITSs

3.3.1.1 Safety monitoring-based approaches

Parallel Monitoring for the Next Generation of Train Control Systems

Wang et al. [106] have proposed a NGTCS, a new Next Generation Train Control System, where new technologies of parallel monitoring are integrated into the railway signaling systems. The authors aim to improves train control system efficiency and intelligence. The proposed approach lies on the adding of new functionality to the conventional signaling system, which is achieved through modifications to existing software by the use of parallel monitoring technology for control subsystems; data sharing and merging; common mode cause error avoidance, and alarms in the case of failures. It monitors the signaling system's subsystems such as tracking interval, train route setting, train speed protection, and temporary speed restriction, where, when a failure occurs in any one of the control subsystems, the parallel monitoring system triggers an alarm to alert staff of an abnormal condition. It is also able to make data comparisons and carry out data confirmation between systems. Hence, the proposed solution is interesting in the sense that it tends towards the implementation of an intelligent signaling system and improves the reliability and safety of the entire system. Nevertheless, if the system is not properly managed then there may arise some constraints in terms of communication, power, etc. Furthermore, in case of fire or emergency, the system does not alert nearby surroundings.

A Novel Train Control Approach to Avoid Rear-End Collision Based on Geese Migration Principle

Wang et al. [107] have addressed collision handling in railway transport network by proposing a train rear-end collision avoidance strategies. With the aim to avoid train rear-end collision to happen due to erroneous commands from Automatic Train

Protection (ATP) equipment or the latter is unable to ensure fail-safe in case of equipment failure, the author propose to use at the same time Centralized Traffic Control (CTC) and ATP equipments. In other words, the ATP and CTC systems cooperate to monitor the interval between two trains and generate warnings in case this interval is crossed. In the proposed approach, the authors used the geese migration theory in which, the ATP controls the train interval as goose interval, adjusting the interval between two following trains locally; while CTC controls the same as goose line to keep the formation globally. CTC act as a centralized monitor in case of emergencies. Hence, the reliability of the original system is enhanced, however, here, only a single track in single way is taken into consideration by the control system. Furthermore, it is a centralized approach where In case of purely centralized approach there is no train-to-train communication and then every train is required to send information messages to nearby stations and the acknowledgment or decision messages from stations are sent to it accordingly to detect a collision each time it occurs. Hence, the total information flow is considerably high.

System Architecture of A Train Sensor Network for Automatic Train Safety Monitoring

Cai et al. [28] have proposed a system architecture of a train sensor network for automatic train safety monitoring, named TSSN (Train Safety Sensor Network). The aim of the proposed sensor system is to provide real-time train working condition monitoring and reliability analysis by tracking and evaluating subjective and hidden danger factors. TSSN installed in the train to monitor the subsystems controlling train's equipments (include traction system, braking system, train control system, door system, etc.), and the train's performance (speed, acceleration, etc.). It consists of multiple sensor layers that monitor train's electrical and mechanical activities, a train data center and a ground data analysis server, which implements fault diagnosis based on a Failure Tree Analysis (FTA) method for a door system. It collects critical equipment state, monitors instant hazards during train traveling, and provides urgent faults instructions for driver. However, the TSSN's hardware and software structure are characterized by high development costs, any failure to collect any event data will result in failure of the whole the proposed system, and the diagnosis is not quick which will result in delay in decision making. In addition, this system increases operation and maintainability expenses.

A Train-centric Communication-Based New Movement Authority Proposal for ETCS-2

Song et al. [96] have focused on the safety of European railways European Train Control System level 2 (ETCS-2) by proposing an approach for the computation of a new type of Movement Authority (MA), which is called Movement Authority Plus (MA+). The proposed approach aims to bridge the interoperability gap between ETCS Levels 2 and 3. The MA+ is designed to be overlaid onto the current ETCS-2, to form a parallel control system, where when ETCS-2 fails, MA+ is able to protect train safety to not interrupt the train's normal operation. In Song et al.'s approach, the following train obtains through a direct communication with the preceding one the location of the latter. Subsequently, it calculates the headway, where if the current headway between them is short that the computed headway by MA+ due to any reason such as an equipment failure or an unsafe interaction between ATP and the train, the proposed MA+ will produce a fail-safe command to the driver to execute an emergency brake. Hence, two strategies are proposed to carry out the minimum train headway distance calculation: (*i*) Normal strategy where each train on the tracks is distinguish based on positioning using the train messages and digital map; and (*ii*) distance estimation method that calculate the train headway distance based on the time-of-arrive when the on-board equipment or its connection with radio block center is abnormal. The authors note whilst the existing MA does not reveal the neighbor trains' route and position and the interlocking system's state, the proposed MA+ would provide this information. Compared to the current ETCS-2 MA, the proposed one is more efficient; however, the main weaknesses of this proposal are that the train control through conventional MA and the new MA+ will result in an information overhead, delay, and degrade service quality. In addition, the MA+ is design is more complex, which will generate energy loss.

Safety Monitor for Train-centric CBTC System

Wang et al. [105] have proposed a novel topology-based technique for guaranteeing the safety of Train-centric Communication-Based Train Control (TcCBTC) systems. The main purpose of the proposed methodology is to provides topological operational semantics for railway networks, MA and the train trajectory. Given that in the TcCBTC system it is the Vehicle On-Board Controller (VOBC) that calculates the MA, the authors propose to integrate the proposed method into the VOBC equipment in order

to ensure its smooth operation. The method requires basic information for the MA algorithm, the original MA generated by the train control algorithm, the speed and brake commands of the train. Safety verification of the train are done through a series of computations of the topology theorems, where the railway network is described as a metric space and the original MA for a train is abstracted as a topological space. The possible train trajectory is induced from the two parameters of speed and brake command and then also expressed as a topological space. The output of the safety monitor is either a safe MA or a fail-safe command to the VOBC. Wang et al. have presented an innovative topology-based method for TcCBTC system, which allow the checking the rationality of the original MA. Unfortunately, this technique is not suitable to perform runtime verification for the ATP function of the TcCBTC system.

Intelligent Safe Driving Methods Based on Hybrid Automata and Ensemble CART Algorithms for Multihigh-Speed Trains

Cheng et al. [34] have designed an Intelligent and Safe Driving Methods (ISDMs) for high-speed trains, which is based on a combination of hybrid automata with the expert system and the data mining algorithms. The main purpose of the proposal is to obtain better speed–distance curves for the trains. In the proposed methods, the authors have used Hybrid Automata (HA) to construct safe distance controller that aims for ensuring the safe tracking distance between two adjacent running trains in real-time. Then, the source driving datasets are clustered into several parts in terms of the train's operational speed, the speed limit of current operational zones, and the driving data volume. Furthermore, smart driving methods are developed based on data mining algorithms: AdaBoost.R and Bagging Classification And Regression Tree (A-CART and B-CART) in order to discover the potential driving rules from the field driving data and establish base learning machines of each clustered dataset, where an Iterative Pruning Error Minimization (IPEM) algorithm is designed to reduce the redundancy of the driving data and improve the computational speed of the learning process. Finally, the base learning machines are combined with HA controller to control the trains' operation. In fact, the proposed methods outperform the conventional Automatic Train Operation (ATO) method in terms of energy consumption. However, the proposed methods exhibit a very high complexity in terms of development and

configuration that may degrade their performances and render them unsuited for practical implementation.

Hybrid Online safety Observer for CTCS-3 Train Control System On-Board Equipment

Zhang et al. [119] have attempted to resolve the issue of over-speed behavior detection between discrete time instants, which can affect the smooth running of the train, for the safety of the Chinese Train Control System-3 (CTCS-3) operation. The authors have proposed a monitoring approach of train speed in continuous time by using the hybrid reachability analysis method, which is integrated into the on-board equipment of CTCS-3. In the proposed approach, the continuous train behavior is modeled by hybrid automata. Then, reachable sets of train behavior starting from the current time instant are computed through reachable sets computation module based on the hybrid model. Furthermore, the safety property set is determined according to the runtime speed limits in the relevant emergency brake intervention and most restrictive speed profile information. Finally, the intersection check between the reachable set and safety property set is performed to decide whether train speed may exceed the speed limit in a short future period. The authors have claimed that their proposed observation approach can detect violations of safety properties during the time intervals between discrete instants, which cannot be achieved by conventional methods. Unfortunately, their approach relies on complex modeling tools, which is difficult to implement. In addition, the authors are focused on the traditional train control system that is equipped with quasi-moving block mode, which not optimize the use of the railway infrastructure.

3.3.1.2 Risks assessment-based approaches

Critical Scenarios and Their Identification in Parallel Railroad Level Crossing Traffic Control Systems

Huang et al. [54] have proposed a critical scenarios identification approach for parallel railroad Level Crossing (LC) traffic control system, where such scenarios are extracted and avoided by controlling the phase of traffic light operations. Huang et al.'s approach aims to handle the dynamic alternation of traffic lights while a train is approaching

the intersection of railroads and roadways in order to keeps the traffic safety to this zone. The proposed approach lies on Deterministic and Stochastic Petri Nets (DSPNs) to model parallel railroad LC control systems for single and double track railroad lines. In particular, two types of transitions, i.e., timed and immediate, are employed. The former type is used to model the traffic light control systems. The latter type is used to describe the dynamic behavior of the trains approaching the crossing zone. The authors have interested in technical aspects; however, LC safety is an issue at the crossroads between technical aspects, operational procedures, and human factors making the proposed solution not suitable to guarantee the safety level required in LC. In addition, the complex situation of multiple crossing along the railway track is not modeled, where these types of situations always create a delay in passing of trains and in some cases may develop the situation of collisions.

Model-Based Diagnosis of Multi-Track Level Crossing Plants

Liu et al. [69] have addressed the problem of vehicle-train collisions at the multi-lane and bidirectional LC. The authors have carried out an analysis pertaining to the diagnosability of two main failure classes that can affect the protection system at automatic LCs, which are failures which may affect the train sensing module that is responsible for detecting trains at the approaching and leaving directions, and failures which may affect the local control system in charge of barriers raising/lowering, sound alarms and road traffic lights. To do this, a Labeled Petri Net (LPN) behavioral model is first established depicting the global system function, including both the normal operation and the faulty behavior. Then, the diagnosability analysis for two considered failure classes based on the established model is performed using three approaches namely, the diagnose approach [92], the verifier approach [113] and the on-the fly and incremental approach [68], where the aim is to detect if all failures can be detected within a finite period of time after their occurrence for the control systems reconfiguration to restrict the failure consequences. In fact, Petri Nets formalism have the ability to model such systems. However, they cannot determine the exact time of transition firing without proper extension in the dimension of time. Moreover, in the established model, only one vehicle can be contained in a place and the intersections and vehicles size is not considered, which does not reflect realism. Besides, the driving behaviors at a congested intersection are not considered.

Fault Tree Analysis Combined With Quantitative Analysis for High-Speed Railway Accidents

Liu et al. [71] have proposed an approach aims at investigating high-speed railway accidents, based on an in-depth study of the factors causing them. According to the relationships and interactions among basic events causing accidents, a fault tree logic diagram is first established. Next, in order to determine where the risks are, the dangers they pose, and what factors have the most significant effects on the rail system by analyzing all possible basic events, the authors have employed FTA method with Quantitative Analysis. Because of the incompleteness of the prior information and the complexity of decision environments, the authors have proposed a novel method, within the framework of intuitionistic fuzzy set theory is proposed to handle this problem, in which the failure possibilities of each basic events in the fault tree are particularly treated as Intuitionistic Trapezoidal Fuzzy Numbers (ITFNs). Finally, once the failure possibilities of each basic events in the fault tree are obtained, the events are sorted in order to select the influential events that contribute enormously to the occurrence of an incident. They reported that the proposed approach was effective to be applied to decrease the occurrence possibilities of similar accidents. However, to calculate the failure possibilities of an event, the failure possibilities of each base event must be calculated, and if the number of base events is larger, it will result in higher computational overhead. In addition, the drawbacks of using FTA is that it is not always practicable in situations where there is a lack of data and it cannot deal with the dynamic process of the accident causation.

In Table 3.2, we recapitulate each reviewed approach based on the following criteria: addressed problem, proposed solution, method used, and safety level.

Approach	Addressed problem	Proposed solution	Method used	Safety level
Wang et al. [106]	Safety issues of next generation control systems operation	Parallel monitoring approach for the next generation of train control systems	Parallel monitoring, data sharing and fusion, and common-mode cause error avoidance technologies	High
Wang et al. [107]	Trains rear-end collision avoidance	Train following interval pre-warning and control approach	Geese migration theory	High
Cai et al. [28]	Safety issues related to train performance and equipment failures	Monitoring and fault diagnosis approach of the subsystems controlling train equipment	Sensors system	Medium
Song et al. [96]	Safety issues of ETCS-2 operation	Computation approach of new movement autority for ETCS-2	Train-distance measurement strategies (Normal and backup strategy)	High
Wang et al. [105]	Safety issues of TcCBTC system operation	Safety monitoring approach for train-centric CBTC system	Topology theorems	High
Cheng et al. [34]	Speed-distance profile optimization issue	Intelligent safe driving approach for high-speed trains	Hybrid automata & expert system and data mining algorithms	High
Zhang et al. [119]	Over-speed behavior detection between discrete time	Hybrid safety observation approach for CTCS-3 train control system on-Board equipment	Reachability analysis	High
Huang et al. [54]	Critical scenarios identification in the LC	Critical scenarios identification approach in parallel railroad LC traffic control systems	Deterministic stochastic Petri networks	Medium
Liu et al. [69]	Vehicle-train collisions issue at the LC	Analysis approach pertaining to the failures affecting the protection system at automatic LC	Petri networks	Medium
Liu et al. [71]	Identification of factors causing accident	investigation approach of high-speed railway accidents	Failure Tree Analysis & Quantitative Analysis	Medium

Table 3.1: Overall comparison of the reviewed approaches proposed for rail ITSs.

Several technical, electrical, human and environmental criteria strongly influence the operating quality of rail transport systems. It is therefore imperative that approaches to ensuring the safety of rail transport systems take into account all these criteria. However, approaches based on the study of these factors cannot guarantee safe and efficient rail traffic [71]. The occurrence of railway accidents is a dynamic process, likewise the factors that cause accidents are changing with the development of the modern rail system. Consequently, the risk analysis that causes accidents in a such environment, based on new data, will always be required to rule out the possibility that railway systems will fall on a possible point of failure. For the detection of critical scenarios that may occur at the level crossing and the assessment of the risks associated with this place, modeling methods are used in [54, 69]. However, the percentage of a true detection remains insufficient for the LC because the latter requires a very high level of safety. Other approaches proposed in [96, 105, 107, 106, 119] have been focused on ensuring the proper operation of control systems. However, these systems are unable to cope with derailments and collisions despite their widespread deployment around the world. This can be justified by the fact that the solutions which have been proposed for the proper operation of these systems make them even more complex and less efficient. In order to reduce the structural and functional complexity of the conventional CBTC system, TcCBTC system has been proposed [105]. However, in TcCBTC system, train location information is acquired by balises where any balise failure leads to an error in determining the location, which causes a malfunction of the control system. Furthermore, the train location between the balises is estimated, which can cause estimation errors. To guarantee the correct operation of these control systems, their behaviors are checked by supervision methods, which are based on the mathematical topology [105] and on the reachability analysis technique [119]. However, these methods are much more complex and leads to excessive computation time. In fact, the sooner a train receives control decisions made by the control system, the more time it will have to react correctly.

To overcome the above-mentioned issues, we propose a train control system, which aims to further improve the functionality provided by the TcCBTC system. Consequently, to guarantee the safety of the proposed system, we propose a new method of supervising the TOBC operation. This method is executed during the entire movement of the train while providing a simple and less complex development environment, and satisfying the real-time requirement of railway system in terms of delays compared to [105] and [119].

3.3.2 Road ITSs

3.3.2.1 Attacks mitigation-based approaches

False safety messages detection-based approaches

A Reputation-Based Announcement Scheme for VANETs

Li et al. [67] have proposed a centralized reputation-based announcement approach in vehicular networks. The proposed approach aims to evaluate received messages reliability, where the reliability of a message is determined based on the vehicle reputation score that generates this message. A message is marked as reliable if the sender vehicle has a high reputation score. To determine a vehicle reputation score, the reputation system server collects feedback from other vehicles about the reliability of its messages and produces the reputation scores for vehicle. This score is collected, updated, and certified using a trusted party. The reputation score evolves, as time elapses, based on the reliability of messages that the vehicle announces. Vehicles tend to give positive feedback for reliable messages. This increases the reputation score. Meanwhile, a reputation score decreases when negative feedback is reported. Reputation-based approaches are useful, but they cannot be used to detect false emergency messages because trust is built over a period of time, and in the event that a fake message comes from a trusted vehicle, there is no way to detect it. Furthermore, the approaches based on centralized server for trust management is not suitable because with the rapid development of ITSs, it is not practical to cope with large numbers of vehicles using a centralized infrastructure. Too many requests will probably bring about high latency or even blocking, which may greatly decrease the Quality of Service for users.

Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection

Zaidi et al. [114] have proposed an approach to detect false information in emergency messages exchange among vehicles in Vehicular Ad hoc Networks (VANETs). The proposed approach relies upon statistical techniques and running on each vehicle. It utilizes a model named *Greenshield's model* to estimate and model uninterrupted traffic. Each vehicle estimates its own flow parameter (F) which should be very similar for vehicles located closely to each other by using a model that employs density and the

average speed of other vehicles in its vicinity. After that, vehicles exchange their own F and density values along with their speed and location information; hence each vehicle could have information about surrounding vehicles. For each received message, vehicles compare the average of the received parameters to its own calculated parameters. If the difference is lower than a threshold, the message is accepted. Otherwise, the sender is monitored for some time and the data is accepted until the number of collected messages is enough to perform a t-test; if the sender is marked as rogue node, it will be reported to other vehicles and the vehicles data will be rejected. According to simulations, the proposed scheme could detect malicious nodes even when 40 % of the vehicles are malicious. However, when the attacker slowly increases their value, it may remain undetected since the attacker manipulates values gradually.

Physical Layer Plausibility Checks for Misbehavior Detection in V2X Networks

So et al. [94] have propose a detection bad vehicle behavior approach in VANETs based on plausibility model. In this work, the authors have addressed physical layer operations, applying three physical layer plausibility checks that are based on the Received Signal Strength Indicator (RSSI) of Basic Safety Messages (BSMs) and the distance between two vehicles. In order to determine whether a received BSM is malicious, the proposed approach relies on collecting and analyzing the RSSI value obtained from each individual BSM. For each BSM, the GPS coordinates from the transmitting vehicle and the receiving vehicle are first recorded to measure the difference in distance between the two vehicles. Then, BSMs with similar distances between transmitting and receiving vehicles are grouped together, and the confidence interval for each group for normal RSSI values based on the BSM dataset for normal behavior using the mean and the variance is computed. Using the confidence intervals as a control parameter, every individual BSM is checked whether is outside of this interval or not. If the RSSI of the BSM at a given distance from the receiver is outside of the confidence interval, then we mark the BSM as anomalous. The three proposed plausibility checks are as follow. The first plausibility check named First-BSM where once a BSM is outside of the confidence interval, the transmitting vehicle is immediately classified as a misbehaving vehicle. The second Majority-BSM is applied with a majority rule to the received BSMs. If the majority of the BSMs are classified as malicious, then the vehicle is classified as malicious. The third plausibility check is referred to as the Weighted-BSM that assigns a score to each vehicle, and updates this score for

every new BSM the vehicle receives from the transmitting vehicle according to a weighted moving average. If the vehicle reaches a score that is below a threshold, which is outside the 99.7% of normal vehicle scores, then the vehicle is classified as an attacker. The proposed approach Identifies and detects spoofing attacks in the Vehicle-to-anything (V2X) application layer. Unfortunately, the proposal is dependent on Road-Side Units (RSUs) and in the event of loss of communication, the security system will be compromised. Also, signal strength can vary greatly due to obstacles and environment, which may make this solution unsuitable.

Detection and Identification of Malicious Cyber-Attacks in Connected and Automated Vehicles' Real-Time Sensors

Eziama et al. [41] have addressed the detection and identification of anomalous behaviors associated with cyber-attacks in Connected and Automated Vehicles (CAVs) networks. The proposed approach is based on combination of Bayesian Deep Learning (BDL) with Discrete Wavelet Transform (DWT). In particular, DWT applies wavelet transform to denoise the noisy sensory BSMs data and decompose them by transforming it into an orthogonal domain and processing operations on the resulting coefficients followed. Then, through reconstruction process, the sensory input is transformed back to original state, where such denoised reconstructed BSMs data is fed into the BDL algorithm for further examination and anomaly detection. The stage of anomaly detection using BDL algorithm is achieved by first splitting the data into training and testing dataset. The proposed approach is trained to develop a prediction on the training dataset. while the testing dataset is fed to the algorithm for prediction test. The results show the ability of the proposed approach to detect and identify anomalous behaviors in the unstable CAVs network states. However, discrete wavelet transform is computationally expensive as well as memory access intensive[55], which increase the deployment cost.

Detecting False Messages in Vehicular Ad Hoc Networks Based on a Traffic Flow Model

Liu et al. [70] have proposed an approach aims at identifying false emergency messages in VANETs. The proposed approach is based on traffic flow theory, and deployed at each vehicle and it operates in a fully distributed style. When receiving an emergency message, a collection process is first performed, in which the vehicle collects its own sensor data and exchanges these data with the nearby vehicles to calculate traffic density of the detection region, which is defined as the upstream and downstream segments of the reported accident site. Then, the traffic flow is modelling using observation data aggregated from travelling vehicles. Furthermore, in the detecting process, the traffic flow model built is employed to analyze the characteristics of vehicular behavior and to estimate the probability density function of traffic parameters. Finally, based on the Bayesian approach, the proposed model calculates the likelihood of traffic patterns, which is further used to verify whether events such as road accidents, reported by the vehicle have really happened. If the model identifies the reported event as wrong, the corresponding vehicles that broadcasted the messages are considered as malicious. The information regarding malicious vehicles are broadcasted to all vehicles in the region. However, Bayesian inference is a computationally intensive process both in computation time and memory requirements, and since, the On-Board Units (OBUs) are highly resource constrained, this approach is not suitable for highly dense regions.

Safety messages verification prioritization-based approaches

A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs

Biswas and Mišić [23] have proposed a safety messages verification prioritization approach in VANETs. The proposed approach relies on bloom filter [24] to compute relevance of the BSM, using some physical attributes of a vehicle such as position, acceleration and velocity along with their enhanced distributed channel access classes. In order to rank a message, the message will be passed through three bloom filters, where each bloom filter checks an assigned portion of safety messages against the existing entries in them. The outcome of the bloom filters is then used in a binary decision tree to achieve the final rank. After that, messages associated to each rank will be randomly processed with a specific verification probability, which is determined

using the backoff time for a packet transmission. Although the proposed approach is secure and scalable, it takes long computational time, and the bloom filter has several performance limitations, as discussed in [39].

CAESAR: A Criticality-Aware ECDSA Signature Verification Scheme with Markov Model

Chen et al. [31] have proposed CAESAR, Criticality-Aware Criticality-Aware ECDSA Signature Verification approach. The proposed approach relies on the use of Multi-Level Priority Queues (MLPQs) and Markov Chain (MC). First, the proposed approach adopts the message classification by the signal strengths of messages in order to dispatch them into MLPQ, where each one of message queues has an interval of signal strength that indicates a message will be allocated to which message queue. Therefore, the receiver gathers its surrounding messages, it then dispatches them into MLPQs based on their signal strengths. Then, the Markov model is adopted to adjust the order of verification, where each state in the MC as considered as the ratio of messages from all received in MLPQs at one time slot, which is achievable at the application layer. A transition between two states represents the probability/portion of CSMs in MLPQs between two sequential time slots. After that, to extract messages from different queues, roulette selection is adopted to select a queue based on the calculated distribution of messages over MLPQs and the random number generated. For the roulette selection procedure, it will firstly iterate all probabilities to generate the ratio of messages over MLPQs as Cumulative Distribution Function (CDF). Then, to iterate each one of CDF and compare it with the random number. If the latter is bigger than one of probabilities, this queue is selected to be returned. Once the selected queue is determined, message scheduler extracts the message from the chosen queue. However, mass broadcast inevitably occurs in traffic, approach solely relying on the queuing may in this case be unable to process all incoming messages, so it becomes difficult for vehicles to process them on time, which lead to massages loss and would cause accidents.

Adaptive Security Provisioning for Vehicular Safety Applications

Hamida et al. [50] have proposed a security approach to increase reliability of the vehicular safety application, where additional measures are introduced to the security procedures. The authors have proposed two security mechanisms, one at the receiver and other at the transmitter side of a vehicular network. The first technique uses channel aware mechanism to prioritize the signature verification of BSMs from closer neighbors, while the second technique consist of selecting the best security level for BSMs according to cryptographic loss rate. At the receiver side, vehicles classify first the received signal strength of BSMs into several safety areas based on the k-means clustering algorithm. The BSMs assigned to different safety areas are then mapped to multilevel priority queues for message verification. The buffer associated with closer area's received messages has a higher priority for verification. On the transmitter side, two security mechanisms have been proposed: the first mechanism uses random selection of transmitter security level to reduce Cryptographic Loss Rate (CLR) and the second mechanism adaptively selects the optimal security level by iteratively calculating CLR and upgrading or downgrading the security level keeping CLR below the required threshold. In random mechanism, each vehicle picks one of the available security levels every BSM transmission depending on elliptic curve prime field (NISTP) and secure hash algorithm digest size, where four levels of security are available. In the adaptive security level selection mechanism, each vehicle evaluates the total packets that are received for verification at the security queue as Pr. Similarly, vehicles find the number of packets which could not get verified within the timeout period as Pl. To find cryptographic loss ratio CLR, vehicles take a ratio of Pr and Pl. Each vehicle uses a threshold that defines a tolerable level of CLR beyond which vehicles need to reduce their security level. If CLR is lower than the threshold during current time, vehicle select the next lower available security level. The proposed mechanisms show improvements in terms of safety metric. Nevertheless, a drawback of this proposal is that signal strength can vary significantly due to obstacles and environment, consequently, a signal strength may not be suitable.

Weighted Priority Based Signatures' Batch Verification Scheme in Vehicular Ad-Hoc Networks

Khan et al. [62] have proposed a weighted priority based signature's verification approach. The authors aim to increases the efficiency of batch verification and mitigating the too long-time issues resulting from the verification of each and every message. Therefore, in the proposed approach, vehicles and RSUs collect messages for some period of time and verifies all collected messages in a batch at once instead of verifying each message. To calculate priority, different network and vehicle related parameters are used, namely, the vehicle type, the trust value of the vehicle, Vehicle's current position and speed, network density, and the Message type. The vehicle type means the purpose of the vehicle like emergency vehicle, traffic authority vehicles, and normal public vehicles. In this approach, priority of emergency vehicles is high, priority of traffic authority vehicles is medium, and normal public vehicle's priority is low. About the trust value of the vehicle, when a vehicle becomes a part of the network, a zero trust value is assigned to the vehicle. As soon as vehicle starts sending and relaying the messages trust value starts to increase or decrease depending upon the actions of that vehicle. By using the trust model proposed by Wei et al. [111], a trust value for each vehicle is calculated and used as one parameter to assign priority to the vehicle. As to message type, safety messages have higher priority over non safety messages, where a default priority value is assigned to each type and whenever RSU receives a message. Priority of a vehicle is updated either after a specific periodic period of time or on leaving or joining highway, identification of malicious signature, etc. To formulate a batch, a weighted priority technique is employed, where for the first time, all the parameters have the same weight. However, once the priority is updated, the weight increases in such a way that vehicles with high priority will have more weight as compared to vehicles of low priority. An advantage of the proposed approach is that it reduces the verification time per message. However, the downsides are that a single false signature can result in an unsuccessful verification of the entire batch, also collecting messages process for verification generate an additional delay.

Verifying Safety Messages Using Relative-Time and Zone Priority in Vehicular Ad Hoc Networks

Banani et al. [21] have proposed an approach to selecting important safety messages for verification in VANETs. The proposed approach prioritizes safety messages based on three metrics, namely, location, direction, and proximity of the sender and relative-time taken between vehicles. The direction and location of a transmitting vehicle relative to the receiving vehicle are used to group messages into four quadrants: in quadrant 1 the transmitting vehicle is traveling in the same direction and is in front of the receiving vehicle, in quadrant 2 the transmitting vehicle is traveling in the same direction and is behind the receiving vehicle, in quadrant 3 the transmitting vehicle is traveling in the opposite direction and is in front of the receiving vehicle, and in quadrant 4 the transmitting vehicle is traveling in the opposite direction and is behind the receiving vehicle. Then, the designed quadrants are combined with close proximity and relative-time rankings to capture the importance of safety messages, where, if a BSM comes from the vehicles in the safe zone of receiver vehicle and belongs to quadrant 4, then the BSM has the lowest priority and will be inserted at the end of the buffer. Otherwise, the BSM will be inserted into the buffer based on the zone (from closest to distant zone). If there are multiple messages in the buffer with the same zone, the messages will be arranged based on the relative time (from low to high value). In order to ensure that only recent messages are verified, messages that are older than a specified time will be dropped. The authors have claimed that their proposed approach gives the highest message verification rate and provides higher awareness of nearby vehicles. However, needs a bit more computation cost and an extra delay, resulting in packet loss, which does not meet the requirements of safety applications.

Pseudonym Certificate Validations under Heavy Vehicular Traffic Loads

Jha et al. [59] have proposed a 3-level priority based approach that categorizes messages as arriving from immediate surrounding neighbors, their neighbors and the rest and assign them a priority before signature validation and insert them in multiple queues based on their priority. Firstly, if the message arrival rate at OBU is lesser than the maximum processing rate, then each new message is directly submitted for verification. Otherwise, the messages are enqueued into one of the priority queues based on its

content. To determine the priority, firstly the heading of the sender is examined and if the vehicle is moving in the opposite traveling direction, then the message is ignored. Then, message content is checked with prior messages to ascertain if it is a replay message. If a message is detected as a replayed message, then it is a candidate for misbehavior reporting. If it is an emergency message, the semantic scheduler checks if it the associated event has been addressed before and ignores newly received messages based on event state. If the public key for message is already computed from prior messages originating at the same sender, then we avoid credential validation by retrieving validations from the cache. Otherwise, the public key is computed from the implicit certificate in the message payload. The performance evaluation results show that this queuing based handling would ease message congestion that occur at a vehicle that processes all received messages on a crowded highway. Nevertheless, it causes packets loss.

Messages Classification and Dynamic Batch Verification Scheme for VANETs

Ferng et al. [43] have proposed MCDBVS, a Messages Classification and Dynamic Batch Verification Scheme, where messages are classified and prioritized so that more important BSMs can be verified earlier in batch. The authors aim at improving the efficiency of message verification and determining the appropriate number of safety messages to be verified. They introduce a method for dynamically adjusting the number of messages to be verified in batch for each verification node, where the batch size is halved when failures of batch verification occur consecutively over a certain threshold to improve the efficiency of batch verification. Otherwise, the batch size is doubled when successes of batch verification occur consecutively over a certain threshold to increase the messages in a batch to be verified. For a failure of batch verification, a divide-and-conquer approach is utilized to find the illegitimate messages. For BSMs, physical attributes can be further associated for prioritization accordingly if the total number of BSMs is over the capacity of verification. Although the above scheme reduces the transmission and calculation overhead, collecting messages process for verification generate an additional delay, and single false signature can cause unsuccessful verification of the entire batch.

3.3.2.2 BSMs dissemination quality-based approaches

BSM: Broadcasting of Safety Messages in Vehicular Ad Hoc Networks

Najafzadeh et al. [79] have proposed a broadcasting approach for BSMs that dynamically adjusts waiting time of a vehicle according to the number of neighbor vehicles and distance from the sender vehicle. The proposed approach relies on beacon exchange among vehicles. First each vehicle determines 1-hop neighbor list by sending periodic hello messages and calculate distance from the neighbors. Then, vehicles in the networks calculate waiting time based on distance between itself and source and number of neighbors. Finally, they broadcast the safety message whenever is waiting time expire. Farthest node with higher neighbors' density relays the message as soon as it receives it. During topology changes, the proposed approach allows vehicles to communicate periodically with each other for routing information, but it has problems that decrease efficiency and performance in the network such as duplicate communication cost due to unnecessary broadcast of control packets even if range of radio of the vehicles is more than neighboring vehicle distance.

BSM Dissemination With Network Coded Relaying in VANETs at NLOS intersections

Goa et al. [45] have addressed Non-Line-Of-Sight (NLOS) condition issue on vehicle-to-vehicle communications at urban intersections to improve the reliability and reduce latency for BSMs broadcast. The proposed approach consists in BSMs delivery in an indirect broadcasting fashion by relay based on Random Ninear Network Coding (RLNC) and the repetitive transmission pattern to enlarge the safety packet reception probability. The authors have proposed two relaying techniques, repetitive transmission with network coding at intersection vehicle, which applies the random linear network coding at a single relay node, and repetitive transmission with network coding at all nodes where all nodes relay coded packets. In the former technique, a node linearly combines all locally stored packets, to form a coded packet, where the packets can be its own packet or a certain number of packets received from neighbors. The rest nodes follow the same rule that they are only allowed to repetitively broadcast their own packets. The latter technique consists at applying RLNC at all nodes. Subject to the

repetitive transmission pattern, every node performs as a relay node. When a node has the chance for transmission, it linearly combines received packets and own safety packet into a coded packet. Both approaches have improved the reliability of BSMs dissemination. However, when the network become denser, they cannot cope with the deteriorating performance where the packet reception rate plummets, also an incorrect setting of RLNC redundancies will result in network traffic overload.

A Safety Message Broadcast Strategy in Hybrid Vehicular Network Environment

Feng et al. [42] have proposed a safety message broadcast approach that is based on VANET cellular architecture. The proposed approach aims at ensuring reliable safety messages transmission with lesser dependencies towards traffic density and fixed access points. In the proposed approach, safety message is transmitted by the electing optimal forwarder. Optimal forwarder is elected based on the priority of each vehicle, considering various factors such as link stability, channel quality, signal strength, etc. Highest priority vehicle broadcast the safety message to the neighbor vehicle in order to transmit safety in-formation to all neighbor vehicles. This approach widely improves channel access efficiency in addition to avoiding redundant data in a connected vehicle environment. However, it suffers from a great packet loss.

Hybrid-Vehfog: A Robust Approach for Reliable Dissemination of Critical Messages in Connected Vehicles

Paranjothi et al. [83] have addressed frequent disconnection problems that are faced to forward the safety messages between vehicles in connected vehicles environment. In this context, the authors have proposed a hybrid approach based on fog computing called Hybrid-Vehfog to disseminate messages in obstacle shadowing regions, and multi-hop approach to disseminate messages in non-obstacle shadowing regions. This approach divides the region into an obstacle zone and a non-obstacle zone. In the former zone, fog layer is located at the edge of a network, which includes access points, gateways, RSUs, base station, etc. RSUs and base stations play a major role in disseminating the messages. Fog layer are responsible for processing the information

received from the vehicles and temporarily store it or broadcast over the network. Cloud in fog computing is used to keep track of the resources allocated to each fog node and to manage interaction and interconnection among workloads on a fog layer. As the vehicles are aware of their locations in relation to the base station, the system deploys and broadcasts the critical messages to the fog layer and when it encounters the obstacle shadowing region. As a result, the messages are disseminated to the vehicles in the shadowing region seamlessly through the fog nodes. In the latter zone, the vehicles communicate with each other directly using a multi-hop technique, allowing communication to be established directly between vehicles. When a new vehicle enters the region, critical messages such as hazard alerts, can be delivered to the vehicle based on a multi-hop technique or the fog nodes based on its location. The benefit of this approach is that it dynamically adapts itself to the changing environment which helps to efficiently disseminate messages with minimal delay. Nevertheless, this approach lacks the capability of operating in a real time environment which means that performance estimation for this model is not efficient.

NSSC: Novel Segment Based Safety Message Broadcasting in Cluster-Based Vehicular Sensor Network

Alkhalifa and Almogren. [15] have proposed NSSC, a Novel Segment based Safety message broadcasting in Cluster based vehicular sensor network that mainly concentrated in three successive functions, namely, cluster formation, collision avoidance and safety message broadcasting. The latter focus on mitigating safety messages loss. The proposed approach is based on clustering architecture, where Variant based clustering approach based in chaotic crow search algorithm is used to form clusters and to elect a Cluster Head (CH) based on the two different metrics that are mobility and connectivity metrics. In order to mitigate the data collision during transmission between CH and Cluster Member, the authors have used Adaptive Carrier Sense Multiple access/Collision Avoidance algorithm, which allocates back-off time based on the buffer size. In safety message broadcasting, the proposed approach adopts Segment based Forwarder Selection (SFS) method, which selects optimal forwarder to broadcast safety message. If any vehicle supposed to accident in the road, then it implements SFS method to broadcast safety message to its member. SFS method initially segments the transmission range into the square region. And then, it divides the square region into two that are front and back regions. Furthermore, these regions are split into left and right diagonal regions. Vehicles present in the center portion

are most appropriate and adequate to carried out safety message broadcast process with reduced number of transmissions. From the center portion, optimal forwarder using Fuzzy-Vikor algorithm is selected. If center portion does not have any vehicle, then forwarder is selected from the side portion in parallel manner which reduces the latency in safety message broadcasting. In the optimal forwarder selection, the fuzzy weight values for some criterion, namely, ability of vehicle to broadcast messages, speed, delivery delay, forwarding probability are calculated. These values are arranged in descending order in order to rank each alternative. Finally, high rank vehicle is elected as forwarder. Obviously, the propose approach diminish the data collisions, but, the CHs have been selected by applying calculation comparison between vehicles in terms of mobility and connectivity without considering a CH location inside its cluster, which degraded performance and may cause data losses.

A Novel Hybrid MAC Protocol for Basic Safety Message Broadcasting in Vehicular Networks

Zhang et al. [118] had addressed the problem of network congestion and waste of network capacity that occur while sending BSMs with high frequency. In this context, they proposed a hybrid Medium Access Control (MAC) protocol for BSMs dissemination based on Physical-layer Network Coding (PNC) and Random Linear Network Coding (RLNC). The RSU broadcasts a polling message to invite vehicles to join in PNC session. Vehicles that successfully receive the polling message reply to the RSU after a short inter-frame space. Then the RSU broadcasts a coordination packet to notify all vehicles about which two vehicles form a PNC pair as well as the total number of PNC pairs, according to their instant locations, where one PNC pair consists of two vehicles that exchange their safety messages that are prioritized by RSU. The latter launches the PNC session. It waits for an arbitrary inter-frame space before broadcasting a beacon packet, which requests the first PNC pair to transmit their BSM packets. After an interval, the first PNC pair send their BSM packets simultaneously. The RSU tries to decode the overlapped signals. After decoding, the RSU will broadcast a downlink packet, which also notifies the next PNC pair by piggybacking their ID information. Upon receiving, the next PNC pair start the next round of BSM packet exchange, and this process repeats for all PNC pairs until the last one. In fact, the proposed approach suppresses the collisions and offers an increased packet delivery ratio. However, the communication with the centralized entities is associated with high communication overhead and delay.

Towards Optimal Dissemination of Emergency Messages in Internet of Vehicles: A Dynamic Clustering-Based Approach

Azzaoui et al. [17] have proposed EMD-IoV. an Emergency Message Dissemination in Internet of Vehicles approach that is based on a clustering strategy. It exploits both Dedicated Short-Range Communication (DSRC) and cellular Long Term Evolution (LTE) wireless communication interfaces to propagate emergency information in a short- and long-range way, respectively. The main objective of the proposed hybrid architecture is to efficiently forward data packets in a certain geographical region, with only a small delay and high percentage of vehicles successfully receiving packets. In this proposal, clustering architecture is proposed to efficiently select the optimal forwarders at each communication hop. The best path is then selected to forward the safety messages from a source vehicle to a destination, taking into account the optimal forwarding between both inter- and intra-geographical regions. Thus, a sender vehicle will forward the emergency messages to the appropriate next-hop vehicle based on the selected path, until the message is transmitted to its destination. The proposed approach highly reduces transmission latency, in addition it improves both vehicles' throughput and successfully delivered emergency packets. However, the clustering process is a complex operation, which may generate a considerable overhead.

In Table 3.2, we recapitulate each reviewed approach based on the following criteria: addressed problem, proposed solution, method used, advantages, and drawbacks.

Approach	Addressed problem	Proposed solution	Method used	Advantages	Drawbacks
Li et al. [67]	False safety messages detection	Reputation-based announcement approach	Reputation system	Provides a solid theoretical basis for calculating reputation	Based on centralised server and can not detect fake message in continuous time
Zaidi et al. [114]		Rogue node detection approach	Greenshield's model	High detection rate	Unreliable in case of attacker manipulates values gradually
So et al. [94]		Physical layer plausibility checks for misbehavior detection approach	Plausibility model	High identification and detection rate	Dependents on RSUs and variation of signal strength
Eziama et al. [41]		Detection and identification of malicious cyber-attacks in vehicles' real-Time sensors	Bayesian deep learning & Discrete Wavelet Transform	Identifies anomalous behaviors in unstable network states	Discrete wavelet transform is computationally expensive
Liu et al. [70]		Detecting false messages based on a traffic flow model approach	Traffic flow theory	Offers high detection accuracy	Bayesian inference is a computationally intensive process
Biswas and Mišić [23]	Safety messages verification prioritization	Cross-layer approach to privacy-preserving authentication	Bloom filter technique	Secure and scalable approach	Bloom filter has several performance limitations
Chen et al. [31]		Criticality-aware ECDSA signature verification approach	Markov model & Multi-level priority queues	Offers high accuracy	Unable to process all incoming messages
Hamida et al. [50]		Adaptive security provisioning approach	Channel aware mechanism	Improves messages verification rate	Signal strength can vary significantly
Khan et al. [62]		Signatures' batch verification approach	Weighted priority	Reduces the verification time per message	Single false signature can result in an unsuccessful verification, and additional delay due to collecting messages process
Banani et al. [21]		Verifying messages approach	Relative-time & Zone priority	Provides high message verification rate and higher awareness of nearby vehicles	Needs a bit more computation cost and an extra delay
Jha et al. [59]		Pseudonym certificate validations approach	Priority queues	Mitigates messages congestion	Causes packets loss
ferng et al. [43]		Messages classification and dynamic batch verification approach	Priority queues	Reduces the transmission and calculation overhead	Causes additional delay due to collecting process
Najafzadeh et al. [79]	Safety messages dissemination quality	Vehicles waiting time adjustment approach	Beacon exchange	Allows periodic communication for routing information	Duplicate communication cost
Goa et al. [45]		Bsms Dissemination approach at NLOS intersections	Random Linear Network Coding (RLNC)	Improves reliability of BSMs dissemination	Incorrect setting of RLNC results in traffic overload.
Feng et al. [42]		Safety message broadcast approach in hybrid vehicular network	VANET cellular architecture	Avoids redundant data	Suffers from a great packets loss
Paranjothi et al. [83]		Hybrid approach for disseminate messages	Fog computing	Adapts itself to the changing environment	Lacks the capability of operating in a real time environment
Alkhalifa and Almogren [15]		Safety message broadcasting approach in cluster-based network	Segment method	Decreases the data collisions	Suffers from packets loss
Zhang et al. [118]		Hybrid medium access control approach for BSM dissemination	Physical-layer & Random Linear Network Coding	Eliminates the collisions and increases packet delivery ratio	Generates high communication overhead and delay
Azzaoui et al. [17]		Dissemination of safety messages approach in Internet of Vehicles	Dynamic clustering	Reduces transmission latency	Generates a considerable overhead

Table 3.2: Overall comparison of the reviewed approaches proposed for the road safety-applications.

Based on previous works reviewed, it is obvious that several issues relating to the road safety applications have been addressed in the literature. However, the existing works have limitations, which requires the design of new solutions. The approaches dealing with the verification prioritization of received messages (see [23, 31, 50, 62, 21, 59, 43]) mostly show flaws in terms of safety, where a false message may be selected as important while a valid message reflecting the real traffic may not be taken into consideration at the right time or will not be fully taken into account, which can lead to the loss of critical data that could endanger the life of the driver as well as the vehicle, for example, since the behavior of the vehicle in this case depends only on the selected messages. The proposed approaches to deal with the attacks risk mitigation based on false messages detection [67, 114, 94, 41, 70], for their part, cannot reassure the safety level required by safety applications. Indeed, they have ability to detect several attacks types. However, the main drawback of some solutions is that they dependent on the RSUs. This presents limitations as they give rise to large communication overhead and delay that are not tolerable in time-critical applications. As well, the security will be compromised in the event of communication loss. Finally, the approaches focusing on quality of BSMs dissemination [79, 45, 42, 83, 15, 118, 17] undoubtedly increases the performance of vehicular communication networks. Nevertheless, their drawback is that they suffer from scalability issue. For instance, in [45] and [118], the authors applied RLNC to enlarge, respectively, the packet reception probability and for safety message dissemination. However, when the network become denser, they cannot cope with the quickly deteriorating performance, furthermore, incorrect setting of RLNC redundancies will result in network traffic overload. In [79], the authors discuss about the analysis of IEEE 802.11p safety related message dissemination in diversified environment. Nevertheless, in dynamic networks, it suffers from route cost which increased with the topology changes due to unnecessary broadcast of control packets.

In order to meet the requirements of safety applications, unlike to the aforementioned works, our work in this thesis deal with validity of BSM messages while basing on the communication parameters, which are greatly useful to detect a disruptive behavior. Our proposal relies on discordant BSM messages detection by checking of each incoming message, where checking a message consists of detecting of incoherence in the values of the metrics that constitute it. In the context of our work, an incoherence is seen as the lack or excess of BSM metrics values. Furthermore, our proposal does not depend on any central infrastructure, it is deployed individually in the vehicle itself and executed in a decentralized manner.

3.4 Conclusion

In this chapter, we focused on security and safety approaches of ITSs. Indeed, several works that have been proposed in the literature, however, these approaches suffer from limitations when it comes to finding a compromise between reliability, efficiency, and safety. In this chapter we have reviewed some recently proposed solutions judged relevant, which we have classified into two main categories. we have also discussed the strengths and shortcomings of each solution and provided a synthesis and comparison of the whole of the reviewed solutions. To overcome the limitations mentioned above, the objective of the next chapter is to present the approach that we propose for rail transport. Our approach is an enhanced train-centric communication-based train control system that aims to solve the issues existing in rail ITSs.

Chapter 4

Ultra-Safe and Reliable Enhanced Train-centric Communication-Based Train Control System

4.1 Introduction

Rail transport is becoming more used and more preferred compared to other means of transportation due to the lack of traffic congestion issues. However, the number of rail accidents is seeing a sharp rise and is continuing to multiply around the world. Train operation control is a critical activity in ensuring that train transportation runs smoothly and efficiently. In this context, we observe a great attention of the researcher community toward the Train-centric Communication-Based Train Control (TcCBTC) system, which has been suggested as an alternative solution to replace the conventional Communication-Based Train Control (CBTC) system. Its aim is to create a next-generation control system, in which the Vehicle On-Board Controller (VOBC) takes care of the train's service safety functions and performs train-to-train communication. Due to its safety-critical nature, specialised technologies must be adopted to guarantee the safety of the system operation. In this chapter, we address this issue by the proposition of *ETcCBTC (Enhanced Train-centric Communication-Based Train Control) system*, which provides efficient control of rail traffic. To ensure the operation's safety, we implement a new safety-checking approach based on process algebra, which aims to track and correct in real time the train behavior. This part of

our work was the subject of a research paper [115]. This chapter is organized as follows. In Section 4.2, we discuss the problem statement, where we give also our objectives. In section 4.3, we firstly present an overview of our proposal, then we give the detailed description of the ETcCBTC system operations. We also provide in this section the results obtained by the safety analysis of our system compared to the existing TcCBTC system. In the section 4.4 of this chapter, we emphasize on the evaluation of our proposal through simulations by comparing it with the conventional systems. Finally, we conclude this chapter in Section 4.5.

4.2 Problem statement

TcCBTC system is a new solution to guard the operation safety of trains. In this system, train location information is acquired by balises that are positioned on the rails. However, any balise failure leads to an error in determining the location, which causes a malfunction of the control system. Furthermore, the location between the balises is estimated, which can cause estimation errors. Due to the fact that such system is required to contain no safety-relevant errors that could lead the railway transportation into dangerous situations [110], specialised technologies must be adopted to guarantee the safety of the system operation. On other hand, with the technological advances and improved functional expectations, rail transport places higher demands on control systems [32]. In this context, some researches have been done in order to verify that all safety-related functions in train control systems run smoothly and efficiently. Nevertheless, the existing solutions for the safe operation of the TcCBTC system are based on methods that are much more complex and leads to an excessive computation time, which is unfit for the railway traffic. For all these reasons, we propose an improved train control system which aims to further improve the functionality provided by the TcCBTC system. Our proposal has two major objectives: 1) improving the architecture of the TcCBTC system in order to further improve the functionality provided by such system and 2) ensuring the operation safety of the proposed system by incorporating a new method of supervising the Train On-Board Controller (TOBC) operation.

4.3 Our proposed approach

In this section, first, we present an overview of our train control system, the developed system architecture, then we give the detailed description of its operation.

4.3.1 Overview

The autonomous vehicles emergence is a significant step forward in the development of safe and dependable ITSs. In this chapter, we focus on the autonomous train that is one of the most rapidly growing applications of autonomous vehicles. In this context, we propose ETcCBTC system, providing efficient control of rail traffic, where an improved architecture is defined, allowing a dual localisation of trains by using the balises and GPS. In order to guarantee the operation safety, we incorporate a new safety checking method, which aims to monitor continuously and in real time the train state. We integrate this component into TOBC equipment. The major contribution of this work is the integration of a process algebra-based model into the safety checking operation. The ideal and fully safe train behavior is modeled by process algebra composing every single possible safe behavior. The safety checking control component monitors continually the train behavior, builds up its corresponding model and crosses the latter with the ideal model through the process algebra's operators. In this way, the ETcCBTC detects upstream the failure risk and corrects the train behavior. Our system has high level of safety compared to the TcCBTC system. Furthermore, our proposed system is very suitable as a railway control system. This is due to the fact that, it satisfies the most stringent requirement of the rail systems in terms of delays, which is of the most importance in time-critical systems, optimizes the communication overhead, and provides safe and efficient train control.

Our work makes four major contributions, which are summarized in the following points:

1. We propose an ultra-safe and reliable ETcCBTC train control system, which provides efficient and safe control of rail traffic.

2. We propose an effective verification method to guarantee the safety of the ETcCBTC system, which makes it possible to monitor the train operation during its movement. In this way, the ETcCBTC system detects situations of violation of train proper operation and corrects the train behavior.

3. Our system presents a high level of safety compared to the TcCBTC system, which is demonstrated by a safety analysis.

4. The proposed system is effective in terms of transmission load and response time, also the proposed safety checking method is effective in the detection of violation in train operation, which is tested by simulations.

4.3.2 ETcCBTC system architecture

The operation of the conventional CBTC system is based on several equipment and uses several communication interfaces between them. In other words, this system relies on ground equipment to locate a train, and the latter moves while relying on an Movement Authority (MA) received from the Zone Controller (ZC). In the conventional train control systems, a ZC calculates the MAs and forwards it to the trains. Therefore, it is important to understand the risks involved in such a system. To remedy the problems caused by the structure and operation of the conventional CBTC system, several TcCBTC systems have been proposed. In these new systems, VOBC equipment provides safety functionalities. However, train location information is acquired by balises, which are positioned on the rails, where any balise failure leads to an error in determining the location, which causes a malfunction of the control system. In addition, the location between the balises is estimated, which can cause estimation errors. To further improve the safety and reliability of TcCBTC systems, we are defining a more improved architecture.

In Fig. 4.1, we illustrate the ETcCBTC system architecture. The designed system architecture is essentially composed of three main and two secondary components, respectively: Train On-Board Controller (TOBC), Traffic Supervision Center (TSC) and the wayside Object Control Unit (OCU), balises and GPS(Global Positioning System). The balises are placed into the tracks, which are used to localize the trains. The obtained information from balises is paired with the GPS information to estimate with more precision the train's position. In case of balise failure, the GPS will be used alone for the localization. The GPS allows to continuously transmit information about the location of trains to TSC which is responsible for monitoring traffic, when it detects a problem (malfunction of a train, train on a bad line, accident), it sends emergency alerts to all the trains in the network. Trains also support TSC by sending a warning commands when they detect their own faults so that TSC performs the emergency locking function. OCU controls the track objects such as points, balises, etc. Data transmission between trains and TSC and OCU is performed via direct communication. The train-to-train exchange is carried out through wireless communication [109]. The deployment of train-centric control system allows direct communication between the trains, where each train calculates in real time its status (position, speed, direction, malfunction alert, etc.) and communicates it to the preceding trains within its communication range.

Upon receiving this data, the TOBC subsystem calculates the MA as well as the protection profile curves. The TOBC constructs a first warning curve corresponding to

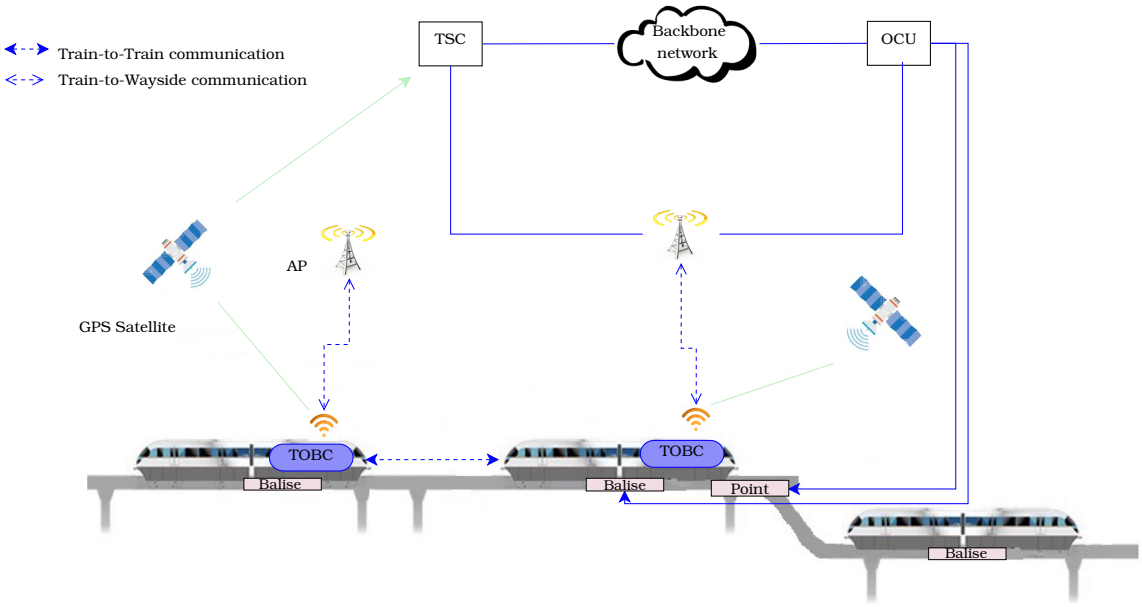

Fig. 4.1: ETcCBTC system architecture.

the authorized speed limit V_{SBC}, and a second control curve corresponding to the speed V_{EBC} above which service braking doesn't allow to reduce the speed of the train at an acceptable value. In the case where the train speed exceeds service braking curve, service braking is triggered to reduce the train speed as soon as possible. In the case where emergency braking curve is reached, emergency braking is triggered to stop the train. In addition, the TOBC subsystem performs train monitoring against any derailment and collision, where each time it receives the train location, it compares it with the travel route plotted by the TSC and with the Movement Authority Limit (MAL), where the latter specifies the stop point that the train must never overshoot. In the event that the location received is not included in the travel routes traced by the TSC or the location reached the MAL, an emergency braking will be executed. Therefore, the train by itself generates control commands through the TOBC equipment.

4.3.3 Safety monitoring method

The proposed method for ETcCBTC system safety control relies on supervising the behavior of the train during its movement and it is based on process algebra. Our

method has three distinct phases, namely, (1) safety policy generation phase, (2) train behavior detection phase, and (3) safety verification phase. The first phase consists of the generating of safety properties that the train must respect during its movement using process algebra. The second phase focuses on detecting the behavior of the train during its movement and modeling them based on process algebra. Finally, the third phase concerns the verification of inclusion of the current train behavior in the defined safety policy. The overall safety verification process carried out by the proposed control method is illustrated by Algorithm 1. The notations used throughout this chapter with their meanings are summarized in Table 4.1.

Symbol	Signification
ρ	Current train behavior
Φ	Safety policy
Acc	Acceleration
EB	Emergency Braking
l	Location
MA	Movement Authority
MAL	Movement Authority Limit
NA	No Action
P	Estimated train behaviors
S	Speed
SB	Service Braking
V_{SBC}	Speed on Service Braking Curve
V_{EBC}	Speed on Emergency Braking Curve
y	State variable

Table 4.1: Notations

The functionalities which ensure safety monitoring are developed in a module integrated into the TOBC equipment. The operation scenario of this module is illustrated in Fig. 4.2. This module has as input parameters: current train speed, current train location, and the MA, which is calculated by the train control algorithm. As for the data related to the brake which are the speeds V_{EBC} and V_{SBC} on the protection curves are acquired via the Over Speed Protection Module (OSPM). These parameters are used to generate the current train behavior from the estimated behaviors as well as the safety policy. A verification of the inclusion of the current train behavior in the safety properties is carried out. In the event that the inclusion is not verified, a warning command will be generated to the TOBC equipment, which indicate a safety breach during the train operation. In other words, if the train exceeds the speeds limit;

or it goes off on the wrong track (derailment); or if its MAL is reached, a warning signal will be sent to the TOBC equipment in order to perform a braking action. In what follows, we describe the basic principle of the proposed method.

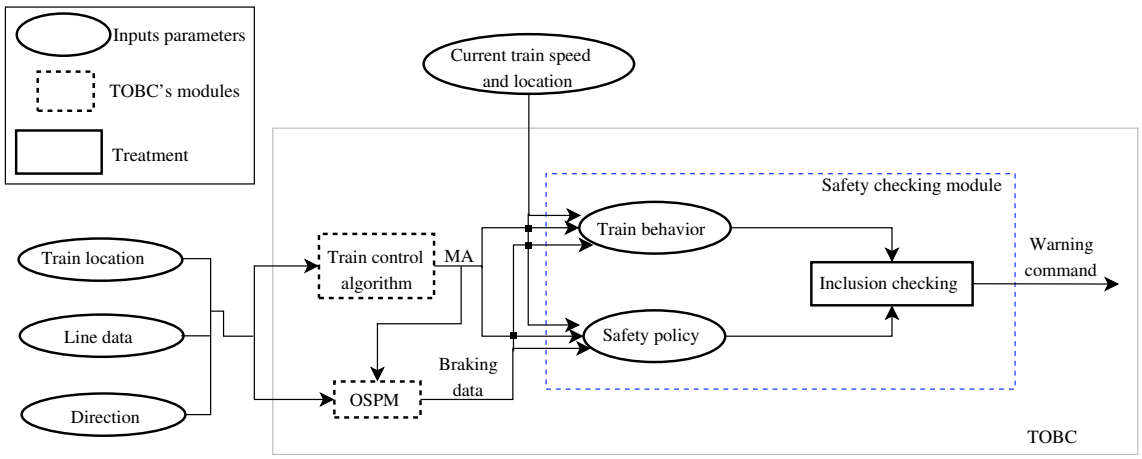

Fig. 4.2: Flowchart of the safety supervision of the proposed ETcCBTC system.

4.3.3.1 Safety policy generation phase

The objective of this phase is to model the ideal and totally safe behavior by process algebra. The safety policy[1] is generated according to the specifications of the standard $IEEE\ 1474.1^{TM}$ [90]. We take into account three crucial points in train operation, namely, (i) speed to guarantee the avoidance of situations where speed limits are exceeded; (ii) trajectory to guarantee the avoidance of entry situations on a bad line (derailment); and (iii) the train's MA to guarantee the avoidance of possible collisions.

In Fig. 4.3, we illustrate the graph which represents the safety policy. We consider a graph $G = \langle V,\ E \rangle$, where V and E represent the set of vertices and edges, respectively. The vertices of the graph represent the actions that the train performs. The existence of an edge which connects two vertices means that the train passes from one action to another action while following the changes related to its speed S and its location l. We assume that in the initial state $Init$ the train is stopped.

While the speed S of the train is lower than the authorized speed limit V_{SBC} on the service braking curve, an acceleration action Acc can be performed by the train. In the case, where the train speed S exceeds or equals the speed limit V_{EBC} on the emergency braking curve, or the location l of a train reached MAL, an emergency braking Eb must be applied. As for the service brake Sb, it must be executed as long

[1]The generated safety policy that the train must respect during its movement is the only variation.

as the train speed S exceeds the speed V_{SBC} and it does not exceed the speed V_{EBC}. We define a state variable $y = 1$ which indicates that the train is in the correct line, and $y = 0$ to indicate that the train enters a wrong line, which leads to the execution of an emergency braking. Also, when the train performs a service braking Sb, it has to perform an emergency braking Eb in the event of exceeding the MAL or the train enters a wrong line (derailment).

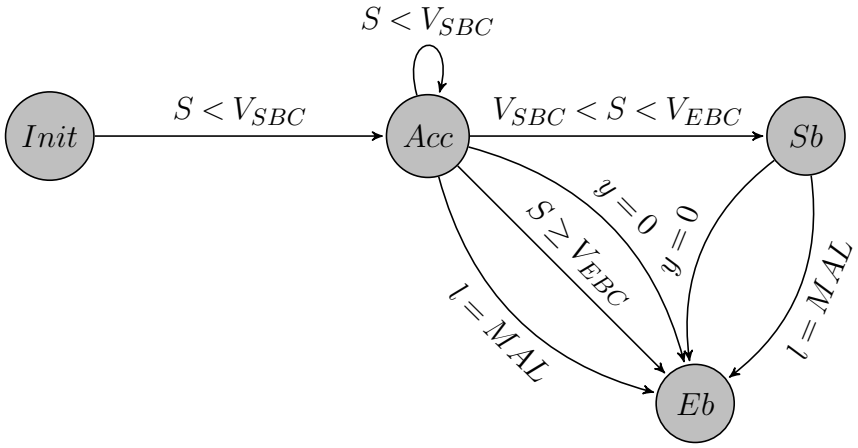

Fig. 4.3: Safety policy graph.

Process algebra based generation of process expression that specify the safety properties Φ according to train speed and location from the graph is described below.

$$\Phi = (S < V_{SBC} \rhd Acc) + ((S > V_{SBC} \wedge S < V_{EBC}) \rhd SB) + (((S \geq V_{EBC}) \vee (l = MAL) \vee (y = 0) \rhd EB) + \perp \rhd NA) \quad (4.1)$$

4.3.3.2 Train behavior detection phase

This phase emphasizes the modeling of train behaviors during its movement. To do this, we estimate all the possible behaviors that the train would perform throughout its movement, and represent them by a graph. Thereafter, from this graph we generate the algebraic expression of the process specifying train behaviors while using process algebra.

We illustrate in Fig. 4.4 the graph of estimated behaviors of the train during its movement. The train could perform an acceleration action Acc if its speed S is lower than or also exceeds the speed V_{SBC}. In the case of the speed that is greater than to the speed V_{SBC}, or less than the speed V_{EBC}, also in otherwise, it could perform

a service braking Sb, as it could perform an emergency braking Eb. When the train enters a bad line, or it reached the MAL, it could execute a service braking Sb, as it could execute an emergency braking Eb. Once the service braking Sb is executed, an emergency braking Eb could be triggered if the train is in a bad line, or also it has reached the MAL.

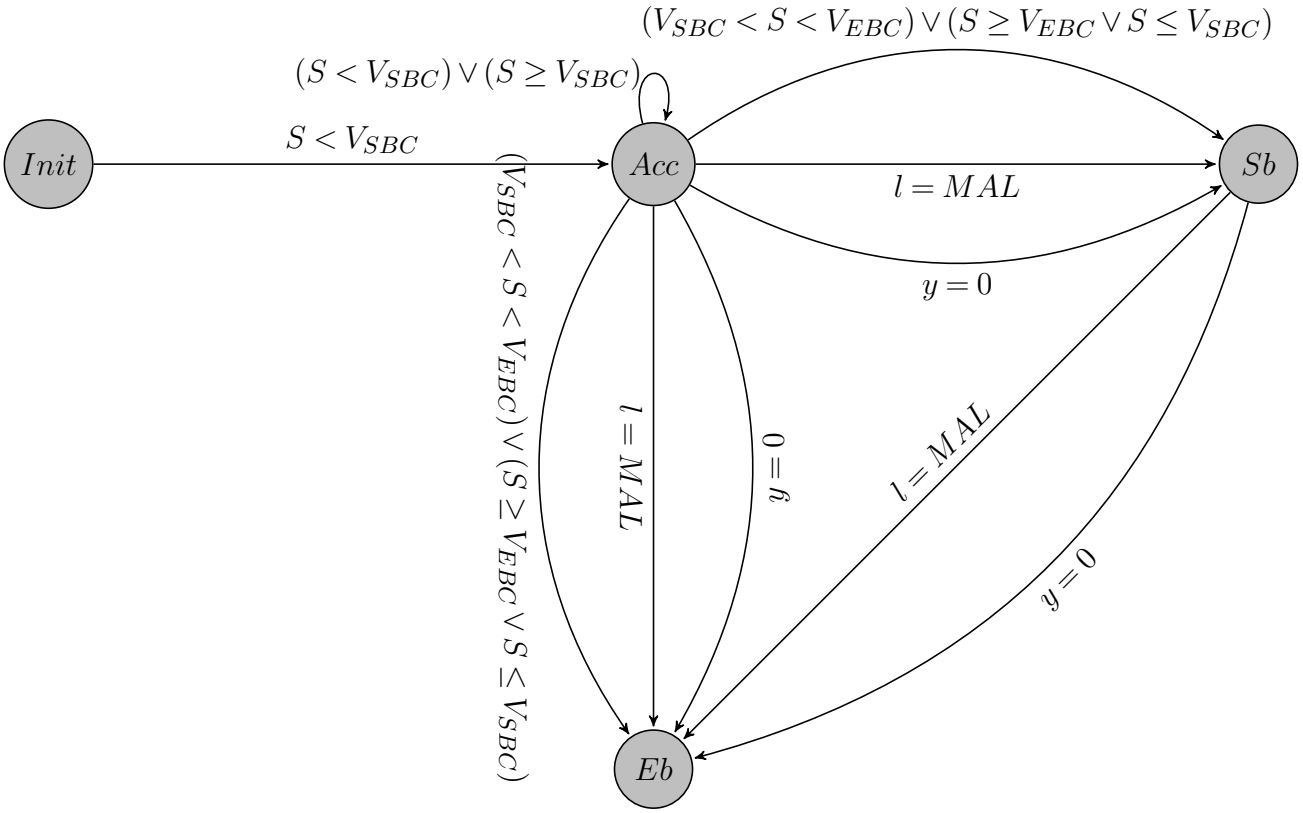

Fig. 4.4: Train behaviors graph.

Process algebra based generation of process expression P that specify all possible behaviors of the train during its movement from the graph is described below.

$$P = ((S < V_{SBC}) \vee \perp \rhd Acc) + ((S > V_{SBC} \wedge S < V_{EBC}) \vee (y = 0) \vee (l = MAL) \vee \perp \rhd SB) + (((S > V_{SBC} \wedge S < V_{EBC}) \vee (y = 0) \vee (l = MAL)) \vee \perp \rhd EB) \tag{4.2}$$

4.3.3.3 Safety checking phase

As illustrated in Algorithm 1, this phase allows to verify the proper operation of the train by checking whether the train throughout its movement respects the defined safety policy. Upon the generation of the safety policy and the train behavior detection is completed, the verification phase of the inclusion of the train behavior in the safety policy starts. The safety verification module uses the current train speed S_i and location l_i in order to obtain the algebraic expression of the current train behavior ρ from the algebraic expressions of the set of estimated behaviors P as well the safety policy. Afterwards, it compares the current behavior of the train to the safety policy. To do this, it calculates the intersection $\rho \sqcap \phi$ between the expression of the process, specifying the current behavior of the train ρ and the expressions of the process specifying the safety policy ϕ such as

$$\rho \sqcap \phi = \sum_{(\alpha_\rho,\ \alpha_\phi) \in \delta(\rho) \times \delta(\phi)} (c_\rho \wedge c_\phi) \rhd u(\alpha_\rho,\ \alpha_\phi).(\partial_{c_\rho \rhd \alpha_\rho}(\rho) \sqcap \partial_{c_\phi \rhd \alpha_\phi}(\phi)), \tag{4.3}$$

where $u(\alpha_\rho,\ \alpha_\phi)$ is a function which allows to unify two actions α_ρ and α_ϕ. We have used the notion of derivatives, where $\partial_{c_\rho \rhd \alpha_\rho}(\rho)$ is the derivative of the process ρ with respect to the action α_ρ, and $\partial_{c_\phi \rhd \alpha_\phi}(\phi)$ is the derivative of the process ϕ with respect to the action α_ϕ. Finally, in order to obtain the result S of calculation $\rho \sqcap \phi$, the safety verification module solves the generated linear system E.

Once the linear system E is resolved, the safety verification module checks the following equality $S = \rho$. If it holds, the safety verification module guarantees the safety of the system. Otherwise, the result S corresponds to the safe operation that the train should perform, and it alerts the TOBC equipment to indicate that the train is malfunctioning, and whether or not a braking action should be performed.

4.3.4 Safety analysis

In this subsection, we carry out an ETcCBTC system safety analysis in order to demonstrate its effectiveness, as well as to illustrate its advantages in comparison to existing TcCBTC systems.

- In the proposed ETcCBTC system, the OSPM monitors train speed against speed limit, and the proposed safety verification module monitors also the train operation in parallel with OSPM, which doubles the safety of train control. In addition, even if the OSPM fails to monitor the train speed, the safety checking module does, which always guarantees the safe control of train operation.

Algorithm 1 Safety checking process

Require: P: Expressions of estimated train behaviors; Φ: expression of safety policy ; V_{SBC}; V_{EBC}; MAL;

1: alert-signal $\leftarrow$ false;
2: $V \leftarrow S_i$;
3: $L \leftarrow l_i$;
4: Obtain the current train behavior ρ from all estimated tain behaviors;
5: **while** (alert-signal = false) **do**
6: $\rho \sqcap \Phi = \sum_{(\alpha_\rho,\ \alpha_\Phi)\in\delta(\rho)\times\delta(\Phi)}(c_\rho \wedge c_\Phi) \rhd u(\alpha_\rho,\ \alpha_\Phi).(\partial_{c_\rho \rhd \alpha_\rho}(\rho) \sqcap \partial_{c_\Phi \rhd \alpha_\Phi}(\Phi))$;
7: $E \leftarrow \rho \sqcap \Phi$;
8: **while** exists expression equivalent to $\rho_i \sqcap \Phi_i$ in the right member of any equation in E that does not appear in the left limb **do**
9: $E \leftarrow E \cup \sum_{(\alpha_\rho,\ \alpha_\Phi)\in\delta(\rho_i)\times\delta(\Phi_i)}(c_\rho \wedge c_\Phi) \rhd u(\alpha_\rho, \alpha_\Phi).(\partial_{c_\rho \rhd \alpha_\rho}(\rho_i) \sqcap \partial_{c_\Phi \rhd \alpha_\Phi}(\Phi_i))$;
10: **end while**
11: Find S the solution of resolution of linear system E
12: **if** $(S = \rho)$ **then**
13: alert-signal $\leftarrow$ false;
14: Go to 2;
15: **else**
16: alert-signal $\leftarrow$ true;
17: **end if**
18: **end while**
19: **Return** alert-signal;

- The data sources for monitoring train operation by OSPM and the safety verification module are the same, thus, this allows to avoid false alarms. Therefore, ETcCBTC allows to ensure a safe train control with quality of service.
- Compared to the conventional TcCBTC system, which relies only on balises to obtain train location information, the proposed ETcCBTC system allows a dual localisation of trains by using both the balises and GPS. Therefore, this allows to localize a train with a higher level of precision, which is critical to guarantee the safety of the system operation.
- The proposed safety checking method not only makes it possible to detect situations of violation of proper operation of the train, but also it allows to propose the safe behavior that the train should perform.

4.4 Performance study

In this section, we evaluate the performance of the proposed ETcCBTC system. We perform a comparison with two conventional systems, namely, CBTC system [85] and TcCBTC system [105] to highlight the efficiency of our solution. In what follows, we describe the simulation parameters, the performance metrics, and finally, we discuss the obtained results.

4.4.1 Simulation parameters

The efficiency of the proposed ETcCBTC system is investigated by means of extensive simulation tests, which we have developed under Matlab environment [4]. The network consists of trains moving on rails with a speed of 430 $km/\ h$. The APs are deployed on the railway line with an average distance of 600 m between them. The scenario is generated by varying the number of trains. We assume that the trains have the same hardware characteristics and processing capabilities. The simulation duration is of 100 s and the obtained results are the average of 25 simulated independent iterations. The simulation parameters are summarized in Table 4.2. Most used simulation parameters are inspired from [87, 104]. The implementation is carried out by programming the operations of each CBTC's component, including the Automatic Traffic Supervision (ATS), the ZC, the on-board computer and communication system. Doing the same also for each component of the TcCBTC system like VOBC, ATS, track-side OCU and communication system.

Parameter	Value
Simulation duration	100 s
Observation area	5000 m^2
Number of trains	{1, 2, 3, 4, 5, 6, 7, 8}
Speed of trains	430 $km/\ h$
Speed on service braking curve	450 $km/\ h$
Speed on emergency braking curve	480 $km/\ h$
Acceleration rate	0.75 m/s^2
Service braking rate	0.85 m/s^2
Emergency braking rate	0.95 m/s^2
Data packet length	400 byte
Data transmission rate	11 $Mbit/s$

Table 4.2: Simulation parameters

We were interested on four important performance metrics, namely, (1) the response time, (2) the transmission load, (3) the safe operation rate, and (4) the safety checking success rate. Through the response time, we analyze how well the proposed system satisfies the most stringent requirement of the rail systems in terms of delays, which is of the most importance in safety-critical systems. Indeed, the sooner a train receives control decisions made by the control system, the more time it will have to react correctly. Through the transmission load, we analyze how well the proposed system optimizes the communication overhead. Optimizing the number of messages exchanged makes it possible to meet with the most restrictive characteristic of rail transport in terms of high mobility of trains. Through the safe operation rate, we analyse how well the proposed system provides safe and efficient train control. Through the safety checking success rate, we evaluate the success percentage of the proposed safety checking method.

4.4.2 The obtained results

4.4.2.1 Response time

This simulation is conducted to discuss the impact of the connected train number on the response time metric. The response time covers the simulation of train movement, train control algorithm, communication, speed monitoring, and safety checking.

In Fig. 4.5, we illustrate the response time of the proposed system and the concurrent systems in function of the train number. We note that when the number of connected

trains becomes high, the response time increases for all the compared systems. Indeed, the obtained results show that the performance of our system is clearly higher compared to the other systems. Regarding the CBTC system, each train sends its status information to the ZC, then it waits to receive an MA. The ZC waits then to receive the locations of the trains that are within its control area before calculating the MA of each train and sending it. This implies a higher response time, which continues to increase with the number of trains. Furthermore, the retransmissions between the ZC and trains in the event of communication errors lead to a considerable response time. In the TcCBTC system proposed by Wang et al. [105], the checking of the safe operation of the VOBC equipment is carried out through an important series of calculations of topology theorems, which implies an increase in response time with the increase of train number. However, in our system, the safety policy generation phase and the train behavior detection phase of the safety verification method contain a minimal amount of calculations, and the verification of a train behavior inclusion in the safety policy is executed in a single operation with less computation. Therefore, thus reducing considerably the response time.

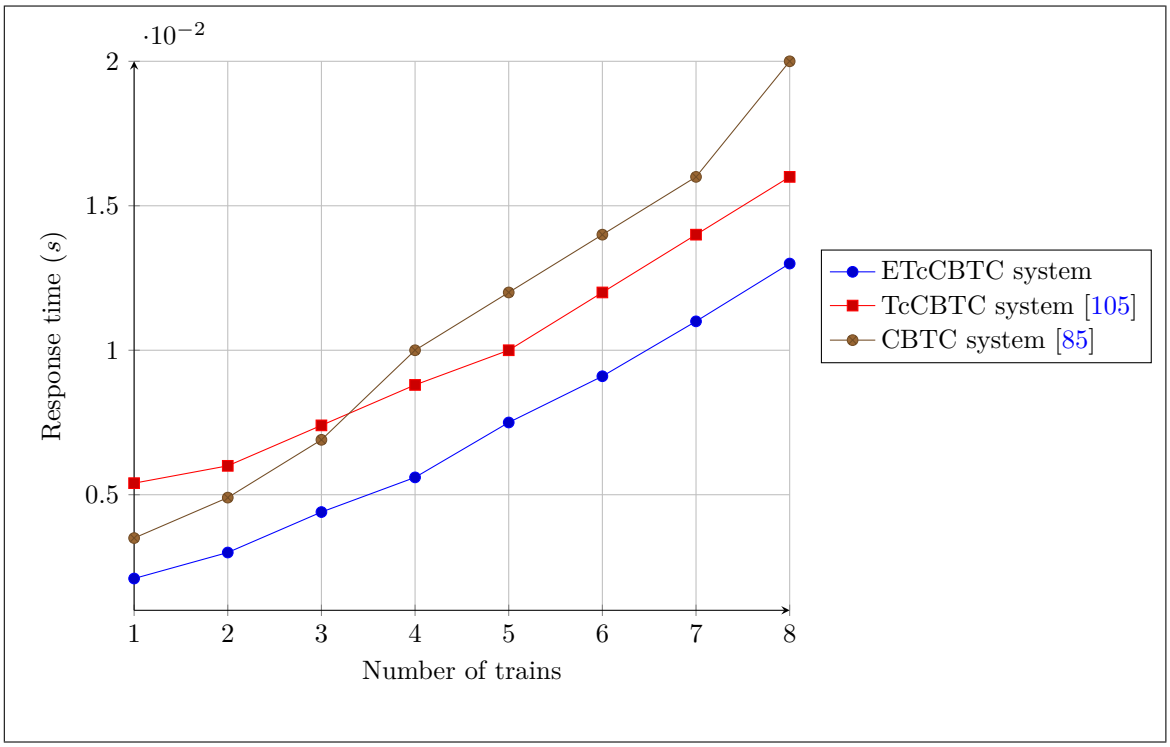

Fig. 4.5: Response time versus trains number.

4.4.2.2 Transmission load

In this simulation, ETcCBTC system and the two concurrent systems are assessed and compared in terms of the transmission load metric.

In Fig. 4.6, we illustrate the transmission load of the proposed system and the concurrent systems in function of the connected train number. We note that when the train number increases, the number of bytes exchanged increases for all compared systems. Regarding the obtained results, our system and the TcCBTC system proposed by Wang et al. [105] have the same transmission load and they show better performance compared to the conventional CBTC system. In the latter, the transmission load remains important. This is due to the broadcasted packets between the trains and ZC in order to generate the MAs. However, for our system and the TcCBTC system proposed in [105] the transmission load is lower. This can be explained by the fact that the MAs are generated by the trains themselves without an intermediate equipment, which decrease the number of communication rounds and the amount of data transmitted. Indeed, the necessary information for MA calculation is sent directly from the front train to the back one. Hence, the train-centric CBTC systems are efficient compared to the CBTC system given the amount of data to be exchanged per unit of time and the connected train number.

The obtained results show that even in high traffic density, the proposed train control system shows very satisfactory results in terms of transmission load and response time, which allows it to be suitable as a railway control system.

4.4.2.3 Safe operation rate

In this simulation, the performance of the proposed system and that of two concurrent systems are compared in terms of the train safe operation rate.

In Fig. 4.7, we illustrate the safe operation rate in function of the OSPM failure probability. We note that the train safe operation rate in the case of the conventional CBTC system and the TcCBTC system proposed in [105] decreases rapidly by increasing the probability of OSPM failure. However, the train safe operation rate in the case of our system remains stable at 100 % whatever the probability of OSPM failure. This is explained by the fact that the OSPM failure probability does not affect the operation of the system, where the proposed safety checking method alerts the TOBC equipment to indicate that the train is malfunctioning, and it should perform a braking action. Regarding the two concurrent systems, when a train exceeds the speed limit, it solicits

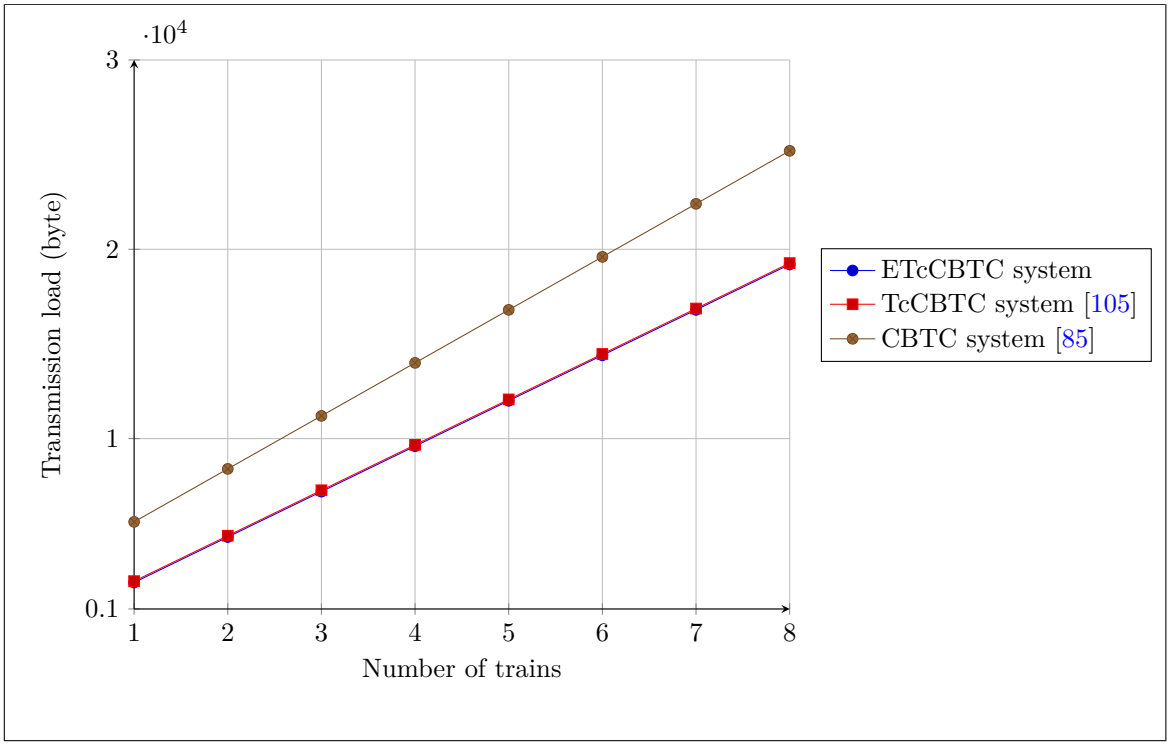

Fig. 4.6: Transmission load versus train number.

the OSPM and if the latter is down, it can issue an unsafe train control, which affects the train safe operation.

4.4.2.4 Safety checking method efficiency

In this last simulation, the performance of the proposed safety checking method is evaluated. To do this, we have measured the check success and false alarm rates over the time. The check success rate indicates the ratio of the number of detecting safe operation violation situations to the total number of safe operation violation situations. The false alarm rate indicates the probability that the method wrongly indicates a safe situation as an unsafe one.

In Fig. 4.8, we illustrate the check success and the false alarm rates in function of time. We note that throughout the train's movement, the check success rate remains very high with a percentage always equal to 100 %. The proposed safety checking method continuously verifies the train operation through a maximum number of train operation states before being ignored or the system being failed, and hence, maintaining a complete successful rate.

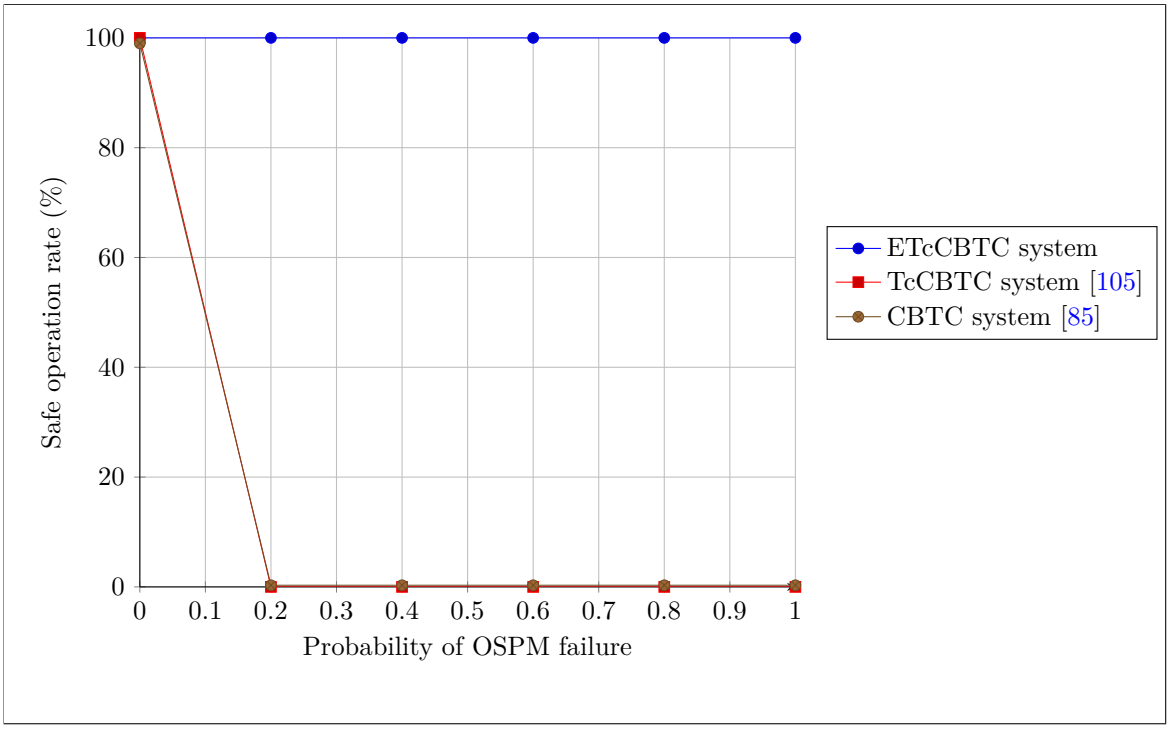

Fig. 4.7: Safe operation rate versus probability of OSPM failure.

4.5 Conclusion

Train control systems have become crucial for assuring the operational safety of trains. Designing an effective architecture for such systems and monitoring their behavior to avoid any operation failure are a major way to guarantee a high level of rail traffic safety. In this chapter, an enhanced train-centric communication-based train control system for railway transports is proposed. This system allows improving the quality and enhancing reliability of the train control. An improved architecture is defined, allowing a dual localisation of trains by using the balises and GPS. To guarantee safe operation of ETcCBTC system, we have then developed a process algebra based formal verification method, which is integrated into the TOBC equipment. The main goal of the verification method consists of the detection of violation situations of the proper train operation during its movement. We have carried out simulations to evaluate the effectiveness of ETcCBTC compared to CBTC and TcCBTC regarding the train safe operation rate, transmission load and response time. Regarding the obtained results, ETcCBTC is 100 % more effective in terms of train safe operation under OSPM failure, 66 % more effective in terms of response time, and 56 % more effective in terms of transmission load.

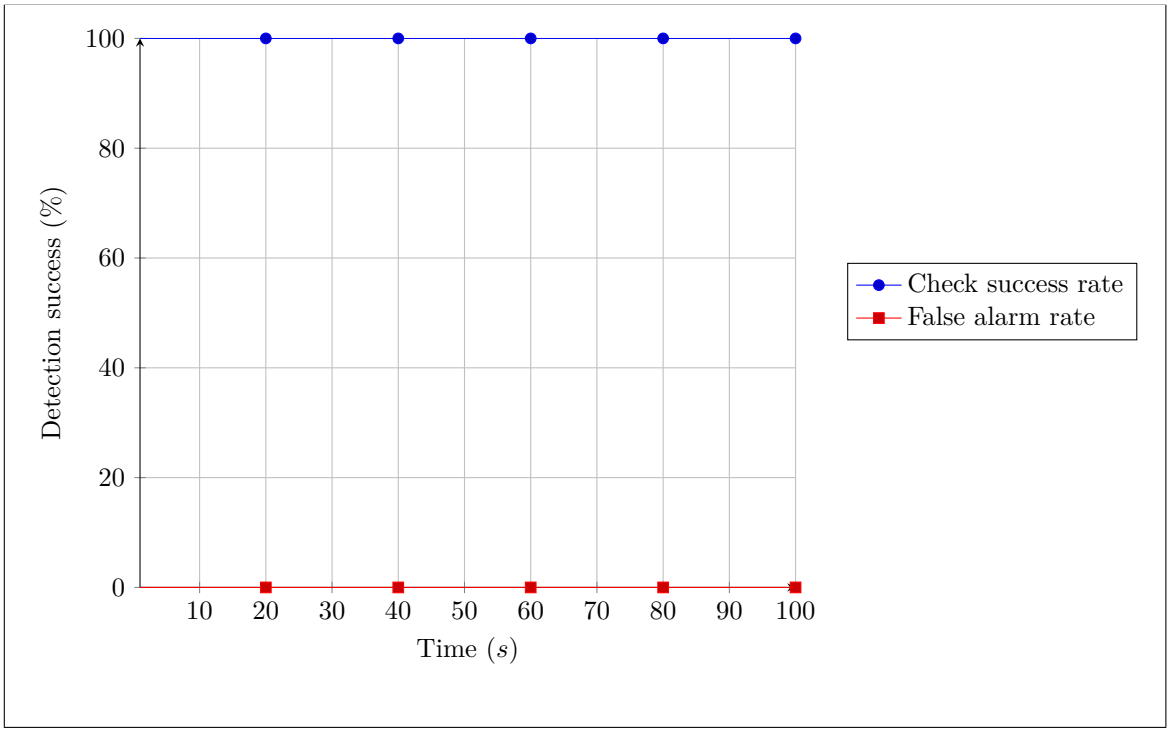

Fig. 4.8: Check success and false alarm rates of our safety checking module versus time.

Chapter 5

Highly Efficient Approach for Discordant BSMs Detection in Connected Vehicles Environment

5.1 Introduction

Connected Vehicles (CVs) are key enabling technology in Intelligent Transportation Systems (ITSs) that introduces great opportunities of improving traffic safety and efficiency. The emergence of CVs technology provides several interesting safety applications. These applications rely on broadcasting of messages by every vehicle on the road. Basic Safety Messages (BSMs) are the most important messages type used in vehicular safety applications. However, several critical issues affecting the BSM messages reliability. In this chapter, we present a *highly efficient discordant BSMs detection model-based approach* proposed for CVs, which prevents disturbance of vehicles. This approach consists of detecting incoherence in BSM metrics values. The proposed approach is based on data anomaly detection using Gaussian distribution approach. This part of our work was the subject of a research paper cited in [116]. This chapter is organized as follows. In Section 5.2 , we discuss the problem statement, where we give also our objectives. In section 5.3, we present the detailed description of our approach as well as the complexity analysis. We evaluate the performances of the proposed solution through simulations with respect of important criteria in Section 5.4. Finally, we conclude this chapter in Section 5.5.

5.2 Problem statement

In the safety-related applications, the most important type of messages used is the BSMs, which is used in V2V communication to announces vehicular information regularly. However, this applications are facing plenty of critical issues that affect the reliability of the information transmitted, namely, open uncontrolled environment, high message rates, unreliable channel quality, etc., which can have serious consequences on human lives, the vehicle itself, and threats to the safety of transportation systems. Accordingly, a key requirement of such safety applications is the validity and reliability of messages diffused. The problem at hand in this chapter is to mitigate the disruption risk of vehicles through detecting the fake messages transmitting from disruptive vehicles. We consider a network model composed of a set of CVs sharing a stretch of road exchanging with each other BSMs, where one or a coalition of disruptive CVs trying to isolate a CV victim by making it overloaded. The impact of such an action would have serious consequences that can endanger the human life. In the fact the CV victim cannot get or communicate its safety messages, it could induce the other CVs perceiving inaccurate information about its physical proximity. Several communication parameters (BSM metrics), namely, the session duration, data rate, packets number, etc. can be maliciously employed by disruptive vehicle to disrupt the CVs communication. As illustrated in Figure 5.1, the disruption risk (discordant message) increases from the moment the BSM metrics take non-standard or statistically unusual values. In the following points, we explain how certain BSM metrics can reveal an unsafe message:

- Period (P) represents the time period of the communication session. The duration of a given session can reveal a disruptive behavior. The disruptive vehicle may try to expend or reduce the exchange duration over the time to occupy as long as possible the vehicle victim or to prevent the correct reception of safety messages.

- Packet number (N) represents the estimated number of packets to send during the communication session. The incoming traffic intensity should be carefully assessed. The higher is the number of packets, the higher is the risk being involved in a disrupt situation. Also, a decrease in the packets normal number causes a missing in information, which leads to incorrect safety messages.

- Rate (R) represents the estimated rate of packet transmission per second. This metric indicates the frequency of session's packets generation. This metric should be jointly assessed with the communicating vehicle distance (D). A disruptive behavior can be suspected if the frequency of data transmission does not square

with the distance D, where the higher data rate from a distant vehicle or the lower data rate from a near vehicle result in risks.

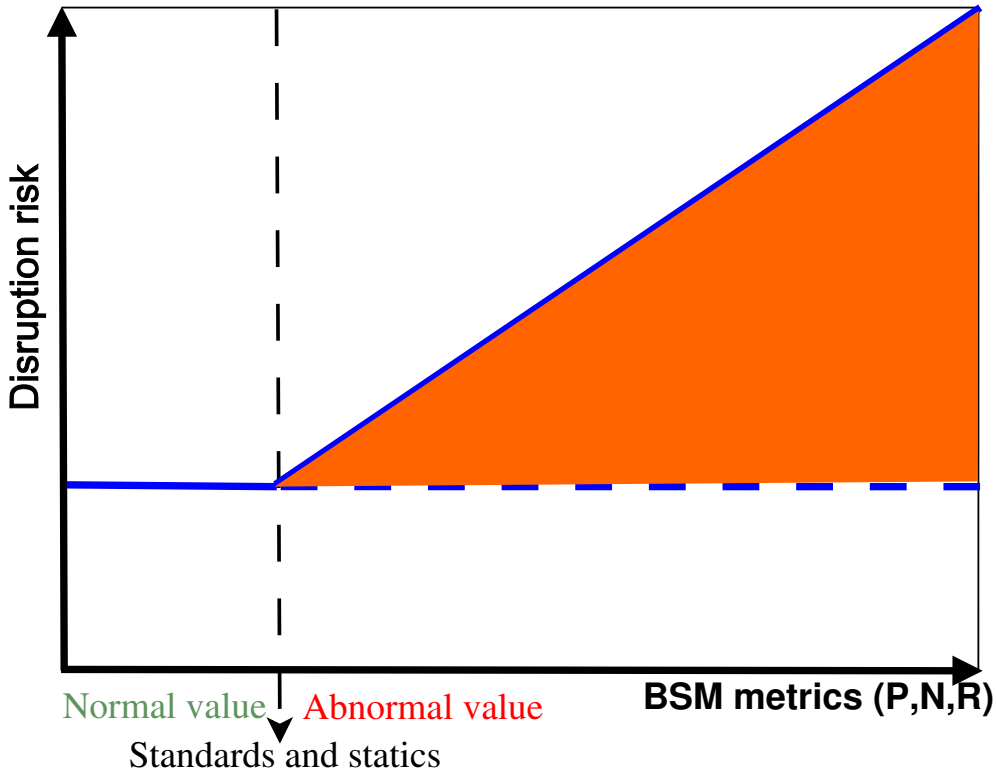

Fig. 5.1: Disruption risk in function of BSM metrics.

With the aim to deal directly with that, our key idea is to build a model that characterizes the values of the normal BSM metrics, then use this model to evaluate the metrics of new incoming messages. In fact, several solutions have been proposed in the literature for BSMs-based applications in CVs environment. However, various challenges still need to be investigated. It has been noted that some existing solutions are specifically addressing the reliability of BSM messages in term of their content without considering its validity. Furthermore, most of the proposed solutions rely on the use of a centralized infrastructure that is not practical to cope with high traffic density. Moreover, most other existing solutions present limitations as they are much more complex that increase the deployment cost, and present performance limits. From this observation, our proposal has two major objectives: 1) designing an incoherence detection technique by elaboration of a BSM traffic model from statistical standard values of BSM metrics, using data anomaly detection where the vehicle receiver rejects

an incoming message if the its metrics do not fit the normal distribution model and 2) dealing with high traffic density by not relying on any centralised infrastructure such as RSU, and avoiding overhead of costly technologies in terms of hardware by not relying on any additional expensive equipment.

5.3 Our proposed approach

In this section, first, we present an overview of our discordant BSMs detection approach in connected vehicles environment, then we give the detailed description of its operation.

5.3.1 Overview

In this chapter, we give a detailed description of the proposed discordant BSM messages detection approach for CVs. This approach is based on incoherence detection in communications parameters among vehicles wile transmitting BSMs. In the context of our work, an incoherence is seen as the lack or excess of the BSM metrics values constituting an incoming message. The proposed approach aims to mitigate the disruption risk of vehicles by malicious BSMs. The main idea of our contribution is to build a normal values model of BSM metrics, then used this model to evaluate the values of BSM metrics of new messages. The proposed model is based on anomaly detection using Gaussian distribution approach. The latter is preferable in this work because being a probabilistic method, the impact of errors can be reduced and it can be used without additional interaction with the environment [58]. Our BSM traffic model is trained under normal values of BSM metrics of a set of communication sessions. A threshold value is then defined from the best performance of the model on a set of data. Any BSM metric being out of the threshold requirement, the message is considered as outlier. In this study, to decide whether to accept or reject an incoming message, the detection process makes use of the vehicles collaboration, which allows them to cross their prediction in order to achieve more precision. Through the complexity analysis, we have verified the efficiency of the proposed approach. Furthermore, in order to demonstrate the effectiveness of the proposed BSM traffic model with comparison to the machine learning-based methods such as Local outliers factor, Isolation forest, and One class SVM, we have conducted simulations using our generated dataset from real traffic. Moreover, through formal evaluation, the performance of the proposed approach is evaluated. The obtained results demonstrate better performance of the proposed

approach in terms of response time, transmission requirement, and communication overhead. The notations used with their meanings are summarized in Table 5.1.

Our work makes four major contributions, which are summarised in the following points:

1. We propose a new technique of invalidity detection of BSMs messages throughout the vehicle movement. In this context, a model-based detection approach is proposed to provide the vehicles with the ability to quickly and preemptively identify discordant safety messages and hence dealing against potential disturbances.

2. The proposed approach is not dependent on any infrastructure such as RSU, or expensive hardware such as lidar, radar, or cameras, it is deployed individually in the vehicle itself and executed in a decentralized manner.

3. The Gaussian distribution approach is used to design the BSM traffic model, thus assuring very high precision with a constant complexity, which is an advantage when compared to the machine learning-based algorithms that has a time complexity increases exponentially with the increasing of dataset size. The proposed model has good performance comparing with machine learning-based algorithms, which is tested by simulations on our VANET generated dataset.

4. The proposed approach is effective in terms of response time, transmission requirement, and communication overhead, which is demonstrated by formal evaluation, while providing a trade-off between efficiency and safety. Moreover, among the advantages of this approach are its ability to detect various attacks types, namely, Denial of Service (DoS), dropping and flooding.

5.3.2 BSM traffic model

The developed detection model is based on Gaussian distribution approach. The analysis unit is a set of representative BSM metrics of communications between CVs. The model is designed under coherent communication data. In other words, the model is trained on a set of standard values $\{x1,\ x_2, ...,\ x_n\}$ of each BSM metric $M_i \in \{M1,\ M_2, ...,\ M_k\}$ in order to model the normal distribution, where each metric is characterized by a distribution

$$N(\mu_{M_i},\ \sigma^2_{M_i}). \tag{5.1}$$

Notation	Description
v_i	Vehicle of identity i
sm_j	Safety message received from v_j
M	Data flow's metric
x	Value of data flow metric
μ_M	Mean of the metric M
σ_M^2	Standard deviation of the metric M
t	Threshold parameter
P	Period
N	Packets number
F	Frequency of data transmission
D	Distance between communicating vehicles
n	BSM messages number
m	Neighbors vehicles number
$\rho(M;\ \mu_M,\ \sigma_M^2)$	Metric M's probability distribution
$P_i(sm_j)$	Probability distribution of the message received from v_j computed by v_i
$\mathbf{P}(sm_j)$	Probability distribution of the message received from v_j

Table 5.1: Notations

Then, a threshold value is defined from the optimal performance value of the model. The metrics with probability less than the threshold report the message as abnormal. The assessment of disruptive behavior is made based on the anomaly detection outcome.

Let $X = \{s_1,\ s_2, ...,\ s_n\}$ be the set of the collected messages, which are the model's input. Each message is characterized by the following metrics: P, N, and F, which represent, respectively, the period, the packet number, and the frequency of data transmission. In order to obtain the probability distribution of normal BSM metrics, the parameters μ and σ^2 are computed for each metric: $\{(\mu_P,\ \sigma_P^2),\ (\mu_N,\ \sigma_N^2),\ (\mu_F,\ \sigma_F^2)\}$. μ and σ^2 are computed, respectively, as follows:

$$\mu_M = \frac{1}{n}\sum_{i=1}^{n} x_{i(M)}, \tag{5.2}$$

$$\sigma_M^2 = \frac{1}{n}\sum_{i=1}^{n}(x_{i(M)} - \mu_M)^2, \tag{5.3}$$

where $M \in \{P,\ N,\ F\}$ and n represents the messages number. The parameter μ represents the values average of the each BSMs metric. The parameter σ monitors

deviations from the BSMs metrics values mean, therefore, identifies violations. The next step consists to define the detection threshold t. The model and the threshold value that give the best performance will be downloaded to the vehicles. The approach we follow in the BSMs traffic model design is illustrated in Algorithm 2.

Algorithm 2 BSMs Traffic Model design

Require: Standard values of BSM metrics;

1: Split the data into training and validation set;
2: **for** each BSM metric M in training data **do**
3: Calculate $\mu_M = \frac{1}{n}\sum_{i=1}^{n} x_{i(M)}$;
4: Calculate $\sigma_M^2 = \frac{1}{n}\sum_{i=1}^{n}(x_{i(M)} - \mu_M)^2$;
5: **end for**
6: Select the threshold value using the validation data;
7: **Return** BSMs traffic model and the threshold;
8: Download the model and the threshold value to vehicles;

5.3.3 Incoherence detection approach

Let's consider two vehicles, where a vehicle v_j communicates its BSM messages to neighboring vehicle v_i (cf., Figure 5.2). Upon the vehicle v_i receives a BSM message from its neighbor v_j, it performs, first, an extraction of the metrics N, P, and F, which are computed, respectively, such as

$$N = \ count\ of\ transferred\ packets, \tag{5.4}$$

$$P = End\ time - Start\ time, \tag{5.5}$$

and

$$F = \frac{N}{P} \cdot \frac{1}{D}. \tag{5.6}$$

The latter metric should be jointly assessed with the communicating vehicle distance (D). That's why, we have considered

$$F = \frac{R}{D}. \tag{5.7}$$

Once extracted, the vehicle v_i evaluates the BSM metrics extracted by computing their probability distributions: $\rho(P;\ \mu_P,\ \sigma_P^2)$, $\rho(N;\ \mu_N,\ \sigma_N^2)$, $\rho(F;\ \mu_F,\ \sigma_F^2)$, where

$$\rho(M;\ \mu_M,\ \sigma_M^2) = \sqrt{2\pi\sigma_M^2}^{-1} \cdot exp^{-(x_{(M)}-\mu_M)^2/2\sigma_M^2}, \tag{5.8}$$

with $M \in \{P,\ N,\ F\}$. The metrics have their normal distribution, where each metrics takes a range of usual values. The probability distribution of the received message sm_j is computed by

$$\rho(sm_j) = \prod_{M\in\{P,\ N,\ F\}} \rho(M;\ \mu_M,\ \sigma_M^2). \tag{5.9}$$

Afterwards, the vehicle v_i contacts the neighboring vehicles, in its transmission range, to request the calculated probabilities of the message received from the vehicle v_j. The collaborative attack is out of scope of our work. Once the probabilities received, the vehicle v_i computes

$$\mathbf{P}(sm_j) = \rho(sm_j) \times \prod_{i=1}^{m} P_i(sm_j), \tag{5.10}$$

where m represent the number of the neighboring vehicles. Finally, $\mathbf{P}(sm_j)$ is compared to the threshold value t. If the probability $\mathbf{P}(sm_j)$ is lesser than the threshold parameter t, the metrics values are claimed to be an anomaly, which means that the vehicle v_j attempts to disturb the nearby vehicles. Therefore, the vehicle v_i interrupts immediately the communication with the vehicle v_j and puts the identity of the vehicle in a blacklist which will be shared between the vehicles of the communication network to prevent it from communicating in the network. Otherwise, the vehicle v_i receive the BSM message and depending on it, the vehicle decides whether or not to adjust its operation. The process of traffic observation is summarized in Algorithm 3.

5.3.4 Complexity analysis

In this sub-section, we present the time, communication, and storage complexity analysis of the proposed approach. The first concept points out the amount of computational time that our approach takes to decide of the safety of a communication session. The second concept indicates the maximum number of messages sent through the network at a given instant. Finally, the third concept indicates the number of parameters required to store. This complexity depends on two factors: (i) the number of the neighboring vehicles, and (ii) the number of the parameters required for the approach's operation.

- *Time complexity:* The BSM traffic model and the determination of the probability distributions of a given BSM message have a time complexity of $O(k)$, where k

Algorithm 3 Incoherence detection process performed by each vehicle

Require: Data flow;

for each received BSM message **do**
    Extract features from the message sm_j:
    $N =$ Count of transferred packets;
    $P =$ End time $-$ Start time;
    $F = (N/P)/D$;
    for each BSM metric $M \in \{P,\ N,\ F\}$ **do**
        Calculate $\rho(M;\ \mu_M,\ \sigma_M^2) = \sqrt{2\pi\sigma_M^2}^{-1} \cdot exp^{-(x_{(M)}-\mu_M)^2/2\sigma_M^2}$;
    end for
    Calculate $\rho(sm_j) = \prod_{M\in\{P,\ N,\ F\}} \rho(M;\ \mu_M,\ \sigma_M^2)$;
    Request from vehicles in transmission range the calculated probabilities of the same message received from the vehicle j;
    Determine the $\mathbf{P}(sm_j)$:
    $\mathbf{P}(sm_j) = \rho(sm_j) \times \prod_{i=1}^{m} P_i(sm_j)$;
    Compare $\mathbf{P}(sm_j)$ and the threshold value t;
    if $(\mathbf{P}(sm_j) < t)$ **then**
        Return Outlier metrics;
    else
        Return Normal metrics;
    end if
    if the message's metrics are normal **then**
        Receive the BSM message;
    else
        Block the message;
        Report the sender;
    end if
end for

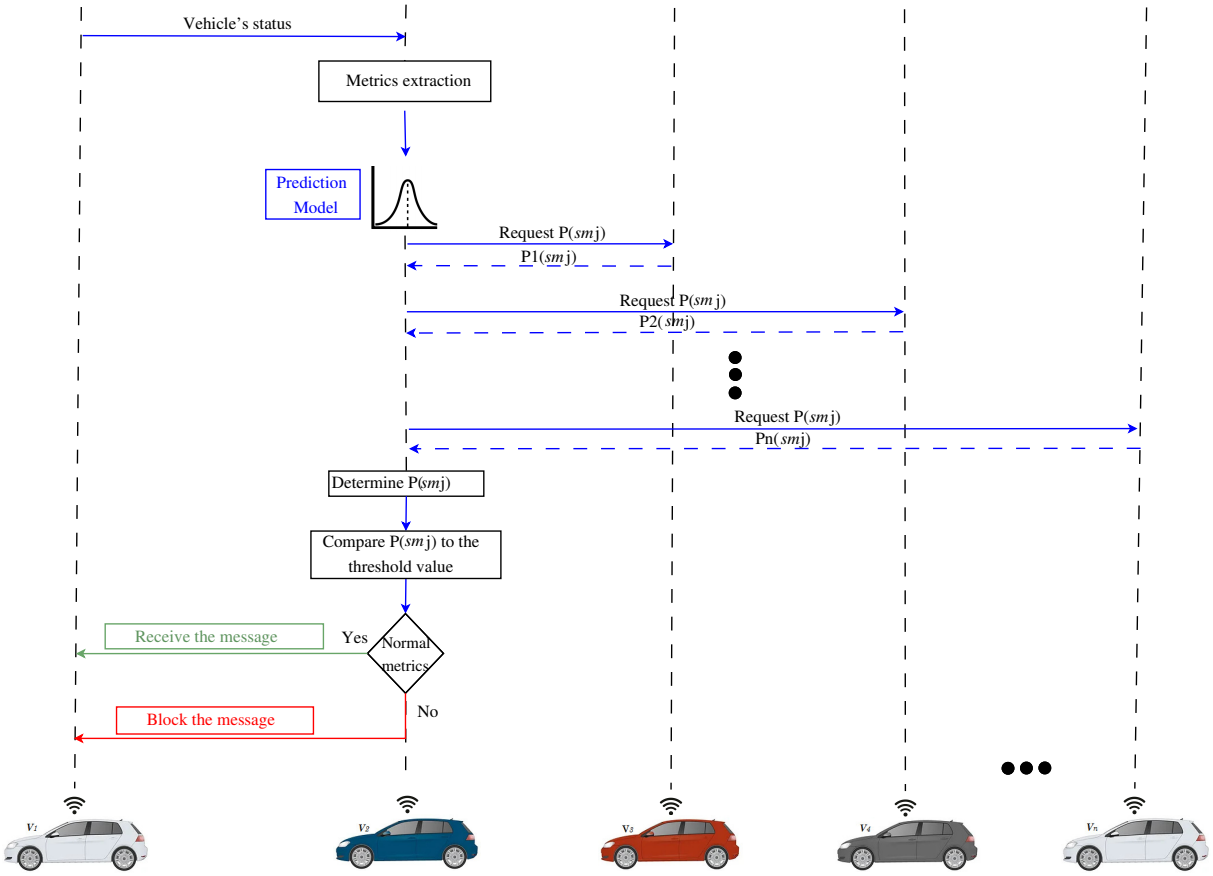

Fig. 5.2: Incoherence detection overview.

represents the total number of communicating vehicles in the network. The time complexity depends only on the number of neighboring vehicles. Therefore, the overall process takes a constant time complexity.

- *Communication complexity:* With the proposed approach, each vehicle will generate a request message to verify the normality of each received BSM message and forwarded it to the neighboring vehicles. Therefore, the communication complexity is $O(k)$, where k represents the number of BSMs received (the number of neighboring vehicles). As a result, these request messages will generate k response message from the neighboring vehicles. Hence, the overall communication complexity is of order $O(k)$.

- *Storage complexity:* In our approach, each vehicle in the network store the mean and the standard deviation of each of the three BSM metrics, and the threshold

parameter. Therefore, the required space is number of parameters multiply by the size of each parameter. The storage complexity is then $O(K)$.

5.4 Performance study

In this part, we evaluate through simulation the performances of the proposed BSM traffic model as well as the overall proposed approach. In what follows, we present the experiment settings and the obtained results.

5.4.1 Experiment setting

5.4.1.1 BSM traffic model efficiency evaluation

The simulations are carried-out using Sklearn package of Python. First, the BSM traffic model is trained under a dataset[1] containing anomaly-free communications traces generating from the Bologna city in Italy. This dataset contains the following BSM metrics.

- Start time is the time when the BSM exchange will start.
- End time is the time when the BSM exchange will end.
- Time period is the time duration of BSM exchange.
- Packets represent number of packets required by this request.
- Rate represents number of packets divided by time period.
- Sender stopping distance is braking distance of sender.
- Receiver stopping distance is braking distance of receiver.
- Actual distance represents distance between sender and receiver.
- Severity is the degree of the requested session emergency.

Then, in order to demonstrate the efficiency of the proposed model, the latter has been tested using our simulated dataset[2] containing communication traces under

[1] [Online]. Available: https://github.com/IhabMoha/datasets-for-VANET/tree/master/Bologna
[2] [Online]. Available: https://github.com/Djamila-Zamouche/Dataset-of-VANET-communication-traces

disturbances. The dataset is generated from simulation of a real traffic scenario using a compound of two software, the vehicular mobility generator SUMO (Simulation of Urban Mobility) [10] and NS-3 (Network Simulator v. 3.29) [29]. We have generated the mobility scenario using SUMO combined with OpenStreetMap [8] by simulating a traffic area of 25 km in the Bologna city (Italy), as shown in Figure 5.3. The resulting mobility traces file is then considered as input file to the NS-3. The communications between the vehicles is designed on the NS-3. The VANET environment consists of 300 vehicles, which including 15 malicious ones conducting malware activities. The steps of the conducted simulations are outlined in the flowchart of Figure 5.4.

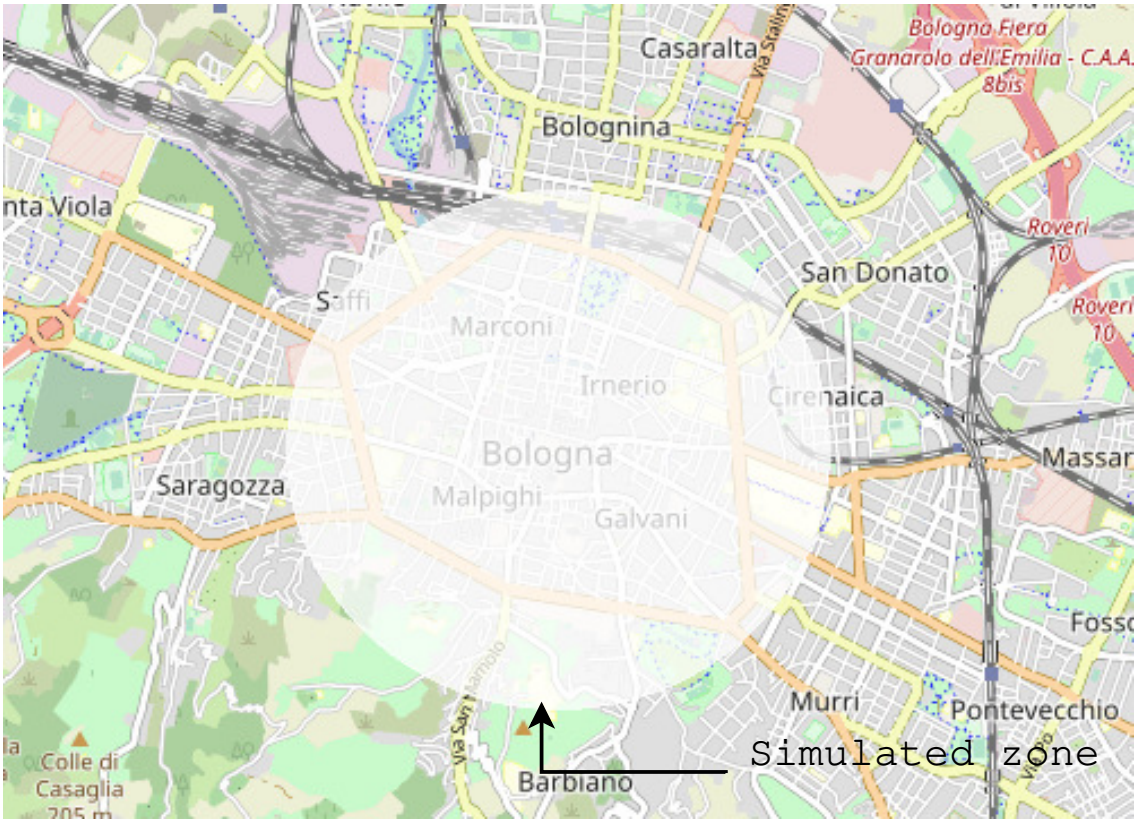

Fig. 5.3: Traffic simulation area.

First of all, we performed features filtering by handling redundancies, filling missing values, and identifying the most relevant features through attributes ranking. We carried-out this part using Weka [6]. The features that we considered are the period, packet number, and rate because of their ability to reveal the abnormal behaviors. The rate is jointly assessed with the distance feature. The others generated features are eliminated.

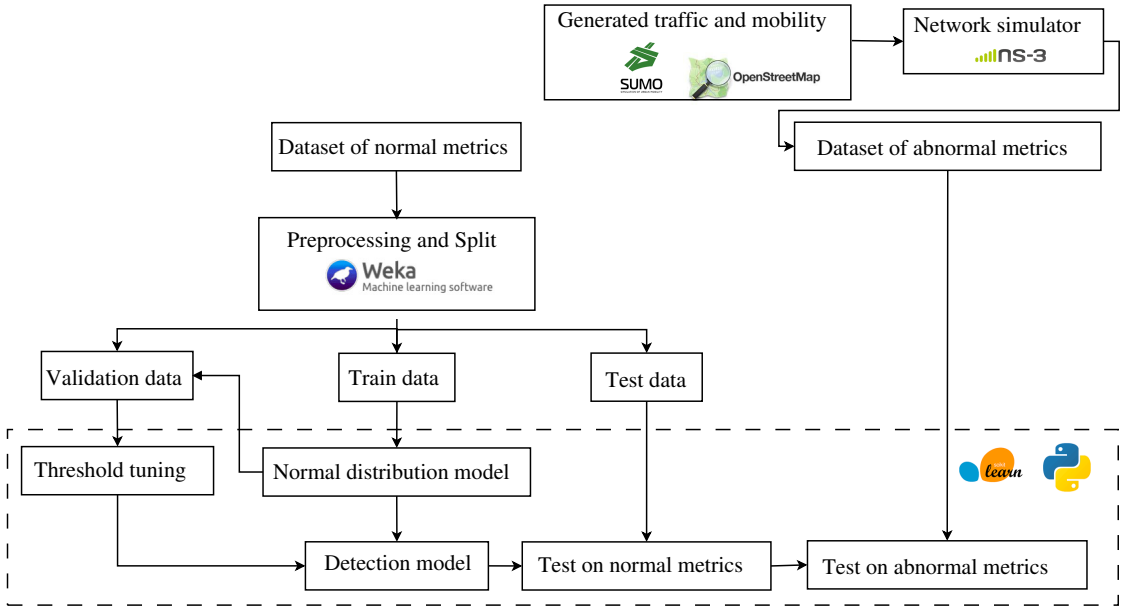

Fig. 5.4: Flowchart of the simulation steps.

The performances of our model are evaluated through different metrics, namely, precision, accuracy, recall, and f1 score.

- Recall: it is defined as the ratio of correctly identified malicious messages to all the malicious ones.

$$Recall = \frac{TP}{TP+FN} \times 100\% \tag{5.11}$$

- Precision: it represents the ratio of correctly identified malicious messages to the number of all the ones identified as malicious, which includes also wrongly identified malicious messages.

$$Precision = \frac{TP}{TP+FP} \times 100\% \tag{5.12}$$

- Accuracy: it represents the ratio of correctly identified malicious messages to the total number of messages.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FP} \times 100\% \tag{5.13}$$

- F1 score: it is defined as the harmonic average of precision and recall.

$$F1\ score = \frac{Precision \times Recall}{Precision + Recall} \times 2 \tag{5.14}$$

where, TP, FP, TN, and FN refer to True Positive, False Positive, True Negative, and False Negative, respectively.

5.4.1.2 Formal specification of our approach and evaluation

Here, we conduct a formal evaluation of our approach using process algebra. The latter provides a means to build a model describing the overall operation of our approach and the correct operations' sequencing, which allows deriving a correct formula of performances measures. We were interested on three important performance metrics, namely, the response time, the transmission requirement, and the communication overhead. Through the response time, we evaluate how well the proposed approach satisfies the most stringent requirement of the safety-related applications in terms of delays. Through the transmission requirement, we evaluate the bandwidth demanded by vehicular communication in the communication channel. Through the communication overhead, we quantify how well the proposed approach optimizes the number of messages exchanged, which makes it possible to meet with the most restrictive characteristic of CVs in terms of high mobility.

We propose Conditional Basic Process Algebra with Communication ($CBPA-C$), an extension of the $CBPA^{*}_{0,1}$ language, which we have described in Chapter 2, via the inclusion of communications and timing information by using variables associated with each action in order to express its duration. The syntax of $CBPA-C$ is defined as follows:

$$P ::= 0 \mid 1 \mid c \rhd \alpha \mid P_1 + P_2 \mid P_1.P_2 \mid P_1^*.P_2 \mid P_1||P_2 \mid \bar{\chi}.\gamma \mid \langle \tau \,\square\, \alpha \rangle \bullet P \tag{5.15}$$

where

- $P_1||P_2$ represents the parallel composition of two processes P_1 and P_2.
- $\bar{\chi}.\gamma$ represents the sequential composition of emission $\bar{\chi}$ and reception γ.
- $\langle \tau \,\square\, \alpha \rangle \bullet P$ indicates a process that can execute action α for a period of time τ, then its behavior becomes the same as P. "$\bullet$" is a prefix operator.

We perform a design of the model of our approach by specification their overall operation. We model by the operation of the receiver vehicle of BSM messages by the process R and its neighbors by the process N, then the global model being a simple sequential composition of these processes. The formal description of the proposed approach is as follow:

$$\Delta ::= \begin{cases} R ::= ((\langle \tau_{ext} \ \square \ \alpha_{ext} \rangle \bullet P.\langle \tau_{detc} \ \square \ \alpha_{detc} \rangle \bullet P) || \langle \tau_{diff} \ \square \ \alpha_{diff} \rangle \bullet P_i).N(v_1, ..., v_m) \\ \qquad .\langle \tau_{det} \ \square \ \alpha_{det} \rangle \bullet P.(\langle \tau_{check} \ \square \ \alpha_{check} \rangle \bullet P.(A + N) \rhd \langle \tau_{resp} \ \square \ \alpha_{resp} \rangle \bullet P \\ \\ N ::= \gamma \rhd \langle \tau_{emis} \ \square \ \bar{\chi} \rangle \bullet P \end{cases}$$

where, m represents the number of neighboring vehicles. The τ_{ext}, τ_{detc}, τ_{diff}, τ_{det}, τ_{check}, and τ_{emis} correspond, respectively, to the time of the metrics extraction, BSM traffic model application, request message diffusion, flow's probability determination, flow checking, communication.

From the model specification, we note that the receiver vehicle of BSM messages performs the broadcast of the request message in parallel with the metrics extraction and the model application. Consequently, the response time metric is derived such as:

$$T = \tau_{ext} + \tau_{detc} + \tau_{comm} + \tau_{det} + \tau_{check} \tag{5.16}$$

The time of metrics extraction τ_{ext} and the model application τ_{detc} depends on the number n of BSM messages received. Thus, the response time is calculated such as:

$$T = \sum_{i=1}^{n} (\tau_{ext} + \tau_{detc}) + \tau_{comm} + \tau_{det} + \tau_{check} \tag{5.17}$$

In order to obtain the execution time of the performed tasks, namely, τ_{ext}, τ_{det}, and τ_{check}, we have opted for a calculating the execution time of the elementary operations ($*$, $-$, $/$) performed in each task. We have calculated the elementary operation execution time on Python 3.7, on a machine, which operate upon Windows 64-bit system, running an Intel Pentium (R) Dual-Core CPU with frequency of 2.3 GHz and 4 Go random memory. The averaged results (on 25 runs) are presented in Table 5.2.

	Number of operations	Execution time ($\times 10^{-4}$ s)
MULT	1	3.6
SUB	1	3
DIV	2	4.24

Table 5.2: Average execution time of elementary operations.

The communication overhead is computed from the total amount of bytes exchanged by the vehicle receiving the safety messages and the neighboring vehicles. The communications overhead metric is calculated such as:

$$C = \lambda + (m \times \beta) \tag{5.18}$$

where, λ denotes the request message length that is set to 26 bytes, β denotes the response message length that is set to 32 bytes, and m represents the number of neighboring vehicles.

5.4.2 The obtained results

5.4.2.1 BSM traffic model's performance

In order to determine the optimal threshold value, we conducted an experiment, where the precision and recall metrics are evaluated using the anomaly-free dataset. The threshold value with which the highest precision and recall will be reached is the optimal value. Figure 5.5 presents the precision and recall curves in function of the threshold. As we can see in Figure 5.5, when the threshold equals to 10^{-13}, our model achieves the highest rate of precision and recall, which is equal, respectively, to 99 % and 85 %.

In Figure 5.6, we illustrate the performances of the model on both dataset in terms of precision, accuracy, recall, and f1 score. We note that the performance metrics remain very high with a percentage very close to 100% with both dataset. As Figure 5.6 shows, the precision with both dataset is, respectively, 100% and 99%. The recall with both dataset is 99% and 85%, respectively, and the f1 score is, respectively, 99.5% and 91.5%. It means that the proposed detection model has a good ability to distinguish abnormal behavior from normal one. Applying the proposed model with both dataset achieves, respectively, 99% and 85% on accuracy, which demonstrates the effectiveness of the proposed model. The higher the accuracy is, the more robust the defense mechanism.

As for our simulated anomaly dataset, we have compared our model with three machine learning-based models for anomaly detection, namely, local outliers factor, isolation forest, and one class SVM. As shown in Figure 5.7, our model is able to maintain a robust and high detection performance. It achieves improvement on the all metrics, namely, precision, accuracy, recall, and f1 score comparing to those three methods. These results confirm then the effectiveness of the proposed model in identifying the unsafe communication. Also, we have compared the execution time of

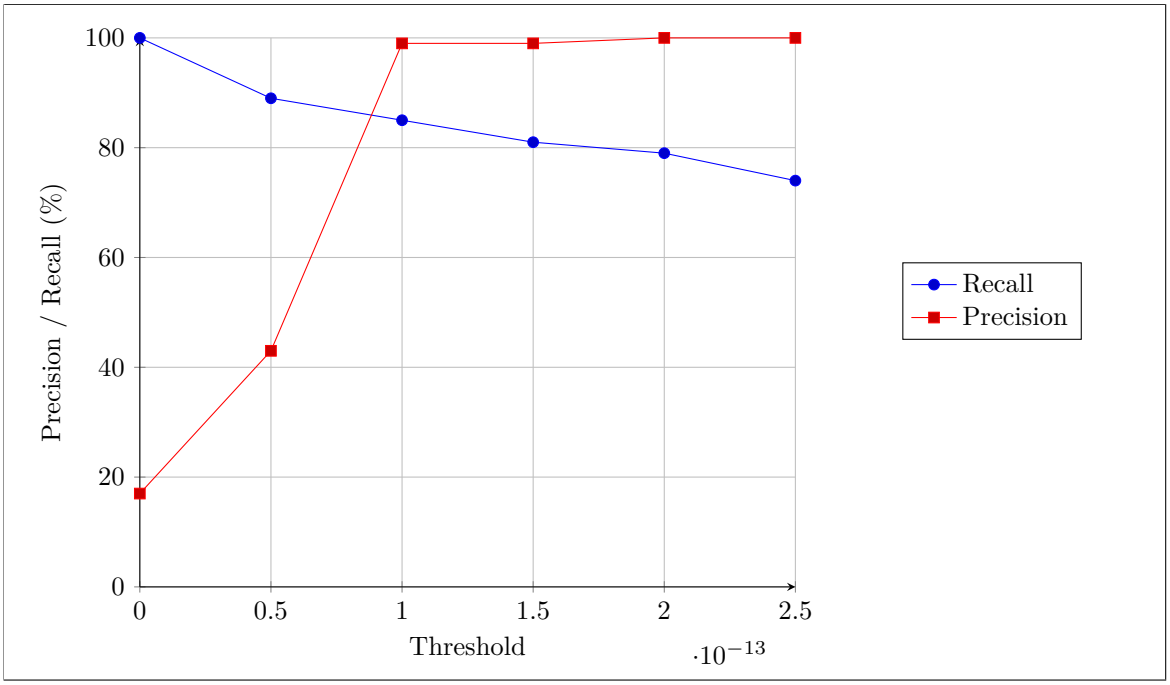

Fig. 5.5: The Precision / Recall versus the threshold.

the aforementioned methods where the obtained results are the average of 20 simulated independent iterations. As we can see in Figure 5.8, when the number of data flow becomes high, the execution time increases for all the compared models. Indeed, the obtained results show that the performances of our model are clearly higher compared to the other models. Consequently, the proposed model satisfies the real-time requirement of safety applications in terms of delays even in high traffic density.

5.4.2.2 The proposed approach's performances

Here, we discuss the performances of the proposed approach in terms of response time, transmission requirement, and communication overhead in function of the number of BSM messages n, and the number of neighboring vehicles m. To do this, we consider a scenario inspired from [89]. We consider a highway with 6 lanes (3 in each direction) of 3 m each. We assume a uniform presence of vehicles, with an inter-vehicle space of 30 m. Vehicles in movement transmit messages every 300 ms over a 300 m communication range. Considering a vehicle located in the middle of the highway, which corresponds to a maximum of received messages. Such vehicle can hear up to 120 vehicles per 300 ms, and the messaging rate in the communication network is 400 messages per

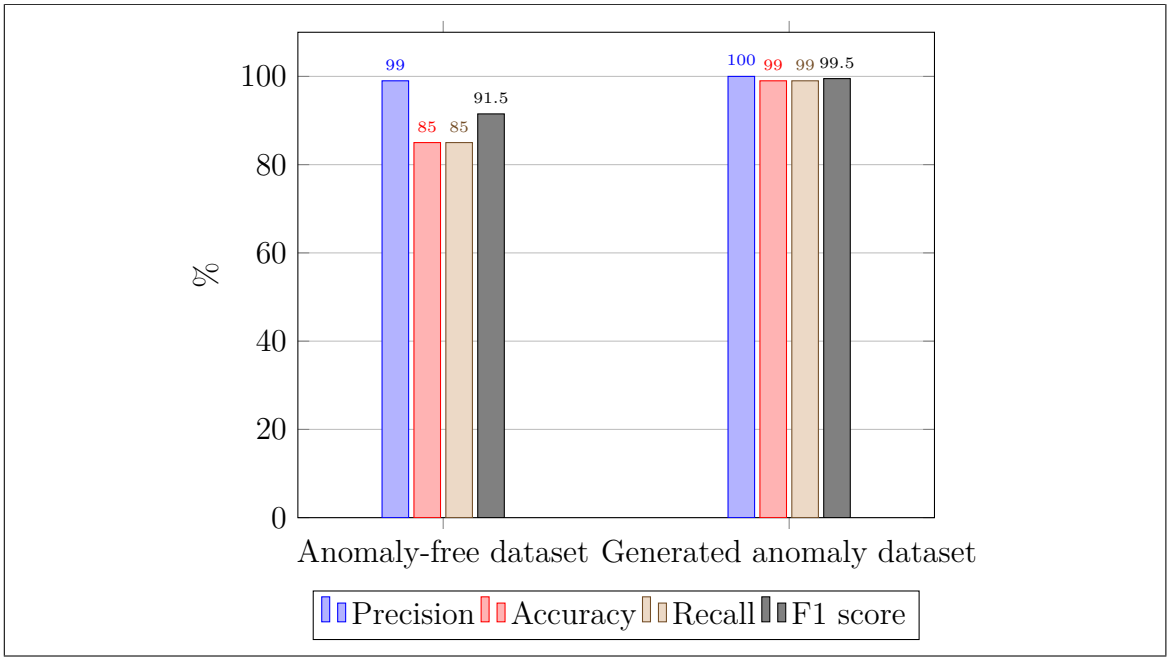

Fig. 5.6: The efficiency of the proposed model.

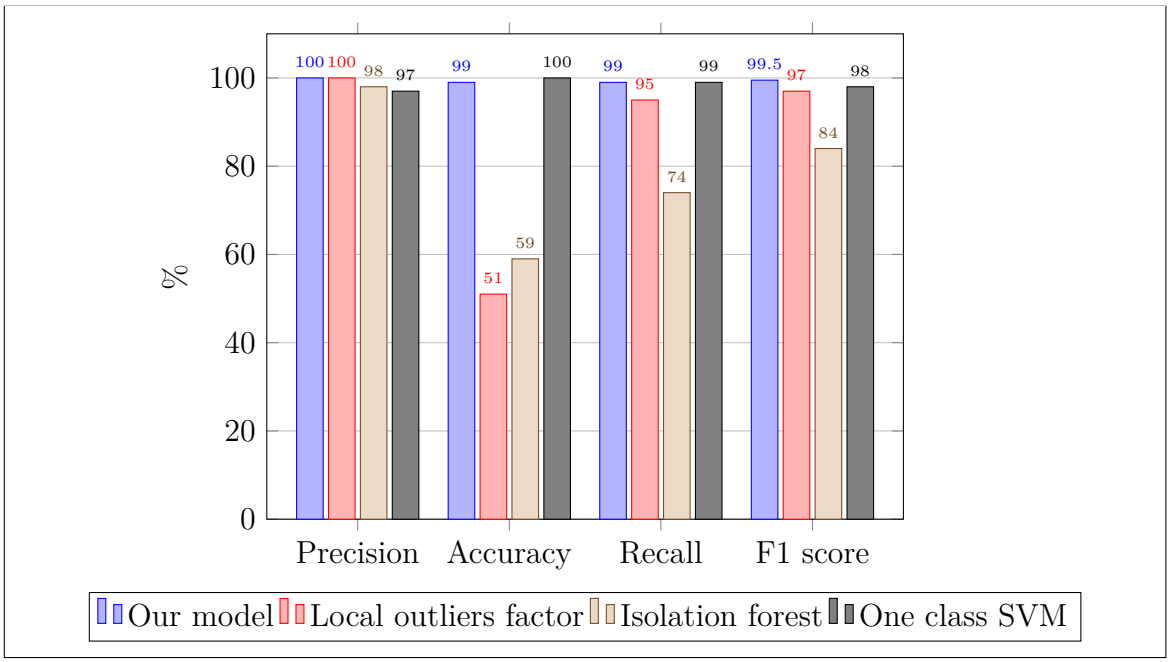

Fig. 5.7: Comparison of the detection efficiency on the generated anomaly dataset.

second. The BSMs messages size is set to 254 bytes. In Table 5.3, we illustrate the results achieved with our approach.

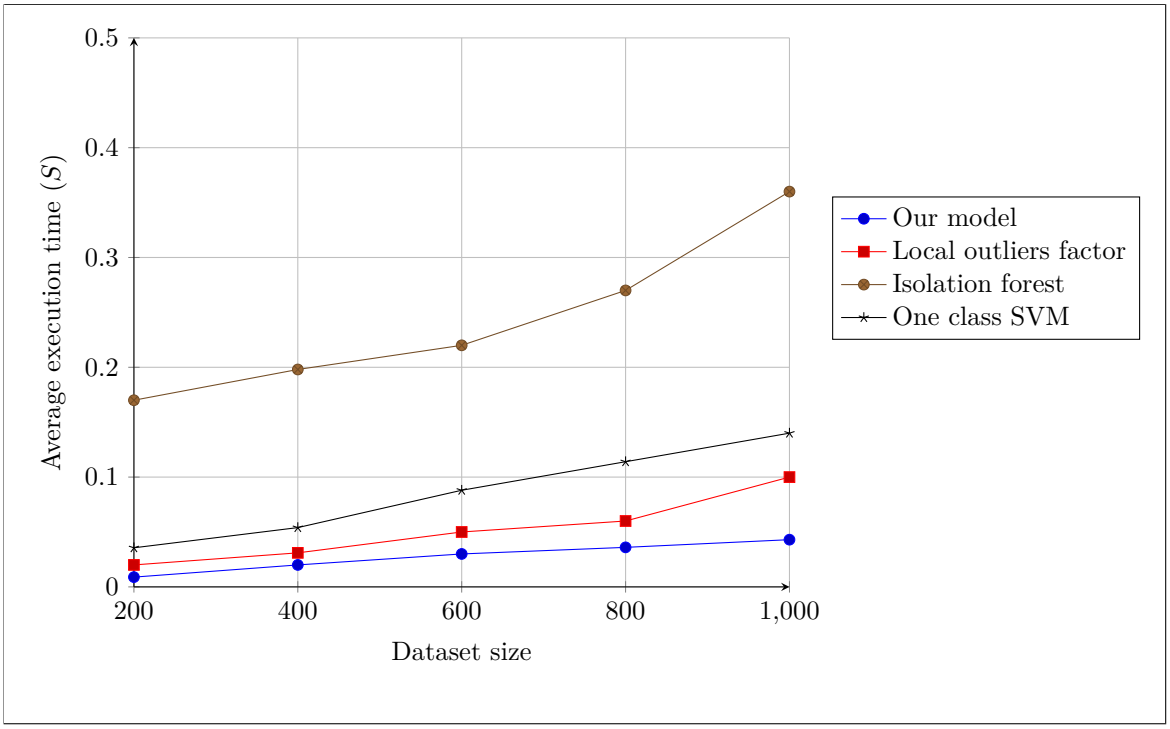

Fig. 5.8: Execution time versus simulated dataset size.

The driver reaction time to safety messages can be on the order of 700 ms or longer [73]. In high traffic where a vehicle may receive lots of messages per second (120 neighbors), the response time of our approach is 368 ms that is less to 700 ms, which will allow the vehicle to process all reliable incoming messages and dealing with all emergency situations. For the transmission requirement, the bandwidth demanded in the communication channel can be calculated in Mbps as [89] $w \times r_m \times s_m$, where w is the number of vehicles in the transmission range, r_m is the messages rate per vehicle, and s_m is the messages size. In our approach, transmission requirement is of 0.103 Mbps. For BSMs messages transmission, is amounts to a throughput of 0.812 Mbps. Therefore, the total transmission requirement is of 1 Mbps that is less than the minimum nominal capacity of DSRC, which is 6 Mbps. Consequently, our approach does not involves a transmission throughput that causes channel overload. Regarding the communication overhead, we note that the increase in the number of neighboring vehicles leads to a slight increase in the communication load in the network. Indeed, in our approach, the verification of the received messages requires a single request message of 26 bytes and m response messages of 32 bytes, which generates a very reduced number of bytes exchanged even in dense network scenarios.

	$m = 20$ $\Rightarrow n = 67$	$m = 40$ $\Rightarrow n = 133$	$m = 60$ $\Rightarrow n = 200$	$m = 80$ $\Rightarrow n = 266$	$m = 100$ $\Rightarrow n = 333$	$m = 120$ $\Rightarrow n = 400$
Response time (s)	0.062	0.12	0.183	0.264	0.3	0.368
Transmission requirement (Mbps)	0.017	0.034	0.051	0.068	0.086	0.103
Communication overhead (bytes)	666	1306	1946	2586	3226	3866

Table 5.3: Performances of the proposed approach.

5.5 Conclusion

The CVs technology allows several interesting safety applications. The BSMs-based applications play a crucial role in traffic safety and efficiency. In this chapter, a new discordant BSM messages detection approach is proposed, which consists of detecting incoherence in BSM metrics values. The proposed approach is based on data anomaly detection using Gaussian distribution approach. The main goal of this approach consists of dealing against potential disturbances, which allows improving the quality of traffic management. We have carried out formal evaluation to evaluate the effectiveness of our proposal regarding the response time, transmission requirement, and communication overhead. We have also conducted simulations to evaluated the efficiency of the proposed BSM traffic model, where the simulation results demonstrate that the model outperforms the concurrent machine learning-based methods, and achieve a promising performance regarding high precision, accuracy, recall, and f1 score.

Chapter 6

Conclusion and Future Directions

"The future is much like the present, only longer."

Dan Quisenberry

6.1 Conclusion

Intelligent Transportation Systems (ITSs) are systems in which communications, control, information processing, control algorithm, electronics, and other technologies are applied into transportation infrastructures. The universal purpose of ITSs is to provide innovative solutions relating to different modes of transportation to make transport safer, more convenient, and smarter. ITSs are based on the collection, processing, integration, and supply of information around vehicular networks, allowing the design a broad range of potential applications related to vehicles, traffic, drivers, passengers and pedestrians. Accordingly, two primary branches of services targeted for ITSs are created, namely, *infotainment applications* that are designed to provide more comfort and assistance to the driver and passengers e.g. Internet access, useful information about weather forecast, nearby point-of-interests, etc.; and *safety applications* that being the most critical objective of ITSs, aim at enhancing road traffic safety including collision avoidance services, accident notifications, and collection and distribution of information related to traffic road conditions. As such, ITSs have the potential to solve the most common challenges related to recent transportation systems such as heavy traffic congestion in large cities, poor traffic management, unreliable services, and so forth. Moreover, it is shown that ITSs have the possibility to act as a key factor for economic and environmental growth in many countries [13]. However, several issues restraining the proper deployment of these systems such as they are based in

several kinds of devices which can cause malfunction, extreme disturbances, several communication interfaces, etc. [18]. Consequently, one of the main challenge to be raised in these systems consists in contributing to enhance their security and safety level, while proposing effective mechanisms.

In the framework of the work described in this dissertation, the purpose was the proposal of new solutions aiming at enhancing ITSs reliability. The main motivation that is governed this thesis work was the proposition of an effective control system in railway transportation, and an efficient discordant safety messages detection mechanism for BSMs-based applications in connected vehicles environment. In the first part of this thesis, we have given a general overview of ITSs, describing their architecture, application as well as enabling technologies. Thereafter, we have devoted the rest of the chapter to introduce some challenges in ITSs environment and point out the security and safety aspects. In the second part of this thesis, we have provided a state of the art on the security and safety approaches of ITSs, where we have classified, surveyed, and compared them. In this context, we have proposed a new taxonomy of the reviewed solutions depending on the followed methods in which we have classified them into two main categories, namely: (1) approaches for railway ITSs, and (2) approaches for road ITSs. Afterwards, for each solution,we have described the main operation while discussing its advantages and shortcoming. Through the latter, we have drawn up comparative tables for each category according to different relevant criteria. In the third part of this thesis, we have presented our first contribution, which is an *enhanced train-centric communication-based train control system* for railway transport. The proposed solution allows improving the quality and enhancing reliability of the train control. To guarantee safe operation of the proposed control system, we've implemented a new safety-checking approach based on process algebra, which aims to track and correct in real-time the train behavior. In order to demonstrate the effectiveness of our proposal, we have analyzed its safety level where it presents a high level of safety compared to the TcCBTC system. In addition, the simulations, which we have developed, show that our proposed mechanism offers effective results in terms of important metrics with comparison to conventional systems. Finally, in the fourth part of this thesis, we have presented our second contribution, which is *a discordant safety messages detection strategy in connected vehicles environment*. Our solution is a decentralized model-based approach providing the vehicles with the ability to quickly and preemptively identify discordant messages and hence dealing against potential disturbances, while ensuring a trade-off between efficiency and safety. Moreover, among the advantages of this approach are its ability to detect various attacks types, namely,

Denial of Service (DoS), dropping, and flooding attacks. The proposed technique is based on data anomaly detection using Gaussian distribution approach. We have carried out formal evaluation to evaluate the effectiveness of our approach regarding important criteria, where the obtained results show that our approach offers effective results. Moreover, we have conducted simulations to evaluated the efficiency of the proposed model, where the simulation results demonstrate that the model outperforms the concurrent machine learning-based methods, and achieve a promising performance.

6.2 Future works

The work proposed in this thesis is an effort to enhance the security and safety of ITSs. Despite the fact that this work achieved encouraging results, there are many additional improvements and there are many challenges still remain to be solved to enable a highly efficient ITS. Therefore, based on the work fulfilled presented in this thesis, we can draw up several short and long term research perspectives. In the short term, we plan to work on the deployment and field testing of our train control system and discordant messages detection mechanism to validate their efficiency. we also plan to address the security challenges in road transportation that still remain to be solved to support and enable a highly secure ITS infrastructure and vehicular communications. In the long term, we plan the design of secure solutions to mitigate security flaws in the framework of other automotive cyber-physical systems, namely, railway transportation and aerial transportation, which raise several security vulnerabilities. Furthermore, another work will focus on the development of new safety methods and techniques for the deployment of an efficient ITS in the framework of aerial transportation. Another area of research will be centered on the design a fully autonomous trains using artificial intelligence techniques. The development of fully autonomous trains will lead to profound changes in the railway sector and it has become a major strategical competitiveness factor for industrialists.

References

[1] (2002). Federal Communications Commission. Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850 – 5.925 ghz Band. Technical report, FCC 02 – 302. [online] http://docs.fcc.gov/public/attachments/FCC-02-302A1.pdf.

[2] (2011). Report on the "Cognitive Control" Session. [online] https://mediatum.ub.tum.de/doc/1251373/file.pdf.

[3] (2018). Global Status Report on Road Safety. World Health Organizations. [online] https://www.who.int/publications/i/item/9789241565684.

[4] (2020). Matlab. [online] http://www.mathworks.com/.

[5] (2021). A Better Future Transformed By Intelligent Mobility. Intelligent Transportation Society of America. [online] https://itsa.org/wp-content/uploads/2021/06/6-24-21_ITSA-Tech-Blueprint.pdf.

[6] (2021). Machine learning software to solve data mining problems. [online] https://sourceforge.net/projects/weka/.

[7] (2021). National ITS Architecture Glossary. U.S. Department of Transportation. [online] http://local.iteris.com/northvalleyits/assets/National_ITS_Architecture_Glossary.pdf.

[8] (2021). Openstreetmap. [online] http://www.openstreetmap.org.

[9] (2021). Safety aspects — Guidelines for their inclusion in standards. International Organization for Standardization. [online] https://www.iso.org/obp/ui#iso:std:iso-iec:guide:51:ed-3:v1:en.

[10] (2021). Simulation of Urban Mobility (SUMO). [online] http://sumo.sourceforge.net.

[11] Agarwal, A. (2010). *Analytical modeling of delay-tolerant data dissemination in vehicular networks*. Boston.

[12] Akhtar, N. and Missen, M. M. S. (2015). Contribution to the formal specification and verification of a multi-agent robotic system. *arXiv preprint arXiv*, page 1604.05577.

[13] Alam, M., Ferreira, J., and Fonseca, J. (2016). *Intelligent Transportation Systems. Dependable Vehicular Communications for Improved Road Safety*, pages 1474–1. Springer.

[14] Ali, K. M. (2017). *An intelligent intrusion detection system for external communications in autonomous vehicles*. PhD thesis, University of Essex.

[15] Alkhalifa, I. and Almogren, A. (2020). Nssc: Novel segment based safety message broadcasting in cluster-based vehicular sensor network. *IEEE Access*, 8:34299–34312.

[16] Atallah, R. (2017). *The next generation intelligent transportation system: connected, safe and green*. PhD thesis, Concordia University.

[17] Azzaoui, N., Korichi, A., B.Brik, and Fekair, M. (2021). Towards optimal dissemination of emergency messages in internet of vehicles: A dynamic clustering-based approach. *Electronics*, 10(8):979.

[18] Bagheri, M., Sirjani, M., Khamespanah, E., Khakpour, N., Akkaya, I., Movaghar, A., and Lee, E. A. (2018). Coordinated actor model of self-adaptive track-based traffic control systems. *Journal of Systems and Software*, 143:116–139.

[19] Bakioglu, G. and Atahan, A. O. (2020). Evaluating the influencing factors on adoption of self-driving vehicles by using interval-valued pythagorean fuzzy AHP. In *Proceedings of the International Conference on Intelligent and Fuzzy Systems*, pages 503–511.

[20] Banani, M. (2018). *Receiver-based prioritization scheme for safety messages in high density vehicular ad hoc Networks*. PhD thesis, Thammasat University.

[21] Banani, S., Gordon, S., Thiemjarus, S., and Kittipiyakul, S. (2018). Verifying safety messages using relative-time and zone priority in vehicular ad hoc networks. *Sensors*, 18(4):1195.

[22] Bernardeschi, C., Fantechi, A., Gnesi, S., Larosa, S., Mongardi, G., and Romano, D. (1998). A formal verification environment for railway signaling system design. *Formal Methods in System Design*, 12(2):139–161.

[23] Biswas, S. and Mišić, J. (2013). A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs. *IEEE Transactions on Vehicular Technology*, 62(5):2182–2192.

[24] Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426.

[25] Bouchelaghem, S. (2019). *Security and privacy in smart cities*. PhD thesis, University of Bejaia.

[26] Brooks, T. T. (2013). ICITST-2013: Keynote speaker 3: Blurred nets: Disruption and the risk to future Internet of Things (IoT) architectures. In *Proceedings of the* 8^{th} *International Conference for Internet Technology and Secured Transactions*, pages 15–15.

[27] Brzozowski, J. A. (1964). Derivatives of regular expressions. *Journal of the ACM*, 11(4):481–494.

[28] Cai, G., Zhao, J., Song, Q., and Zhou, M. (2019). System architecture of a train sensor network for automatic train safety monitoring. *Computers & Industrial Engineering*, 127:1183–1192.

[29] Carneiro, G. (2018). NS-3: Network simulator 3. In *UTM Lab Meeting*, volume 20, pages 4–5.

[30] Chakraborty, S., Das, P., and Pal, S. (2020). IoT foundations and its application. In *IoT and Analytics for Agriculture*, pages 51–68.

[31] Chen, C., Lee, S. W., Watson, T., Maple, C., and Lu, Y. (2017). Caesar: A criticality-aware ecdsa signature verification scheme with markov model. In *Proceedings of the* 2017 *IEEE Vehicular Networking Conference*, pages 151–154.

[32] Chen, T., Wang, H., Ning, B., Zhang, Y., Tang, T., and Li, K. (2018). Architecture design of a novel train-centric CBTC system. In *Proceedings of the International Conference on Intelligent Rail Transportation*, page 1–5.

[33] Cheng, H. and Ma, Z. (2016). A literature overview of knowledge sharing between petri nets and ontologies. *The Knowledge Engineering Review*, 31(3):239–260.

[34] Cheng, R., Yu, W., Song, Y., Chen, D., Ma, X., and Cheng, Y. (2019). Intelligent safe driving methods based on hybrid automata and ensemble CART algorithms for multihigh-speed trains. *IEEE Transactions on Cybernetics*, 49(10):3816–3826.

[35] Cimatti, A., Roveri, M., Susi, A., and Tonetta, S. (2010). Formalization and validation of safety-critical requirements. *arXiv preprint arXiv*, page 1003.1741.

[36] Colombo, A. W., Karnouskos, S., Kaynak, O., Shi, Y., and Yin, S. (2017). Industrial cyberphysical systems: A backbone of the fourth industrial revolution. *IEEE Industrial Electronics Magazine*, 11(1):6–16.

[37] Corno, F. and Sanaullah, M. (2014). Design-time formal verification for smart environments: an exploratory perspective. *Journal of Ambient Intelligence and Humanized Computing*, 5(4):581–599.

[38] Dasgupta, A. and Wahed, A. (2014). Laboratory statistics and quality control. *Clinical chemistry, immunology and laboratory quality control*, 11(4):47–66.

[39] Dharmapurikar, S., Song, H., Turner, J., and Lockwood, J. (2006). Fast packet classification using bloom filters. In *Proceedings of the* 2006 *Symposium on Architecture For Networking And Communications Systems*, pages 61–70.

[40] Engoulou, R. G., Bellaïche, M., Pierre, S., and Quintero, A. (2014). VANET security surveys. *Computer Communications*, 44:1–13.

[41] Eziama, E., Awin, F., Ahmed, S., Santos-Jaimes, L. M., Pelumi, A., and Corral-De-Witt, D. (2020). Detection and identification of malicious cyber-attacks in connected and automated vehicles' real-time sensors. *Applied Sciences*, 10(21):7833.

[42] Feng, D., Yajie, M., Fengxing, Z., Xiaomao, W., and Kai, H. (2018). A safety message broadcast strategy in hybrid vehicular network environment. *The Computer Journal*, 61(6):789–797.

[43] Ferng, H. W., Chen, J. Y., Lotfolahi, M., Tseng, Y. T., and Zhang, S. Y. (2019). Messages classification and dynamic batch verification scheme for VANETs. *IEEE Transactions on Mobile Computing*, 20(3):1156–1172.

[44] Fujita, H. and Zualkernan, I. (2008). Enforcing security policies using algebraic approach. In *Proceedings of the* 7^{th} *Software Methodologies, Tools, and Techniques*, volume 182, pages 84–98.

[45] Gao, Y., Chong, P. H. J., and Guan, Y. L. (2017). BSM dissemination with network coded relaying in VANETs at NLOS intersections. In *Proceedings of the* 2017 *IEEE International Conference on Communications*, pages 1–6.

[46] Godefroid, P., Peled, D., and Staskauskas, M. (1996). Using partial-order methods in the formal validation of industrial concurrent programs. *IEEE Transactions on software engineering*, 22(7):496–507.

[47] Gravina, R., Palau, C. E., Manso, M., Liotta, A., and Fortino, G. (2018). *Integration, interconnection, and interoperability of IoT systems*. Springer, New York.

[48] Guerrero-Ibáñez, A., Flores-Cortés, C., Damián-Reyes, P., and Pulido, J. R. G. (2012). Emerging technologies in transportation systems: Challenges and opportunities. *International Journal of Wireless Networks and Broadband Technologies*, 2(4):12–40.

[49] Hahn, D., Munir, A., and Behzadan, V. (2019). Security and privacy issues in intelligent transportation systems: Classification and challenges. *IEEE Intelligent Transportation Systems Magazine*, 13(1):181–196.

[50] Hamida, E. B., Javed, M. A., and Znaidi, W. (2017). Adaptive security provisioning for vehicular safety applications. *International Journal of Space-Based and Situated Computing*, 7(1):16–31.

[51] Hernandez-Jayo, U. and la Iglesia, I. D. (2013). Reliability of cooperative vehicular applications on real scenarios over an IEEE 802.11 p communications architecture. In *Proceedings of the International Conference on E-Business and Telecommunications*, pages 387–401.

[52] Hoare, C. A. R. (1978). Communicating sequential processes. *Communications of the ACM*, 21(8):666–677.

[53] Hrizi, F. (2012). *Control mechanisms for intelligent transportation systems (ITS) cooperative safety applications*. PhD thesis, TELECOM ParisTech.

[54] Huang, Y. S., Weng, Y. S., and Zhou, M. C. (2010). Critical scenarios and their identification in parallel railroad level crossing traffic control systems. *IEEE Transactions on Intelligent Transportation Systems*, 11(4):968–977.

[55] Ibraheem, M. S., Hachicha, K., Ahmed, S. Z., Lambert, L., and Garda, P. (2019). High-throughput parallel DWT hardware architecture implemented on an FPGA-based platform. *Journal of real-time image processing*, 16(6):2043–2057.

[56] Ingibergsson, J. T. M., Kraft, D., and Schultz, U. (2017). Declarative rule-based safety for robotic perception systems. *Journal of Software Engineering for Robotics*, 8(1):17–31.

[57] Islam, S. R., Uddin, M. N., and Kwak, K. S. (2016). The IoT: Exciting possibilities for bettering lives: Special application scenarios. *IEEE Consumer Electronics Magazine*, 5(2):49–57.

[58] Jafarzadeh, H. and Fleming, C. (2021). Gaussian process-based model predictive controller for connected vehicles with uncertain wireless channel. In *Proceedings of the* 2021 *IEEE International Intelligent Transportation Systems Conference*, pages 3515–3520.

[59] Jha, S., Yavvari, C., and Wijesekera, D. (2018). Pseudonym certificate validations under heavy vehicular traffic loads. In *Proceedings of the* 2018 *IEEE Vehicular Networking Conference (VNC)*, pages 1–7.

[60] Jraisat, L. (2020). Information sharing in sustainable value chain network (SVCN)—the perspective of transportation in cities. *In Digital Twin Technologies and Smart Cities*, pages 67–77.

[61] Kenney, J. (2011). Dedicated short-range communications (DSRC) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182.

[62] Khan, Z. S., Alaraj, A., Rekha, S. N., Azam, F., and Zubair, M. (2017). Weighted priority based signatures' batch verification scheme in vehicular ad-hoc networks. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, volume 2.

[63] Kleinberg, S. and Mishra, B. (2012). The temporal logic of causal structures. *arXiv preprint arXiv*, page 1205.2634.

[64] Lee, C. H., Lim, K. G., Tan, M. K., Chin, R. K. Y., and Teo, K. T. K. (2017). A genetic algorithm for management of coding resources in VANET. In *Proceedings of the* 2017 *IEEE* 2^{nd} *International Conference on Automatic Control and Intelligent Systems*, pages 80–85.

[65] León-Coca, J. M., Reina, D. G., Toral, S. L., Barrero, F., and Bessis, N. (2014). *Intelligent transportation systems and wireless access in vehicular environment technology for developing smart cities*, pages 285–313. Springer.

[66] Li, D., Zhao, Y., Ranjitkar, P., Zhao, H., and Bai, Q. (2018). Hybrid approach for variable speed limit implementation and application to mixed traffic conditions with connected autonomous vehicles. *IET Intelligent Transport Systems*, 12(5):327–334.

[67] Li, Q., Malip, A., Martin, K. M., Ng, S. L., and Zhang, J. (2012). A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology*, 61(9):4095–4108.

[68] Liu, B., Ghazel, M., and Toguyéni, A. (2014). Toward an efficient approach for diagnosability analysis of des modeled by labeled petri nets. In *Proceedings of the* 2014 *European Control Conference (ECC)*, pages 1293–1298.

[69] Liu, B., Ghazel, M., and Toguyéni, A. (2015a). Model-based diagnosis of multi-track level crossing plants. *IEEE Transactions on Intelligent Transportation Systems*, 17(2):546–556.

[70] Liu, J., Yang, W., Zhang, J., and Yang, C. (2020). Detecting false messages in vehicular ad hoc networks based on a traffic flow model. *International Journal of Distributed Sensor Networks*, 16(2):1–12.

[71] Liu, P., Yang, L., Gao, Z., Li, S., and Gao, Y. (2015b). Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Safety Science*, 79:344–357.

[72] Lu, W., Yi, Z., Liu, W., Gu, Y., Rui, Y., and Ran, B. (2021). Efficient deep learning based method for multi-lane speed forecasting: a case study in Beijing. *IET Intelligent Transport Systems*, 14(14):2073–2082.

[73] Ma, X., Zhang, J., Yin, X., and Trivedi, K. (2011). Design and analysis of a robust broadcast scheme for VANET safety-related services. *IEEE Transactions on Vehicular Technology*, 61(1):46–61.

[74] Marrella, A., Mecella, M., Halapuu, P., and Sardina, S. (2015). Automated process adaptation in cyber-physical domains with the smartpm system (short paper). In *Proceedings of the* 2015 *IEEE* 8^{th} *International Conference on Service-Oriented Computing and Applications*, pages 59–64.

[75] Milner, R., Parrow, J., and Walker, D. (1992). A calculus of mobile processes. *Information and computation*, 100(1):1–40.

[76] Mouton, F., Nottingham, A., Leenen, L., and Venter, H. S. (2018). Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Africa Research Journal*, 109(2):133–148.

[77] Mughal, B. M. (2012). *Performance evaluation of single-hop periodic safety beaconing for vehicle-to-vehicle communication in VANET*. PhD thesis, Teknologi Petronas University.

[78] Munir, A. (2017). Safety assessment and design of dependable cybercars: For today and the future. *IEEE Consumer Electronics Magazine*, 6(2):69–77.

[79] Najafzadeh, S., Ithnin, N., Razak, S. A., and Karimi, R. (2014). BSM: broadcasting of safety messages in vehicular ad hoc networks. *Arabian Journal for Science and Engineering*, 39(2):777–782.

[80] Naufal, J. K., Camargo, J. B., Vismari, L. F., de Almeida, J. R., Molina, C., González, R. I. R., Inam, R., and Fersman, E. (2017). A^2CPS: A vehicle-centric safety conceptual framework for autonomous transport systems. *IEEE Transactions on Intelligent Transportation Systems*, 19(6):1925–1939.

[81] Nguyen-Minh, H. (2016). *Contribution to the intelligent transportation system: security of safety applications in vehicle ad hoc networks*. PhD thesis, Avignon.

[82] Nilsson, J., Fredriksson, J., and Coelingh, E. (2017). Trajectory planning with miscellaneous safety critical zones. *IFAC-PapersOnLine*, 50(1):9083–9088.

[83] Paranjothi, A., Tanik, U., Wang, Y., and Khan, M. S. (2019). Hybrid-vehfog: a robust approach for reliable dissemination of critical messages in connected vehicles. *Transactions on Emerging Telecommunications Technologies*, 30(6):e3595.

[84] Parkinson, S., Ward, P., Wilson, K., and Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, 18(11):2898–2915.

[85] Pascoe, R. D. and Eichorn, T. N. (2009). What is communication-based train control? *IEEE Vehicular Technology Magazine*, 4(4):16–21.

[86] Petit, S. (2016). World Vehicle Population Rose 4.6 % in 2016. Wards Auto, https://wardsintelligence.informa.com/wi058630/world-vehicle-population-rose-46-in-2016.

[87] Pochet, J. (2018). *Performance evaluation of a suburban railway line partially equipped with a CBTC automation*. PhD thesis, Paris Saclay University, France.

[88] Rajkumar, M. N., Nithya, M., and Krithika, M. (2016). Security requirements and mechanisms in vehicular ad-hoc networks (VANET). *World Scientific News*, 41:214.

[89] Raya, M. and Hubaux, J. P. (2005). The security of vehicular ad hoc networks. In *Proceedings of the* 3^{rd} *ACM workshop on security of ad hoc and sensor networks*, pages 11–21.

[90] Rumsey, A. F., Achakji, G., Bois, S., Braban, C., Childs, F., Crispo, M., ..., and Graponne, V. (2004). *IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements*, pages 1474–1. IEEE.

[91] Sakiz, F. and Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks*, 61:33–50.

[92] Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., and Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on automatic control*, 40(9):1555–1575.

[93] Shladover, S. E. (2018). Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems*, 22(3):190–200.

[94] So, S., Petit, J., and Starobinski, D. (2019). Physical layer plausibility checks for misbehavior detection in V2X networks. In *Proceedings of the* 12^{th} *Conference on Security and Privacy in Wireless and Mobile Networks*, pages 84–93.

[95] Sohail, M., Ali, R., Kashif, M., Ali, S., Mehta, S., Zikria, Y. B., and Yu, H. (2020). Trustwalker: an efficient trust assessment in vehicular internet of things (VIoT) with security consideration. *Sensors*, 20(14):3945.

[96] Song, H., Liu, H., and Schnieder, E. (2018). A train-centric communication-based new movement authority proposal for ETCS-2. *IEEE Transactions on Intelligent Transportation Systems*, 20(6):2328–2338.

[97] Stanciu, E. A., Moise, I. M., and Nemtoi, L. M. (2012). Optimization of urban road traffic in intelligent transport systems. In *Proceedings of the* 2012 *IEEE International Conference on Applied and Theoretical Electricity*, pages 1–4.

[98] Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., and Laarouchi, Y. (2013). Survey on security threats and protection mechanisms in embedded automotive networks. In *Proceedings of the* 2013 43^{rd} *Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop*, pages 1–12.

[99] Toor, Y., Muhlethaler, P., Laouiti, A., and Fortelle, A. D. L. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE communications surveys tutorials*, 10(3):74–88.

[100] Uzcátegui, R. A., Sucre, A. J. D., and Acosta-Marum, G. (2009). WAVE: A tutorial. *IEEE Communications magazine*, 47(5):126–133.

[101] Vehicle Safety Communications Consortium (2005). Vehicle Safety Communications Project, Task-3 Final Report, Identify Intelligent Vehicle Safety Applications Enabled by DSRC, Technical Report No. DOT HS 809 859.

[102] Voelcker, J. (2014). 1.2 Billion Vehicles on World's Roads Now, 2 Billion by 2035. Report. Green Car Reports, https://www.greencarreports.com/news/1093560_1-2-billion-vehicles-on-worlds-roads-now-2-billion-by-2035-report.

[103] Wagh, M. B. and Gomathi, N. (2019). Optimal route selection for vehicular ad hoc networks using lion algorithm. *Journal of Engineering Research*, 7(3):178–199.

[104] Wang, H., Yu, F. R., Zhu, L., Tang, T., and Ning, B. (2015). A cognitive control approach to communication-based train control systems. *IEEE Transactions on Intelligent Transportation Systems*, 16(4):1676–1689.

[105] Wang, H., Zhao, N., Ning, B., Tang, T., and Chai, M. (2018). Safety monitor for train-centric CBTC system. *Institution of Engineering and Technology Intelligent Transport Systems*, 12(8):931–938.

[106] Wang, J., Wang, J., Roberts, C., and Chen, L. (2014a). Parallel monitoring for the next generation of train control systems. *IEEE Transactions on Intelligent Transportation Systems*, 16(1):330–338.

[107] Wang, J., Wang, J., Roberts, C., Chen, L., and Zhang, Y. (2017). A novel train control approach to avoid rear-end collision based on geese migration principle. *Safety Science*, 91:373–380.

[108] Wang, T., Shen, L., and Ma, C. (2014b). A process algebra-based detection model for multithreaded programs in communication system. *Transactions on Internet and Information Systems*, 8(3):235–274.

[109] Wang, X., Liu, L., Zhu, L., and Tang, T. (2019). Train-centric CBTC meets age of information in train-to-train communications. *IEEE Transactions on Intelligent Transportation Systems*, 21(10):4072–4085.

[110] Wang, Y., Chen, L., Wei, J., Kirkwood, D., Xu, Q., Lv, J., and Roberts, C. (2016). On-line conformance testing of the communication-based train control (CBTC) system. In *Proceedings of the* 2016 *IEEE International Conference on Intelligent Rail Transportation*, pages 328–333.

[111] Wei, Z., Tang, H., Yu, F. R., Wang, M., and Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology*, 63(9):4647–4658.

[112] Wyk, F. V., Wang, Y., Khojandi, A., and Masoud, N. (2019). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 21(3):1264–1276.

[113] Yoo, T. and Lafortune, S. (2002). Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on automatic control*, 47(9):1491–1495.

[114] Zaidi, K., Milojevic, M. B., Rakocevic, V., Nallanathan, A., and Rajarajan, M. (2015). Host-based intrusion detection for VANETs: A statistical approach to rogue node detection. *IEEE transactions on vehicular technology*, 65(8):6703–6714.

[115] Zamouche, D., Mohammedi, M., Aissani, S., and Omar, M. (2021a). Ultra-safe and reliable enhanced train-centric communication-based train control system. *Computing (Springer Publisher)*.

[116] Zamouche, D., Omar, M., Mohammedi, M., and Aissani, S. (2021b). Highly efficient approach for discordant BSMs detection in connected vehicles environment. *submitted to Journal of wireless network (Springer Publisher)*.

[117] Zeng, W., Khalid, M. A., and Chowdhury, S. (2016). In-vehicle networks outlook: Achievements and challenges. *IEEE Communications Surveys Tutorials*, 18(3):1552–1571.

[118] Zhang, M., Ali, G. M. N., Chong, P. H. J., Seet, B. C., and Kumar, A. (2019a). A novel hybrid MAC protocol for basic safety message broadcasting in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(10):4269–4282.

[119] Zhang, Y., Wang, H., Yuan, T., Lv, J., and Xu, T. (2019b). Hybrid online safety observer for CTCS-3 train control system on-board equipment. *IEEE Transactions on Intelligent Transportation Systems*, 20(3):925–933.

Abstract

Over the last decades, advancements in computing, electronics, and mechanical systems have been resulting in the development of transportation all over the world, which has been providing a lot of benefits for many aspects of human life. Intelligent Transportation Systems (ITSs) are advanced applications that aim to make the transportation infrastructures safer, more convenient, and smarter by using information that is shared among vehicles such as crash warning, sudden-brake warning, lane change warning, and so on. Thus, such systems provide a wide variety of services including, but not limited to, traffic control, traffic management, passenger and road safety, and remote region connectivity. However, several challenges hampering the proper operation of these systems, such as extreme disturbances and they rely on several kinds of devices that can cause malfunctions. Moreover, vehicular communications are expected to be subject to severe breaches that affect the reliability of the exchanged information. Seeking to improve the safety and protect human life, in this thesis, we address these problems by providing improvements to the existing STIs. In particular, we have proposed an *enhanced train-centric communication-based train control system* for railway transportation that allows improving the quality and enhancing reliability of the train control. Moreover, we have proposed our second contribution that manifests itself in the proposition of a *discordant safety messages detection strategy in connected vehicles environment* that provides the vehicles with the ability to quickly and preemptively identify discordant messages and hence dealing against potential disturbances, while ensuring a trade-off between the efficiency and safety. The proposed mechanisms are evaluated through simulations in terms of important metrics. The obtained results highlight the promising performances of our proposals.

Keywords: Intelligent Transportation Systems, Vehicular Networks, Security, Safety, Process Algebra, Anomaly Detection.

Résumé

Au cours des dernières décennies, les progrès de l'informatique, de l'électronique et des systèmes mécaniques ont entraîné le développement de transport dans le monde entier, ce qui a apporté de nombreux avantages à de nombreux aspects de la vie humaine. Les Systèmes de Transport Intelligents (STIs) sont des applications avancées qui visent à rendre les infrastructures de transport plus sûres, pratiques et intelligentes en utilisant des informations partagées entre les véhicules, telles que l'avertissement de collision, l'avertissement de freinage soudain, l'avertissement de changement de voie, etc. Ainsi, ces systèmes fournissent une grande variété de services, y compris, mais sans s'y limiter, le contrôle et la gestion du trafic, la sûreté des passagers et des routes, et la connectivité des régions éloignées. Pour autant, plusieurs défis entravent le bon fonctionnement de ces systèmes, tels que des perturbations extrêmes et ils reposent sur plusieurs sortes de dispositifs qui peuvent provoquer des dysfonctionnements. De plus, les communications véhiculaires sont susceptibles de faire l'objet de violations graves qui affectent la fiabilité des informations échangées. Cherchant à améliorer la sûreté et à protéger la vie humaine, dans cette thèse, nous adressons ces problèmes en apportant des améliorations aux STIs existants. En particulier, nous avons proposé un *système amélioré de contrôle des trains basé sur les communications et centré sur les trains* pour le transport ferroviaire qui permet d'améliorer la qualité et la fiabilité du contrôle des trains. De plus, nous avons proposé notre deuxième contribution qui se manifeste par la proposition d'une *stratégie de détection de messages de sûreté discordants dans un environnement de véhicules connectés* qui fournit aux véhicules la capacité d'identifier rapidement et de manière préventive les messages discordants et donc de faire face contre les perturbations potentielles, tout en assurant un compromis entre l'efficacité et la sûreté. Les mécanismes proposés sont évalués par des simulations en termes de métriques importantes. Les résultats obtenus mettent en évidence les performances prometteuses de nos propositions.

Mots clés : Systèmes de Transport Intelligent, Réseaux Véhiculaires, Sécurité, Sûreté, Algèbre de processus, Détection d'Anomalies.

ملخص

على مدى العقود الماضية، أدت التطورات في الحوسبة، الإلكترونيات، والأنظمة الميكانيكية إلى تطوير وسائل النقل في جميع أنحاء العالم، الذي قدم الكثير من الفوائد للعديد من جوانب الحياة البشرية. أنظمة النقل الذكية عبارة عن تطبيقات متقدمة تهدف إلى جعل النقل أكثر أمانًا، أكثر ملاءمةً، وأكثر ذكاءً من خلال استخدام المعلومات التي يتم مشاركتها بين المركبات مثل التحذير من الاصطدام، التحذير من الفرامل المفاجئة، التحذير من تغيير المسار، وما إلى ذلك. وبالتالي، توفر هذه الأنظمة مجموعة من الخدمات المتنوعة بما في ذلك، على سبيل المثال لا للحصر، مراقبة حركة المرور وإدارتها، سلامة الركاب والطرق، والاتصال بالمناطق البعيدة. ومع ذلك، هناك العديد من التحديات التي تعيق التشغيل السليم لهذه الأنظمة، مثل الاضطرابات الشديدة وكونها تعتمد على عدة أنواع من الأجهزة التي يمكن أن تسبب اختلالات وظيفية. علاوة على ذلك، من المحتمل أن تكون اتصالات المركبات موضوع لانتهاكات خطيرة تؤثر على موثوقية المعلومات المتبادلة. سعياً لتحسين السلامة وحماية حياة الإنسان، في هذه الأطروحة، نعالج هذه المشاكل من خلال توفير تحسينات على هذه الأنظمة. على وجه الخصوص، لقد اقترحنا *نظامًا محسنًا للتحكم في القطارات قائم على الاتصالات ومرتكز على القطار* للنقل بالسكك الحديدية يسمح بتحسين جودة التحكم في القطار وتعزيز موثوقيته. علاوة على ذلك، فقد اقترحنا مساهمتنا الثانية التي تتجلى في اقتراح *إستراتيجية الكشف عن رسائل السلامة المتعارضة في بيئة المركبات المتصلة* التي توفر للمركبات القدرة على تحديد الرسائل المتعارضة بسرعة واستباقية وبالتالي التعامل مع الاضطرابات المحتملة، مع ضمان المفاضلة بين الكفاءة والسلامة. تم تقييم الآليات المقترحة من خلال عمليات المحاكاة من حيث مقاييس هامة. النتائج التي تم الحصول عليها تسلط الضوء على الأداء الواعد لمقترحاتنا .

الكلمات الرئيسية: أنظمة النقل الذكية، شبكات المركبات، الأمن، السلامة، عملية الجبر، كشف الشذوذ.