



Thèse de doctorat

Pour obtenir le grade de
Docteur de l'Université
POLYTECHNIQUE HAUTS-de-FRANCE

Discipline: **Informatique**

Présentée et soutenue par: Fatma SALEM

Le 06/09/2018, à Valenciennes

Ecole doctorale :
Sciences Pour l'Ingénieur (SPI)
Equipe de recherche, Laboratoire :
Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines (LAMIH)

Fiabilité et Sécurité des Systèmes Embarqués Communicants pour les Transports: Modélisation et Optimisation

---

Président de jury

- Fouzia Boukour, Chargée de Recherche HDR, IFSTTAR, France

Rapporteurs

- Ahmed Eltawil. Professor, University of California, Irvine, USA
- Vahid Meghdadi. Professeur, Université de Limoges, France

Examinateurs

- Noureddine Idboufker, Professeur, Ecole Nationale des Sciences Appliquées de Marrakech (ENSA), Maroc

Directeurs de thèse

- Smail Niar, Professeur, LAMIH UMR UPHF/CNRS 8201, France

Co-encadrant de thèse

- Yassin El-Hillali, Maître de Conférences, IEMN UPHF, France

I dedicate this thesis to

My parents, who gave me an appreciation of learning and taught me the value of perseverance and resolve.

My husband, for his unfaltering support and understanding while I was completing this research.

My children, who have made me stronger, better and more fulfilled than I could have ever imagined.

Acknowledgments

I would like to express my deep gratitude to my supervisors, Prof. Smail Niar and Dr. Yassin El-Hillali for their contributions, support, and kindness during the course of my Ph.D. research. I also wish to thank all the members of my committee for their valuable participation and insights.

I would like to thank the Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines (LAMIH) and the Laboratoire de l'Institut d'Electronique de Microélectronique et de Nanotechnologie (IEMN) at the Polytechnic University Hauts-de-France for their support.

Many thanks also to my colleagues in LAMIH for their help, support and friendship all over the years.

Finally, my thanks go to the Ministry of Higher Education and Scientific Research in Libya for sponsoring my Ph.D.

Résumé

Véhicule-à-tous (V2X) se référe à un Système de Transport Intelligent (ITS) où les véhicules et l'infrastructure sont interconnectès. Cette connectivitè permet une connaissance prècise des conditions de circulation sur l'ensemble du rèseau routier, ce qui contribue à amèliorer la sècuritè routière, rèduire les temps d'encombrement et èviter les pertes èconomiques. Cette communication permet aussi une variètè de nouvelles applications pour la sècuritè routière et l'infodivertissement. Bien que la communauté de scientifique ait réalisé de grands progrès dans l'ètude sur le V2X, il reste encore des défis à surmonter et des problèmes clès qui doivent être étudiés plus en profondeur. Cette thèse considère deux des questions les plus importantes; fiabilité et sécurité des communications V2X. Du point de vue de la fiabilité, nous proposons d'abord une méthode basée sur la modèlisation de l'utilisateur pour èvaluer la capacité de la norme DSRC IEEE 802.11p à rèpondre aux exigences de Qualité De Service (QoS) de la diffusion des messages de sécurité. La nouveauté de la méthode réside dans son application qui élimine le probléme de la définition d'un modèle Markovien par la détermination des moments d'équilibre du processus de retard. Cette methode fournit des informations importantes sur les paramétres de conception IEEE 802.11p et sur ses fonctionnalités, ce qui permet d'améliorer la configuration proposée. De plus, nous proposons un modèle Régénératif pour reśoudre le problème de la caractérisation des processus de trafic interconnecté dans les réseaux V2X hybrides à grande échelle. Ce dernier est une préoccupation majeure pour parvenir à une opérabilité efficace et adéquate pour les réseaux de véhicules à grande échelle. Du point de vue de la sécurité, nous introduisons une nouvelle méthodologie d'optimisation. Notre méthodologie lie les exigences de QoS des différentes classes d'application avec le paramètre de conception de base du mécanisme de résolution de contention dans le protocole MAC IEEE 802.11p. En outre, un nouvel algorithme de détection d'attaque de brouillage dans l'environnement véhiculaire est proposé. L'algorithme utilise la méthodologie d'optimisation développée pour définir un seuil de détection et intégre la méthode séquentielle de détection pour détecter les attaques de brouillage à chaque fois que la valeur seuil est franchie. Des expérimentations analytiques et de simulation approfondies ont été effectuées pour chaque contribution afin de montrer la validité des méthodes/modèles proposés et de prouver leur efficacité.

Mots clés : Réseaux de Véhicules - V2X - Fiabilité- Sécurité - Optimisation - IEEE 802.11p - Modélisation - VANET

Abstract

Vehicle-to-anything (V2X) refers to an Intelligent Transportation System (ITS) where the vehicles and infrastructure systems are all interconnected with each other. This connectivity provides precise knowledge of the traffic situations across the entire road network which in turn helps to enhance traffic safety, reduce congestion time, avoid economic losses, in addition to enable a variety of novel ITS applications for road safety and passenger infotainment. V2X communications is based on two technologies; Dedicated Short-Range Communications (DSRC) which is an essential technology for realizing V2X and cellular networks which provide an off-the-shelf potential solution for V2X communications. Although the research community has achieved much great progress on V2X study, there are still some challenges that need to be overcome and some key issues that need to be further investigated. This thesis considers two of the most prominent issues; reliability and security of V2X communications. From the reliability perspective, we first propose User Model-based Method to evaluate the capacity of IEEE 802.11p-based DSRC standard to meet the Quality-of-Service (QoS) requirements of safety messages dissemination. The novelty of the method lies in its application which avoids the problem of defining a Markovian model by determining the steady state moments of the induced delay process. This applicability feature provides important insights about IEEE 802.11p design parameters and its functionality leading to proposed reconfigurations for enhanced performance. Moreover, we propose Regenerative model, that we believe to be the first to address the problem of interconnected-traffic process characterization in large-scale hybrid V2X networks. The latter is a primary concern in achieving efficient and adequate operability for large-scale vehicular networks. From the security perspective, we introduce a new optimization methodology which ties the QoS requirements of different application classes with the basic design parameters of the contention resolution mechanism in IEEE 802.11p MAC protocol. In addition, a novel detection algorithm for jamming attacks in the vehicular environment is proposed. The algorithm utilizes the developed optimization methodology to define a detection threshold. By integrating the sequential detection of change method it traces and detects jamming attacks whenever the threshold value is crossed. Analytical and simulation experimentations have been performed for each contribution to show the validity of the proposed methods/models and to prove their efficiency.

Keywords: Vehicular Networks - V2X - Reliability - Security - Optimization - IEEE 802.11p - Modeling - VANET

Contents

Contents i

List of Figures vi

List of Tables viii

List of algorithms ix

List of Symbols x

List of Acronyms xiii

1 Introduction 1

1.1 General Context 1

1.2 Motivations 5

1.2.1 Meeting the QoS of Real-time Applications 6

1.2.2 Operability Challenge in Large-scale Deployment . . . 7

1.2.3 Vulnerability of IEEE 802.11p to DoS Attacks 8

1.3 Contributions of the Thesis 9

1.3.1 Proposition of User Model-based Method for IEEE 802.11p MAC Performance Evaluation 10

1.3.2 Efficient Modeling of IEEE 802.11p Output Process for V2X Interworking Enhancement 10
1.3.3 Optimization Methodology for DSRC Enhancement 11
1.3.4 QoS-based Sequential Detection Algorithm for Jamming Attacks in VANET 12
1.4 Structure of the Thesis 13

2 User Model-Based Method for IEEE 802.11p-based DSRC Performance Evaluation 14

2.1 Introduction 14
2.2 An Overview of Multiple Access and Related Works 17
2.2.1 Multiple Access Problem 17
2.2.2 Related Works 18
2.3 IEEE 802.11p for Vehicular Communications 20
2.3.1 DSRC Spectrum Allocation 20
2.3.2 The Contention Resolution Algorithmic System 22
2.4 User Model 23
2.4.1 Finite Population Model 23
2.4.2 Infinite Population Model 25
2.5 Stability Analysis 26
2.5.1 System of Equations Related to the Per-segment Length 28
2.5.2 On the Relation Between the User Model and Stability of IEEE 802.11p 30

2.6 Model Validation and Performance 31
2.7 Conclusions 35

3 Efficient Modeling of IEEE 802.11p Output Process for V2X Large-scale Enhancement 37

3.1 Introduction 37
3.1.1 Motivation 40
3.1.2 Main Contribution 42
3.2 V2X Hybrid Interworking and Related Works 43
3.2.1 V2X Hybrid Architectures 43
3.2.2 Related Works 45
3.3 Regenerative Model 46
3.4 Numerical Evaluation 50
3.4.1 Mean Segment Throughput 50
3.4.2 Mean Cumulative Distance Over a Segment 53
3.4.3 Model Validation 56
3.5 Description of the Output Process 58
3.5.1 The Output Process in Low Traffic Scenario 59
3.5.2 The Output Process in High Traffic Scenario 60
3.5.3 Evaluation of the Description Models 62
3.6 V2X Application Scenario 64
3.7 Conclusions 68

4 QoS-based Sequential Detection Algorithm for Jamming Attacks in VANET 70

4.1 Introduction 70

4.2 Related Works and Contributions 72
4.2.1 Related Works 72
4.2.2 Motivations and Contributions 74
4.3 Jamming Attacks in VANET 76
4.3.1 Vulnerability of IEEE 802.11p MAC to Jamming Attacks 76
4.3.2 Attacker Model 78
4.4 System Model and Problem Formalization 79
4.4.1 Network Architecture 79
4.4.2 Problem Formalization 81
4.5 Optimization Methodology for IEEE 802.11p Configuration 82
4.5.1 Traffic Classes and Quality of Service Criteria 82
4.5.2 EDCA Quality of Service Support 83
4.6 QoS-based Sequential Detection Algorithm (QoS-SDA) 87
4.6.1 QoS-SDA for Memoryless Model 88
4.6.2 Decision Threshold Selection 90
4.7 Simulation Model and Results 92
4.8 Conclusions 95

5 General Conclusions **97**

5.1 Summary of the Thesis 97
5.2 Summary of the Results 100

5.2.1 User Model-based Method for IEEE 802.11p MAC Performance Evaluation 100
5.2.2 V2X Interworking Enhancement 101
5.2.3 Optimization Methodology for IEEE 802.11p Reconfiguration 102
5.2.4 Securing VANET Against Jamming Attacks 103
5.3 Future Work 104

Publications **107**

Appendix A Proof of the Assertion Given in (3.12) **108**

Appendix B Bounds on the Expected Value of CRI Length **111**

Appendix C Proof of Lemma 4 **114**

Appendix D Proof of Lemma 5 **115**

Bibliography **117**

List of Figures

Figure 1.1 V2X communications in an urban scenario 2
Figure 1.2 WAVE protocol architecture 4
Figure 1.3 Progress of main contributions 9

Figure 2.1 DSRC allocated spectrum 21
Figure 2.2 EDCA backoff procedure 22
Figure 2.3 Average delay of Finite and Infinite model for different access classes 32
Figure 2.4 Average delay for messages of different access classes . 33
Figure 2.5 Rejection rate for messages of different access classes . 34
Figure 2.6 Average number of sending attempts for different access classes 34
Figure 2.7 Attempts' distribution for various input rates 35

Figure 3.1 Average packet delay and departure distribution . . . 41
Figure 3.2 DSRC-cellular hybrid architecture 44
Figure 3.3 Interdeparture distribution for different input traffic rates 58
Figure 3.4 Actual, Bernoulli and FOMP at low and high traffic rates 63

Figure 3.5 Bernoulli interdeparture process vs. actual process . . 63
Figure 3.6 System probabilities $P_{\acute{m}m}$ vs. input traffic rate λ . . . 64
Figure 3.7 Mean uplink delay as a function of the output rate, $M = 3$ 66
Figure 3.8 Mean uplink delay as a function of the output rate, $M = 5$ 67
Figure 3.9 The total interworking average packet delay 68

Figure 4.1 CSMA/CA procedure in IEEE 802.11p 78
Figure 4.2 Envisioned network architecture 80
Figure 4.3 Cluster data rate under normal network conditions; no jamming 86
Figure 4.4 Power and false alarm curves for different threshold values 91
Figure 4.5 Time evolution of QoS-based sequential detection algorithm (QoS-SDA) 91
Figure 4.6 The algorithmic performance under different attacker models 93
Figure 4.7 Detection probability (a) and delay (b) as a function of the attack rate 94
Figure 4.8 Rejection rate as a function of CW size and the attack rate 95

List of Tables

Table 2.1	EDCA parameters for CCH	23
Table 2.2	CRI length giving m packets in the first slot . .	29
Table 2.3	Parameters setting for simulation scenario	32
Table 3.1	Expected CRI length and the service rate given m packets in the first slot	51
Table 3.2	Upper bounds on the interdeparture distribution	56
Table 4.1	Traffic stability region	85

List of Algorithms

Algorithm QoS-based Sequential Detection Algorithm (QoS-SDA) 89

List of Symbols

α . . . . . Output rate of 802.11p MAC

AC_i . . . . . Traffic class category

β_i . . . . . Output process of 802.11p MAC

$\boldsymbol{b}$ . . . . . Burstiness coefficient

CH_i . . . . . Channel status process

CW . . . . . Contention window size

D . . . . . Average transmission delay

D_B . . . . . Bernoulli mean packet delay

D_K . . . . . First Order Markov packet delay

d . . . . . Interdeparture distance

$d(\infty)$ . . . . . Steady-state of the interdeparture distance

ε_k . . . . . Upper bound on CRI length

ζ_i^j . . . . . Inter-renewal times of the process $\{S_i, y_i\}$

ζ . . . . . Decision threshold

F . . . . . Mean of the sample function of d

η_m . . . . . Finite mean of the input distribution

L . . . . . Frame length in slot units

L_m . . . . . Mean CRI length given m multiplicity in the 1^{st} slot

$L_{m|n}$ . . . . . Mean CRI length conditioned on having n users with counter value zero

L_s . . . . . Lower bound on successful transmissions

l . . . . . Mean segment length

λ^* . . . . . System throughput

$\lambda^*(CW)$ . . . . . System throughput at defined CW value

λ_{Ci} . . . . . Cluster data rate

λ_l . . . . . Lower bound on cluster data rate

λ_i . . . . . Traffic class input rate

λ_u . . . . . Upper bound on cluster data rate

μ . . . . . Mean of the input divergence distribution

M . . . . . Total number of generated packets in the system

m . . . . . Finite number of generated packets

N_n . . . . . Number of arrivals in the n-th frame

P_0 . . . . . Probability of users with zero counter value

P . . . . . Bernoulli output parameter

P_D . . . . . Detection probability

P_{FA} . . . . . False alarm probability

P_m . . . . . Input probability distribution with m users

$P_{\acute{m}m}$ . . . . . System transition probabilities

$P_i(m_1^n)$ . . . . . n-th dimensional distribution of traffic rate in frames

P_r . . . . . Upper bound on the output probability distribution

P_T . . . . . Probability of success

q . . . . . Probability of unsuccessful transmission

R_i . . . . . Collision resolution point

S . . . . . Fraction of the successful transmissions

S_i . . . . . Number of successful transmissions

S_B . . . . . Average number of Bernoulli packets in uplink

S_K . . . . . Average number of Markov packets in uplink

S_n . . . . . Mean of successful transmissions in 1^{st} CRI partition

S_m . . . . . Mean of CRI successful transmissions given m multiplicity

$S_{m|n}$ . . . . . Mean of CRI successful transmissions conditioned on having n packets in the first partition

σ_m^2 . . . . . Finite variance of the input distribution

T . . . . . Slot Time

τ_j . . . . . j-th segment of counting process S_i

U_d . . . . . Upper bound on the transmission delay

y_i . . . . . Packet transmission delay

Y . . . . . Expected value of the sample function of y_i

List of Acronyms

AC . . . . . Access Class

ACK . . . . . Acknowledgment

AIFS . . . . . Arbitration Inter-Frame Space

Brn . . . . . Bernoulli distribution

BS . . . . . Base Station

BT . . . . . Backoff Timer

CAM . . . . . Cooperative Awareness Massage

CCH . . . . . Control Channel

CDMA . . . . . Code Division Multiple Access

CH . . . . . Cluster Head

CM . . . . . Cluster Member

CSMA . . . . . Carrier Sense Multiple Access

CSMA/CA . . . . . Carrier Sense Multiple Access with Collision Avoidance

CRI . . . . . Contention Resolution Interval

CW . . . . . Contention Window

DCF . . . . . Distributed Coordination Function

DCFA . . . . . Deterministic Conflict Free Access

DEN . . . . . Decentralized Environmental Notification

DoS . . . . . Denial of Service

EDCA . . . . . Enhanced Distributed Channel Access

FDMA . . . . . Frequency Division Multiple Access

FOMP . . . . . First Order Markov Process

i.i.d	Independent and Identically Distributed
ITS	Intelligent Transportation System
I2V	Infrastructure to Vehicle
KPI	Key Performance Indicator
LSRA	Limited Sensing Random Access
MAC	Medium Access Control
OBU	On Board Unit
Pois	Poisson distribution
PHY	Physical layer
QoS	Quality of Service
RMA	Random Multiple Access
RSU	Road Side Unit
SCH	Service Channel
TDMA	Time Division Multiple Access
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to anything
VANET	Vehicular Ad hoc Network
WAVE	Wireless Access in Vehicular Environment
WBSS	Wave-based Basic Service
WSA	Wave Service Advertisement

Chapter 1

Introduction

Working together to make Vehicle-to-anything (V2X) a reality.

1.1 General Context

During the digital age, the motor vehicle has evolved from a simple mechanical apparatus to a smart body of sensors that can measure different attributes, enhancing both vehicle safety and driving experience. However, with the explosive growth in the number of vehicles, urban roads and highways are becoming plagued by traffic congestions and road crashes. As a result, deaths caused by traffic accidents have been increasing rapidly, which impose serious socioeconomic threats. The latest "Global status on road safety" report presented by the World Health Organization (WHO) has listed the annual casualties of motor vehicle crashes with a total of 1.2 million fatalities, which makes road traffic accidents a leading cause of deaths globally[1]. Furthermore, traffic jams have become another troublesome problem, especially in large cities. For instance, highway jams posed 42 hours of travel delay and wasted 19 gallons of fuel for a commuter yearly, adding up to an annual economic loss of $160 billion in U.S alone [2]. In EU, the statistical trends and outlooks for passenger transport demand from 1990 to 2030 show that the transport economic and environmental negative impacts will continue to increase unless drastic new policy and technological measures are taken [3].

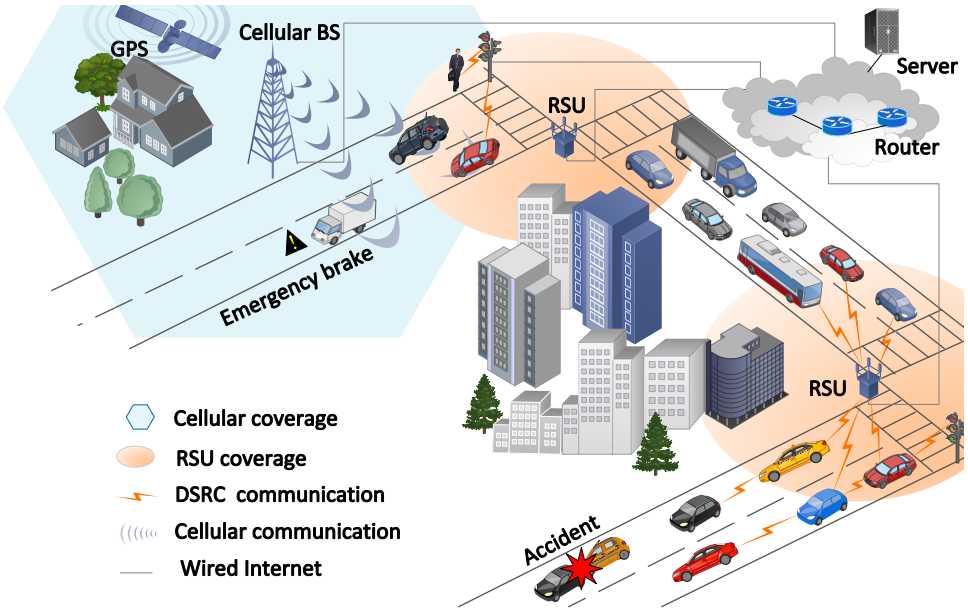


Figure 1.1: V2X communications in an urban scenario

To address these problems, there have been worldwide efforts from governments, academic institutions and industrial organizations under the big umbrella of Intelligent Transport Systems (ITS), to define Vehicle-to-anything (V2X) communications. V2X is a promising communication technology with a great potential of supporting a variety of novel ITS applications to improve traffic safety and efficiency. As defined by the Third Generation Partnership Project (3GPP) group [4]. V2X is aiming to enable Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P) communications, as illustrated in Figure 1.1.

An essential technology for realizing V2X communications is Dedicated Short-Range Communications (DSRC). DSRC is the only wireless technology that can potentially meet the extremely short latency requirement for road safety messaging and control. In fact, the unique feature of low latency secures the role of DSRC, as an essential communication technology in future hybrid multi-radios V2X networks. Although there is no globally agreed-on definition for DSRC, DSRC generally refers to a speed, short range wireless interface between vehicles and road infrastructure. The feasibility of such connectivity is performed through On-Board Units (OBUs) located inside

the vehicle and surface transportation infrastructure like Road-Side Units (RSUs), traffic lights and signs. The DSRC is achieved over reserved radio spectrum bands, which differ in North America, Europe, and Japan. Various DSRC standards are developed by different standardization bodies in these regions including; IEEE 802.11p standard by IEEE in North America [5], the developed ITS-G5 standard by the European Telecommunications Standards Institute (ETSI) in Europe [6], and ARIB STD-T109 by the Association of Radio Industries and Businesses (ARIB) in Japan [7].

In general, standards-based DSRC vehicular communication has been so far implemented to a great extent based on IEEE 802.11p [8, 9]. IEEE 802.11p is more flexible to support multiple device types including the mobile OBUs, the stationary RSUs and other envisioned devices like portable units and hand-held devices carried by pedestrians. This flexibility feature in IEEE 802.11p standard emerges from its inherited IEEE 802.11.x family characteristics, including simplicity and distributed medium access control mechanism. IEEE 802.11p is the current version of IEEE 802.11 standard that incorporates amendment for Wireless Access in Vehicular Environments (WAVE). The WAVE protocol stack is composed of IEEE 802.11p and a standard family IEEE 1609. IEEE 802.11p standardizes the communication aspects related to the Physical (PHY) layer and Medium Access Control (MAC), while IEEE 1609 has been developed to define the upper layers.

The different standards of IEEE 1609 family and their integration with IEEE 802.11p into WAVE architecture are shown in Figure 1.2. The physical layer (PHY) is orthogonal frequency division multiplexing (OFDM) as defined in IEEE 802.11 and works in the 5.9 GHz frequency spectrum band (5.850-5.925 GHz in the U.S., 5.855-5.925 GHz in Europe). The data link layer includes two sublayers Medium Access Control (MAC) and Logical Link Control (LLC) which works as an interface between MAC and the upper layer. In IEEE 802.11p MAC, different Quality of Service (QoS) classes are obtained by prioritizing the data traffic. Therefore, application messages are categorized into different Access Classes ACs, with AC_0 has the lowest and AC_3 the highest priority. Each AC has different contention parameters to contend its messages for one of the shared DSRC channels. This multi-channel operation is extensionally designed for vehicular communication by

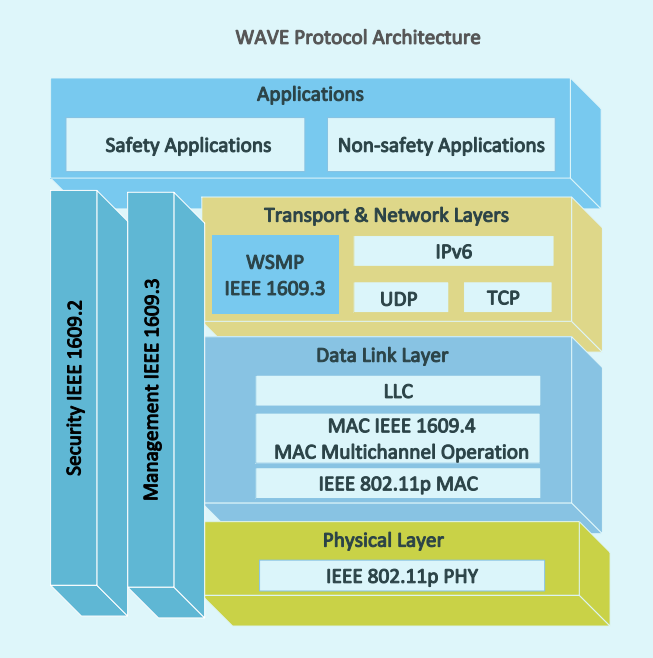


Figure 1.2: WAVE protocol architecture

the standard IEEE 1609.4. The standard IEEE 1609.4 describes how a node switches alternatively among DSRC channels for both safety applications and non-safety applications. Above the LLC sublayer, the protocol stacks separate into two sets of protocols. The standard IEEE 1609.3 defines WAVE Short Message Protocol which designed for optimized operation in vehicular networks. WSMP allows applications to directly control physical characteristics (e.g., channel number, transmitter power). The WAVE Short Messages (WSMs) can be sent in any channel while IP messages are not allowed in control channel. Management services are associated with different data plane entities to provide layer-specific functions that are necessary for the system operation. In particular, the standard IEEE 1609.4 specifies extensions to the standard IEEE 802.11 MAC Layer Management Entity (MLME) and the standard IEEE 1609.3 specifies a WAVE Management Entity (WME). The standard IEEE 1609.2 specifies security services for the WAVE networking stack and for applications running over that stack.

Even though cellular network technologies provide an off-the-shelf potential solution to support V2X communications, dedicated short-range commu-

nications (DSRC) remains an essential technology for realizing V2X communications. The centralized nature of cellular networks limits their ability to support low latency V2X communications, which can jeopardize the effectiveness of safety applications. Moreover, it is unclear whether the cellular network capacity alone can accommodate V2X data traffic along with the increasing data-traffic load from its legacy cellular users, particularly with the expected seven-fold increase in the global mobile data between 2016 and 2021 [10]. Consequently, this motivated our research to look into enhancing the DSRC technology so that it will be able to support reliable and secure V2X communications, either in pure-DSRC V2X networks or in hybrid DSRC-cellular V2X networks. Central to the entire discipline of enhancing the DSRC technology is the concept of the shared communication channel, particular attention must be given to the Medium Access Protocol (MAC), which determines much of the network behavior.

In this thesis, we make contributions to provide enhanced and efficient DSRC communications by proposing a new modeling technique to IEEE 802.11p-based DSRC MAC protocol so that important insights can be gained about IEEE 802.11p configuration and its functionality to support efficient V2X communications. Then we extend our model to be applied in large-scale hybrid V2X networks. In this framework, we provide solutions to the interworking issue in order to overcome the operability challenge and to enable large-scale V2X deployment. We also introduce an optimization methodology to promote the QoS support across all the Access Classes (ACs) in IEEE 802.11p standard. In this context, the methodology is adopted to enhance the security in V2X communications. In particular, the methodology is applied in conjunction with the sequential detection of change method in developing a novel detection algorithm for Denial of Service (DoS) attacks in the vehicular environment.

1.2 Motivations

The current section provides an overview of the motivations for our research and introduces the novel techniques and methodologies used in its contributions as they will be detailed in Section 1.3

1.2.1 Meeting the QoS of Real-time Applications

Communication-based safety technology is considered as a more efficient approach than the traditional active safety technology in terms of detection range, field of view and cost. As a vital part of V2X communications, supporting both V2V and V2I communications, Vehicular Ad Hoc Networks (VANETs) provide many safety-related applications such as cooperative collision warning, intersection collision avoidance, lane departure assistance, emergency electronic brake lights, road conditions (e.g., slippery road, work zone area), etc.,[11–13]. Safety applications can play a significant role in reducing the number of accidents, with reference to the study in [14], V2X communications elevate the collaboration among vehicles, pedestrians, and transport infrastructure, which promises to eliminate 80% of the current road crashes.

A distinguishing feature in safety applications is the limited time of data transmission, therefore traffic safety applications could be classified as real-time systems; once an emergency situation occurs it is necessary to inform all surrounding vehicles with safety messages in time. One of the crucial elements in real-time wireless communication is the MAC protocol, which works on allocating the channel resources fairly and in a predictable way among the network users. In VANTE, a safety-related message needs to be delivered before the deadline, thus it is of a considerable importance to get the MAC of IEEE 802.11p standard to analyze if the standard protocol meets the stringent QoS demands of real-time safety applications.

This thesis proposes a new modeling technique towards investigating the capacity of IEEE 802.11p to support real-time data transmission. The fundamental tradeoffs among the Key Performance Indicators (KPIs) of IEEE 802.11p, namely latency, reliability, and throughput are identified, and the inter-relationships among them is defined in precise mathematical terms.

1.2.2 Operability Challenge in Large-scale Deployment

One of the main challenges inherent to the deployment of large-scale vehicular networks is operability. This issue arises due to DSRC low scalability which originates from its short range nature (up to 1000 m for RSUs) and results in fragmentations in large-scale networks [15, 16]. In addition, the IEEE 802.11p-based DSRC MAC protocol design has a great impact on scalability, in large-scale networks with high traffic density, the increase in collision among the transmitted packets in the shared communication channel results in an increase in the packet rejection rate leading to a degradation in IEEE 802.11p performance [17]. Hence, an inclusion of both DSRC and cellular technologies is a more viable solution for efficient V2X communications in this case. However, the interworking between DSRC and cellular network technologies induces many design challenges, which are not comprehensively addressed by existing approaches, as they only focus on parts of the problem. For example, to resolve the multi-hop problem which is mainly originating from V2X hybrid architecture and consequently to enhance the interconnected system, characterizing the traffic output processes generated by the network nodes is of a fundamental importance. The latter is a major issue in most of today's networking structures and the vehicular environment is not an exception. However, the unique characteristics of vehicular networks add to the complexity of this problem and make any attempt to its solution quite challenging.

The analytical tractability inherent to the memoryless models has tempted many researchers to adopt such models for the description of internetwork traffic processes. Due to their strike characteristics, the adoption of such models in vehicular networks may lead to erroneous identification of the bottlenecks of the interconnected system and to erroneous packet delay calculations which cannot be tolerated, especially for critical real-time safety applications. In V2X interworking, the lack of an accurate description of IEEE 802.11p-based DSRC output process presents the major difficulty in evaluating the interworking performance, this output process is the input process to the other nodes in the interconnected network, i.e., cellular Base

Stations (BSs) and RSUs, and affects considerably its operation.

This thesis makes a major contribution to optimize the traffic flow in the future V2X communications by developing the Regenerative model which provides a complete description for the output process of IEEE 802.11p based-DSRC standard. Unlike the memoryless models, the proposed model captures the deviations of the actual output process of IEEE 802.11p under different traffic intensities. At the same time, this model is simple enough to lead to a tractable analysis of the interconnected system performance. A procedure for the calculation of the parameters of the model has been developed based on the true statistics of the relevant events in IEEE 802.11p actual output process.

1.2.3 Vulnerability of IEEE 802.11p to DoS Attacks

As already mentioned, Vehicular Ad hoc Network (VANET) is a self-organizing network that works on both V2V and V2I communications and presents a key component of the future V2X communications. VANET has a great potential of enabling real-time traffic safety and efficiency applications for people on roads. Therefore, attacking and misusing such network could cause destructive consequences. Drawing upon our previously developed models for IEEE 802.11p based-DSRC standard, we observe the vulnerability of the standard to Denial of Service (DoS) attacks. In particular, our analysis reveals that the distributed contention resolution mechanism in IEEE 802.11p MAC protocol is more susceptible to jamming attacks, one kind of DoS attacks in which the jammer (attacker) can fully or partially prevent legitimate nodes from accessing the network.

Motivated by this observation, this thesis proposes a novel detection algorithm for jamming attacks which is specifically tailored for the vehicular environment; taking into account the QoS requirements imposed by different applications, the change in traffic intensity and the medium access contention mechanism. First, we develop an optimization methodology for IEEE 802.11p MAC which ties QoS requirements of the access classes ACs with the contention mechanism design parameters. This will allow us to determine detection threshold value to distinguish normal operation and attacks. Then,

we integrate the sequential detection of change method with the developed methodology and we propose the QoS-based Sequential Detection Algorithm (QoS-SDA).

1.3 Contributions of the Thesis

In this section we briefly resume the major contributions of this dissertation. We classify them according to the area they naturally belong to, as illustrated in Figure 1.3.

In the area of maintaining connectivity and enhancing the communication reliability in V2X networks, the main contributions are:

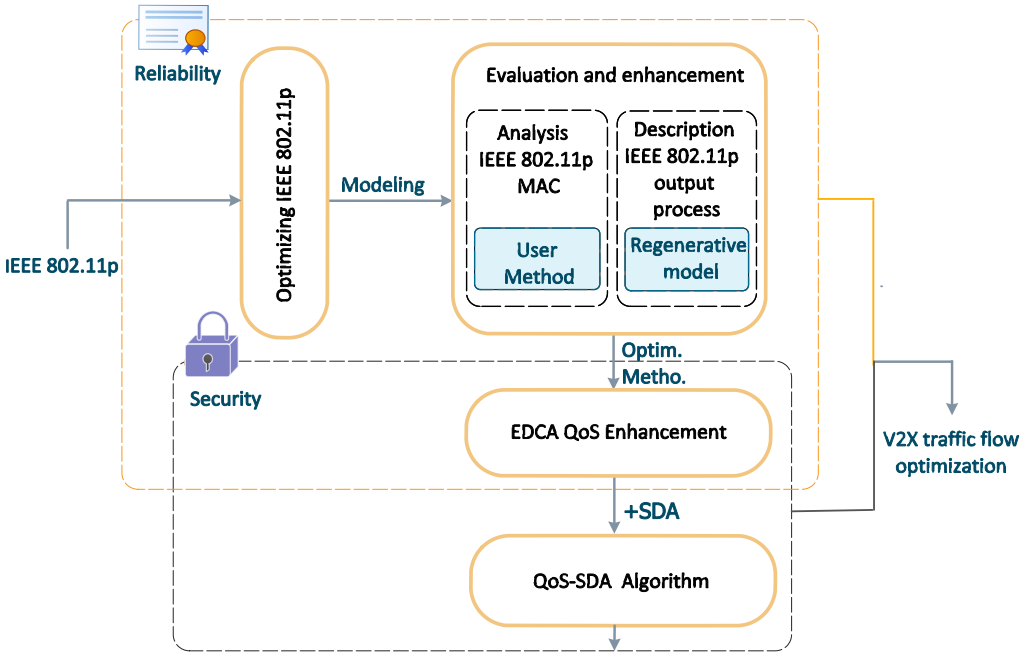


Figure 1.3: Progress of main contributions

1.3.1 Proposition of User Model-based Method for IEEE 802.11p MAC Performance Evaluation

Most of the research in enhancing and evaluating IEEE 802.11p MAC protocol performance has emphasized the use of the Markovian models. However, one feature of Markovian models is very apparent; it is possible to list more disadvantages than advantages in their use. One important drawback of the Markovian models, in this case, is they developed under the saturated traffic conditions, which do not actually reflect the real operation of IEEE 802.11p MAC protocol and consequently fail to provide a complete stability analysis of the protocol.

This thesis looks at IEEE 802.11p MAC protocol analysis from a different perspective that helps to reduce the problem of defining a Markovian model to the problem of determining the steady-state moments of the induced transmission delay process. The proposed method is built on the user density so that the capacity of IEEE 802.11p when employed for real-time applications can be evaluated in the saturated and unsaturated traffic conditions. Moreover, the method provides complete stability analysis of 802.11p MAC protocol which gives us opportunities to further investigate the design parameters of 802.11p MAC, leading to proposed reconfigurations for improved performance.

1.3.2 Efficient Modeling of IEEE 802.11p Output Process for V2X Interworking Enhancement

The next original contribution of this thesis is an efficient solution approach for the basic problem in analyzing hybrid V2X interconnected systems; that is, characterizing the output process of IEEE 802.11p-based DSRC standard. In Chapter 3, we present the Regenerative model that we believe to be the first model which provides a complete description for the output process of IEEE 802.11p leading to traffic flow optimization in the future V2X communications. The major novelties of the proposed model can be summarized as follows:

- Due to its regenerative property, the model leads to define description

models which provide a complete description of IEEE 802.11p output process when employed under different traffic intensities.

- The model incorporates several design parameters in IEEE 802.11p including, contention window size, packet generation rate and the service rate so that important insights can be gained about 802.11p configuration and its functionality to support efficient V2X communications.
- As compared to the widely adopted Poisson model, the proposed Regenerative model is superior in terms of ability and sensitivity to detect changes in IEEE 802.11p output process.

The above mentioned characteristics land the Regenerative model well to describe IEEE 802.11p output process in the future V2X hybrid interworking.

In the area of securing V2X communications against cyberattacks, the main contributions are the following:

1.3.3 Optimization Methodology for DSRC Enhancement

The developed methodology ties the Quality of Service (QoS) requirements of the access classes *ACs* with the basic contention mechanism design parameters in IEEE 802.11p-based DSRC MAC protocol. The aim of this optimization methodology is twofold. The first objective is to propose a procedure to further investigate the design parameters of 802.11p MAC leading to enhanced reconfigurations for improved performance. The second objective is to identify IEEE 802.11p MAC *stability region*, i.e., the input rate region where the traffic is maintained for the access classes. This *stability region* is further used in defining a reference value to distinguish between IEEE 802.11p normal operation and its operation under security threats. As a result, this methodology and the corresponding results are incorporated in the design of a novel detection algorithm for jamming attacks in vehicular networks, which represents our next contribution.

1.3.4 QoS-based Sequential Detection Algorithm for Jamming Attacks in VANET

Motivated by two considerations; the obtained results from the proposed User Model-based Method which revealed security vulnerabilities in IEEE 802.11p MAC protocol and the developed optimization methodology, we propose QoS-based Sequential Detection Algorithm (QoS-SDA). The algorithm can effectively detect jamming attacks, while false detections occur infrequently. Specifically, this contribution can be summarized as follows:

- Utilizing the developed optimization methodology, we define IEEE 802.11p *stability region* from which we decide on a detection threshold value.
- We integrate the developed methodology with the sequential detection of change method and we propose the QoS-based Sequential Detection Algorithm (QoS-SDA).
- The important performance characteristics of QoS-SDA are accuracy and speed, while jamming attacks are detected with a low probability of false alarms. The reported results further prove that the proposed algorithm has a high capability in detecting different jamming attacks even under a small attacking rate.

While our research spans two prominent parts in the field of vehicular networks, i.e., reliability and security of V2X communications, our contributions overall present a new understanding of IEEE 802.11p-based DSRC standard and provide significant improvements for its functionality which in total result in efficient and secure V2X communications. Particularly, the key strengths of this research are its analytical/modeling techniques which we believe to be an attractive alternative to the existing approaches as they represent fairly general tools that could be applied to the conventional wireless networks as well, while their implementations simultaneously involve minimal complexities.

1.4 Structure of the Thesis

The thesis is composed of five chapters and the remaining is organized as follows. Chapter 2 presents the proposed User Model-based Method for IEEE 802.11p MAC protocol performance evaluation in safety applications. The developed method is based on two population user models; Finite and Infinite population model. Chapter 3 extends the proposed method in Chapter 2 to be applied in large-scale vehicular networks and presents the Regenerative model for IEEE 802.11p output process description. The output process modeling and the corresponding results are then incorporated in the performance enhancement of V2X communications in DSRC-cellular hybrid interworking. Chapter 4 focuses on securing vehicular communications, first a novel optimization methodology for EDCA quality of service support is introduced. Then the developed methodology is used in conjunction with the sequential detection of change method to develop the QoS-based Sequential Detection Algorithm (QoS-SDA) for jamming attacks in the vehicular environment. Chapter 5 summarizes the thesis, discusses its findings and contributions, points out limitations of the current work, and also envisions future research directions.

Chapter 2

User Model-Based Method for IEEE 802.11p-based DSRC Performance Evaluation

One very important prerequisite for the successful and also sustainable deployment of V2X is the efficiency of the employed DSRC communication standard.

2.1 Introduction

The backbone of the Intelligent Transportation Systems (ITS) is the Vehicular Ad-hoc Networks (VANETs) which support Vehicle-to-Vehicle (V2V) as well as Vehicle-to-Infrastructure (V2I) communications; the two key components of V2X communications. VANET aims to increase traffic safety and efficiency by warning and informing the driver about road events and hazards. The application area in VANET ranges from safety-related warning applications to information and entertainment non-safety applications. A clear distinction needs to be made between non-safety and safety applications. The main role of non-safety applications is to provide comfort for the driver and passengers, improving traffic system (e.g., parking availability services), adding entertainment (e.g., internet connectivity) while making sure that it does not affect the safety applications [18]. On the other hand,

the goal of safety applications is to improve driving safety level by exchanging safety relevant information between vehicles and between vehicles and other ITS road components. Clearly, safety applications imply increased requirements on the wireless communication and the challenge is not only to overcome the behavior of the unpredictable wireless channel and its errors but also to cope with dynamics of the network due to vehicle movement. By making the invisible visible, VANET enables two types of traffic safety applications, namely Safety and Safety-of-life applications, both sharing one communication channel [13]:

- *Safety applications*: aim to enhance the safety and efficiency of the overall transport system by increasing safety and reducing traveling time and congestion. Safety applications include work zone warning, road condition warning and transient vehicle signal priority.

- *Safety-of-life applications*: aim to reduce the number of fatalities/injuries on the roads by alerting the driver about dangers in advance; that is to communicate about an upcoming emergency situation before the situation is a fact and probably it could be avoided. Safety-of-life applications include event-driven, cooperative collision warning and intersection collision avoidance.

Safety applications in VANETs are discussed in detail in [19, 20]. From the communication perspective, the two safety applications are supported by two safety-related messages: periodic messages and event messages. These types of safety messages are described in the standardized works [21, 22] of European Telecommunication Standards Institute, ETSI. According to ETSI, periodic messages, also called Beacons, are Cooperative Awareness Messages (CAMs) [22]. Beacons are status messages containing status information about the sender vehicle like position, speed, heading, etc., with the purpose of providing the drivers with fresh information about the surrounding environment and their nearby neighbors. On the other hand, Event Messages are Decentralized Environmental Notifications (DENs) that warn unexpected hazards [21]. DENs are messages sent by a vehicle to detect a potential dangerous situation on the road. This information should be disseminated to

alarm not only nearby neighbors but also all vehicles situated in close neighborhoods about a probable danger that could affect the incoming vehicles.

Suitable safety-related messages' communication has low latency (in the range of milliseconds), can cope with the high relative speeds between vehicles (up to 200 km/h) and high dynamic network topology, in addition to be able to bridge a substantial distance (up to 1 km). Such strict requirements impose different challenges in the design of communication standard that should be able to support the most demanded safety applications. Wireless access and communication in VANETs are based on WAVE protocol (Wireless Access in Vehicular Environments) and the main enabling communication standard in the protocol is IEEE 802.11p. IEEE 802.11p is a DSRC-based standard which standardizes the communication aspects related to Physical (PHY) and Media Access Control (MAC) layers in WAVE. The PHY generally addresses the reliability or the error probability of the system; however, if channel access provided by the MAC layer is not a reliable fact the benefits of the PHY cannot be exploited. Hence, the MAC protocol design and its performance in VANET require more attention and focus and should be seriously considered.

In this chapter, we evaluate the communication capacity of IEEE 802.11p MAC protocol to support reliable and efficient communication for safety applications. In this work, we take different approach than those taken in the existing studies. We propose in Section 2.4 a User Model-based Method to evaluate the real-time requirements of IEEE 802.11p MAC. The method uses a powerful result from the theory of regenerative processes, in effect, to reduce the problem of defining a Markovian model (which is so prevalent in literature) to the problem of determining the steady-state moments of the delay process. Its simplicity, together with its operational properties, provides the means for the stability analysis of IEEE 802.11p which is far more difficult to obtain when a Markovian model is adopted. This stability analysis can provide us opportunities to further investigate the design parameters of IEEE 802.11p MAC, leading to proposed configurations for improved performance.

The rest of this chapter is organized as follows: In Section 2.2 we discuss the multiple access problem and review selected related works. Section 2.3 explores IEEE 802.11p for vehicular communications; its spectrum allocation and the MAC contention resolution scheme. In Section 2.5 we present system

stability analysis which depends on the real-time induced delay process when the User model is adopted. Based on the presented analysis we conducted detailed simulations in Section 2.6. In Section 2.7, we present and discuss our conclusions.

2.2 An Overview of Multiple Access and Related Works

2.2.1 Multiple Access Problem

A common distinguishing feature in the safety applications, i.e., Safety-of-life and Safety, is the limited time of data transmission, therefore traffic safety applications could be classified as real-time systems; there should be an upper bound on the transmission delay that is smaller than the deadline. If the emergency message does not reach its destination before a certain deadline then the data is more or less useless and the missed deadline will have more severe consequences on the system performance. A crucial aspect in this respect is the efficient sharing of a common transmission channel among the participating population of the network users (i.e., vehicles). This problem is referred to as the multiple access problem since many independent users attempt to access and hence share a common channel for data transmission.

The solution to the multiple access problem is by using a multiple access protocol which works on allocating the channel between the network users. At a highest level of classification of Multiple Access protocols we could distinguish between Deterministic Conflict-free Access (DCFA) and Random Multiple-Access protocols (RMA) [23]. Deterministic Conflict-free protocols are designed to ensure that transmissions by users, utilizing a common channel for their transmissions, are successful. This is achieved by allocating the channel resources to the users without any overlap between the portions of the channel utilized by different users. Within DCFA protocols we distinguish between Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA). Random Multiple-Access protocols differ in principle from Deterministic Conflict-free

since a transmitting user is not guaranteed to be successful. The protocol must advise a way to resolve conflicts once they occur so all messages are eventually transmitted successfully as is done in Aloha type and the various versions of Carrier Sense Multiple Access (CSMA) protocols.

In view of VANET's bursty-nature users, Random Multiple-Access protocols become more efficient than Deterministic Conflict-free Access protocols. Generally, in the mobile wireless systems the adoption of full sensing random access algorithms is not possible since the latter require that each user knows the overall channel feedback history from the beginning of time. In contrast, Limited Sensing Random Access protocols (LSRA) only require that each user observes feedbacks from the time that he generates a packet to the time that this packet is successfully transmitted; that is the only implementable subclass in RMA protocols is the class of LSRA protocols. The implementation of LSRA is done through the MAC layer which provides a controllable resource-allocation for the shared channel among the network users.

2.2.2 Related Works

A considerable amount of literature has been published on developing analytical models for the IEEE 802.11 MAC protocol family [24–26]. The majority of these studies have been based on Bianchi's work in [27]. Bianchi analyzed the performance of a saturated network using two-dimensional Markov chain in which each stage represents the backoff time counter of a node. Early analytical methods for the IEEE 802.11p protocol were presented in the works of Torrent-Moreno *et al.* [28, 29]. These works investigated critical information dissemination in 802.11p VANET. In a similar vein to Torrent-Moreno's work, Gallardo *et al.* in [30] and [31] have developed a Markov-based analytical model to study the behavior of the Enhanced Distributed Channel Access (EDCA) considering specific conditions of the Control Channel (CCH) in vehicular environment. One drawback of the proposed model is that it is unidimensional in the sense that it did not consider the internal contention among the supported Access Classes ACs. He *et al.* in [32] have proposed a two-dimensional discrete Markov chain to study the influence of different Arbitration Inter-Frame Space (AIFS) in IEEE 802.11p EDCA. The authors

considered only the saturated condition of the traffic for immobile vehicles at an urban intersection. In [33–36], another Markovian models were developed for evaluation and enhancement of IEEE 802.11p MAC protocol which did not take into account all the required factors such as saturation and the internal competitions among the access classes. One common factor is that the existing recent works are mostly based on Markovian models which usually give insufficient information on the stability of IEEE 802.11p MAC protocol due to their scalability and hidden state issues; as a result, this limits their ability to correctly represent the unique characteristics of the vehicular environment.

Several attempts have been made to investigate the capacity of IEEE 802.11p MAC protocol to provide reliable safety message dissemination under different physical environments. In [37, 38] and [39] the protocol investigated through a comparative performance evaluation for different radio propagation and driving environments. The studies in [40, 41] examined the performance of IEEE 802.11p MAC under different routing protocols and for relatively small sized networks. Overall, these studies did not investigate the scalability issue in VANET; in vehicular environment, safety data operations and their time limitations are dictated by the application objective, in conjunction with the users' density. Varying users' density induce dynamics in the delay process mainly within the worst case scenario when a large population of users is considered, hence establishing a relation between the models of user's population is eminent in order to address these challenges. In contrast to the aforementioned studies, the proposed User model allows us to consider both the saturated and the unsaturated traffic conditions, in addition, to derive equations related to internal contention resolution process which was not appropriately addressed in most of the existing studies.

2.3 IEEE 802.11p for Vehicular Communications

2.3.1 DSRC Spectrum Allocation

IEEE 802.11p is a standard protocol intended to operate with IEEE 1609 standard suite to provide Wireless Access in Vehicular Environment (WAVE) in order to support safety and commercial non-safety applications for vehicular communications. The IEEE 802.11p standardization process originates from the allocation of DSRC spectrum band in the United States and the effort to define the technology for usage in the DSRC band. In USA, the Federal Communication Commission (FCC) allocated 75 MHz of DSRC spectrum at 5.9 GHz to be used exclusively for V2V and V2I communications. In Europe, the Electronic Communications Committee of the European Conference of Postal and Telecommunications Administrations (CEPT) has allocated a 30 MHz of spectrum band in the 5.9 GHz range for the purpose of supporting vehicular communications for safety and mobility applications.

Referring to Figure 2.1, the IEEE 802.11p spectrum is divided into six Service Channels (SCH) and one Control Channel (CCH) each with bandwidth of 10 MHz from channel 172 to 184. The control channel, channel 178, is assigned for common safety-related and control data. The control information over CCH is sent by the WAVE providers (e.g., RSUs) into Wave Service Advertisement (WSA) to announce the possible set up of Wave-based Basic Service (WBSS) over a given SCH. The FCC further designated service channels 172 and 184 for Safety-of-life and public Safety applications respectively. The other service channels are designated for non-safety and traffic efficiency applications. In order to lower costs and to encourage VANET deployment and adoption, the standard defines a channel coordination mechanism that allows single radio ITS nodes to switch between the CCH and the SCH. The multichannel operation allows these nodes to receive important safety messages while general purpose applications are active [42, 43]. The rationale behind such bandwidth allocation with special support for safety indicates the primal importance of safety applications in VANET.

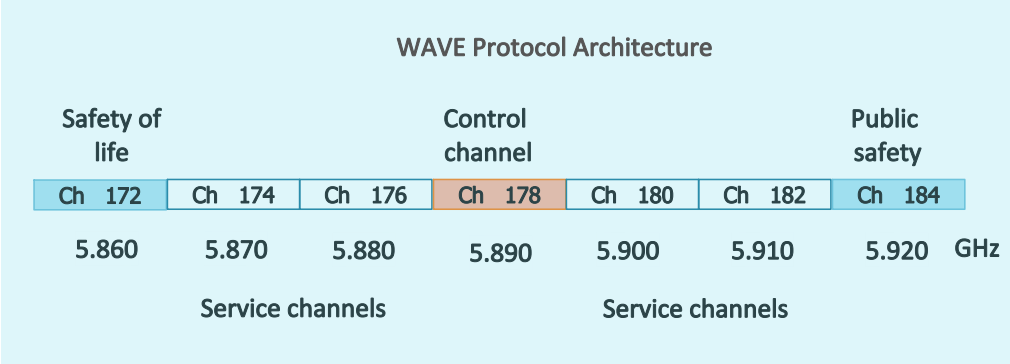


Figure 2.1: DSRC allocated spectrum

IEEE 802.11p standard is not a standalone standard; it is a modified version of IEEE 802.11a. The IEEE 802.11p physical layer is OFDM-based, and quite similar to the IEEE 802.11a physical layer (PHY) design. The main difference is in the overall bandwidth used, which is 10 MHz for IEEE 802.11p instead of the 20 MHz of IEEE 802.11a [5]. Practically all the other changes in the PHY stem from this difference. IEEE 802.11p uses the Enhanced Distributed Channel Access (EDCA) as MAC method, which is an enhanced version of the basic Distributed Coordination Function (DCF) from IEEE 802.11a. The EDCA uses (CSMA) with collision avoidance (CSMA/CA) while prioritization is provided by four access categories with AC_0 has the lowest priority and AC_3 the highest priority.

In the proposed User Model-based Method, we particularly focus on how well the implemented contention resolution process can guarantee low delays and high channel access rates for safety-critical communications. Since the focus of the analysis is on the MAC layer, some reasonable assumptions regarding the PHY should be made. We consider one-dimensional vehicular network and slotted channel, we also assume synchronous transmissions where the packet's transmission can start only at the beginnings of the slots. The generated packets are stored in an infinite size buffer on a first in, first serve base. We also require that no propagation delays exist and collisions are the only cause of channel errors; that is, a single packet transmission is always successful and that collisions cause destruction of all the involved packets which must then be retransmitted.

2.3.2 The Contention Resolution Algorithmic System

With the foregoing assumptions adopted, let the queues of all users be empty at the beginning of slot $T_0 - 1$ and let the algorithmic system starts at slot T_0 so that the CCH channel is idle. Then, the active users whose buffer queues are nonempty at T_0 start attempting to transmit and the collision resolution process begins. This initial process will involve only the traffic formed by the head packets coming out of the buffers of the active users where a Contention Resolution Interval (CRI) starts. The successful user in the current CRI reserves the channel to sequentially transmit all his stored packets at T_0, while the remaining users hold their transmissions. A holding/backlogged user will wait until its Backoff Timer (BT) decreases to zero to be able to transmit.

The BT value is chosen randomly from a uniform distribution and drawn from a Contention Window (CW) in the interval $(0, CW_{min})$. This latter value can only start to be decremented after the channel is sensed idle for period greater than or equal to an AIFS (Arbitration Inter-Frame Space), as shown in Figure 2.2. For every retransmission attempt, the BT value will be doubled from its initial value until reaching CW_{max} and then if the packet reached the maximum number of attempts it will be rejected out of the system. The contention parameters, adopted from [42] are shown in Table 2.1. In addition, the values of CW_{min}, CW_{max} are defined as 15 and 1023 respectively and the maximum number of attempts is set to seven attempts.

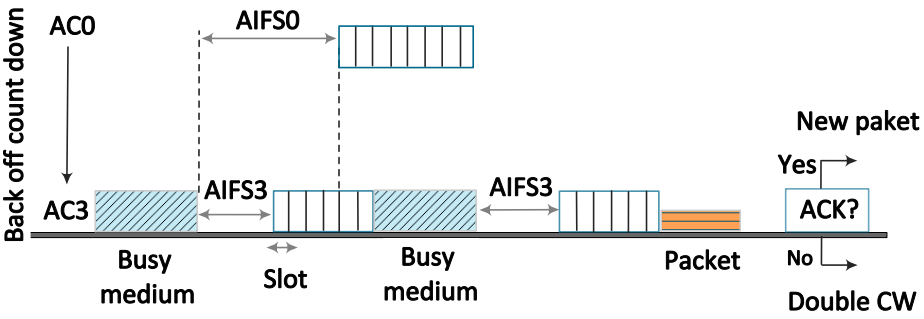


Figure 2.2: EDCA backoff procedure

Table 2.1: EDCA parameters for CCH

AC	ACI	CW_{min}	CW_{max}	$AIFS$
Background	AC_0	15	1023	9
Best effort	AC_1	15	152	6
Safety	AC_2	7	15	3
Safety-of-life	AC_3	3	7	2

2.4 User Model

The IEEE 802.11p MAC is based on Carrier Sense Multiple Access (CSMA) protocol, which lies within the class of Random Multiple Access protocols (RMA). In the analysis of such protocols, two population user models could be considered [44] :

1. Finite population model: where a finite number m of identical and independent users (i.i.d) are attempting to get access to a common channel.

2. Infinite population model: where the cumulative packet arrival process for $m \to \infty$ is comprising a homogeneous Poisson process with intensity λ packets per slot.

In order to quantitatively assess the performance of IEEE 802.11p MAC protocol, the analytical model should be developed with a set of suitable parameters. It is worth mentioning that some of the parameters presented in the analysis that follows are deterministic and some of which are random variables.

2.4.1 Finite Population Model

We initially consider the finite model: Given a slotted channel and a finite number m of i.i.d users. In slot time T, each user s possesses the following attributes:

- The user generates a number N_T^s of packets. The random variables N_T^s are i.i.d with distribution

$$P_m(N_T^s = n) = p_n, \quad N_T^s \sim P_m(\eta_m, \sigma_m^2) \tag{2.1}$$

  where η_m and σ_m^2 are the finite mean and the variance of the distribution respectively. Once a packet is generated the user will retain it in an infinite size buffer.

- At the beginning of a slot T, the user is assumed to be in one of the two modes: active, if his buffer queue is nonempty, or non active (this makes the analysis more meaningful since the assumption of the saturated mode where all the users are active and have packets to be transmitted will not be the only considered mode).

- If we redefine (2.1) to take the form $P_m(N_T^s = 1) = p_1$, then $p_1 \triangleq p_T$ where p_T denotes the probability of an active user to transmit once in the slot T.

Let T correspond to a starting point of some CRI, then the probability that a backlogged user retransmits in any of following slots is independent of how many slots it has waited. The probability that a backlogged user retransmits in i-th slot is a geometrically distributed having the form

$$P(i) = (1-q)^{i-1}q \tag{2.2}$$

q is the probability of a backlogged user to retransmit once in the slot i.

If $\overline{T}$ is the ending point of the current CRI, then at $\overline{T}+1$ the next CRI starts. The probability that there are n new active users at the beginning slot of the next CRI is

$$P_m(n \mid L) = \binom{m}{n}(1-p_T)^{(m-n)L}(p_T)^{nL} \tag{2.3}$$

where L is the expected length of the previous CRI in slot units.

2.4.2 Infinite Population Model

Given a Random Multiple Access protocol (RMA) and an input distribution satisfying ϕ mixing conditions as those in (2.1), the problem then is to exploit the dynamics of the protocol, to find those per-CRI properties of the underlying function of the process that could be used to evaluate the throughput and subsequently to assess the system stability. In real-time safety applications, the stability of IEEE 802.11p MAC protocol translates to maintain the data traffics with finite bounded delays and non-increasing rejection rates. In this case, all the necessary stability conditions are asymptotic, assuming asymptotically large number of users and require that the acting high rates be bursty. Needless to say that characterizing the IEEE 802.11p MAC properties under the Infinite model would then be required to render the stability analysis possible.

The Infinite population model is derived from the Finite model if we let m diverges to extreme and η_m and σ_m^2 in (2.1) simultaneously to decrease, such that

$$\lim_{m\to\infty} m\eta_m = \mu \qquad 0 < \mu < 1 \tag{2.4}$$

Furthermore, if $P_m(n) = P_m(n \mid 1)$ in (2.3). Then, $P_m(n)$ is the distribution of n active users at the beginning of a single slot with mean parameter mp_T whereas p_T decreases as m increases

$$\lim_{m\to\infty} mp_T = \lambda \qquad \text{for a positive constant } \lambda \tag{2.5}$$

If, in addition to the existence of the limit in (2.5), the mean of the divergence distribution is equal to the limit of the mean, i.e., $\mu = \lambda$, then $P_m(n)$ converges in distribution to Poisson such that

$$\lim_{m\to\infty} P_m(n) \to Pois(\lambda) \colon Pois(\lambda) = e^{-\lambda}\frac{\lambda^n}{n!} \tag{2.6}$$

Thus, under the conditions stated above, Poisson theorem holds [45], which simply states that independently of the arrival process per user, as long as it is i.i.d, the limit of the cumulative arrival process is Poisson. A connection between the performance of IEEE 802.11p under the Finite and the Infinite

population model is established in the sequel of the following section.

2.5 Stability Analysis

As previously mentioned, the stability of IEEE 802.11p MAC protocol in real-time safety applications translates to maintain the data traffics with finite bounded delays. In this section we present stability analysis in terms of the induced delay process, where we define the delay experienced by a transmitted packet as the time difference between its arrival and the end of its successful transmission. The evaluation of MAC stability in IEEE 802.11p is then related to the existence of the steady state of the delay process. The method for the delay analysis is motivated by the work in [46]. We express the analytical characteristics in the following lemma

lemma 1. *Let the algorithmic system of IEEE 802.11p MAC starts at time* T_0 *and define the sequence* $\{R_i\}_{i\geq 1}$ *such that* $T_0 \leq R_1 \leq R_2 \leq \ldots$ *to be the collision resolution time points on the most ending edges of slots containing successful transmissions and at which the lag is one. Let* $S_i, i \geq 1$ *to be the number of successful transmissions in the interval* $(T_0, R]$ $\forall R \in \{R_i\}_{i\geq 1}$ *then*

$$S_i = \sum_i 1(R_i \leq R) \qquad \forall R \in \{R_i\}_{i\geq 1},\, i \geq 1 \tag{2.7}$$

Thus S_i is a renewal counting process where the inter-renewal times $\zeta_j^i,\ 1 \leq j < i$ are i.i.d. If $y(n)$ denotes the packet delay; the distance between its arrival and its successful transmission, then for the process $\{S_i, y_i(n)\}$ with inter-renewal times ζ_i^j, the following regenerative theorem holds [47]

For the process $\{S_i,\, y_i(n)\}$, $i \geq 1, n \geq 1$ with iner-renewal times ζ_j^i, $1 \leq j < i$, its sample path τ_j in the time interval $(R_j, R_{j+1}]$ is described by:

$$\tau_j = \left(\zeta_j^i,\, y_j(n) : 1 \leq j < i,\, n \geq 1\right) \tag{2.8}$$

Then τ_j is the j-th segment of the process S_i and the process $y_i(n)$ is a regenerative process with respect to it. The process $y(n)$ is regenerative over all the renewable points $\{R_i\}_{i\geq 1}$ as its segments τ_i have i.i.d lengths. Giving

that the sequence $\{\tau_i, i \geq 1\}$ is i.i.d, then the mean segment length

$$E\{\tau_i\} = E\{\tau_1\} = \Gamma \tag{2.9}$$

If the mean segment length is bounded, i.e.

$$\Gamma < \infty \tag{2.10}$$

Then, the nonnegative real-valued sample function $\{f(y(n), n \geq 1)\}$ of the discrete time process $y(n), n \geq 1$ is also regenerative over all $\{R_i\}_{i\geq 1}$ as it inherits the regenerative property.

Let us define Y to be the expected value of the sample function $\{f(y(n), n \geq 1)\}$ in the first segment τ_1 such that

$$Y = E\left\{\sum_{n=1}^{\tau_1} f\big(y(n)\big)\right\} < \infty \tag{2.11}$$

From the strong law of large numbers the first equality in the following expression holds with probability one

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N}\Big\{f\big(y(n)\big)\Big\} &= \lim_{N\to\infty} \frac{1}{N} E\left\{\sum_{n=1}^{N}\Big\{f\big(y(n)\big)\Big\}\right\} \\ &= \frac{1}{\Gamma} E\sum_{n=1}^{\tau_1}\Big\{f\big(y(n)\big)\Big\} = \frac{Y}{\Gamma}\end{aligned} \tag{2.12}$$

Let us define the function $f\left(y(n)\right)$ such that $f\left(y(n)\right) = y(n)^i$ as this will permit the computation of the i-th moment of the steady state delay process. Since our interest in the first moment then there exists a real number D such that:

$$D = \lim_{N\to\infty} \frac{1}{N} E\left\{\sum_{n=1}^{N} y(n)\right\} = E\big\{y(\infty)\big\} = \frac{Y}{\Gamma} \tag{2.13}$$

D is the mean packet delay.

If the mean segment length is bounded and expected value of the sample function $f(y(n))$ exits, then the mean of the limiting distribution of the delay process exist and its value is given in terms of (2.9) and (2.11).

2.5.1 System of Equations Related to the Per-segment Length

Our objective here is to develop a system of equations from which Γ can be determined, in addition to derive equations related to internal collision resolution process. The computation of the mean segment length Γ in (2.13) depends on the input traffic rate. If the rate of the input traffic is μ, then

$$\Gamma = \mu L \tag{2.14}$$

where L is the mean value of the CRI length.

In the following we compute the mean CRI length.
Define L_m to be the mean of the CRI length given that it starts with a collision multiplicity m (i.e., m users in the first slot), let $L_{m|n}$ to be the mean of the CRI length conditioned on having n users with counter value 0. Then from the description of the contention resolution algorithmic system, the following equations hold:

$$L_{m|n} = \begin{cases} 1 & \text{for } m = 0, 1 \quad (2.15a) \\ 1 + L_n + L_{m-n} & \text{for } 1 \leq n \leq m \quad (2.15b) \\ 1 + L_m & \text{for } n = 0 \quad (2.15c) \end{cases}$$

The probability that n users will transmit in the first slot after the collision slot is $P_m(n)$. Since $L_m = \sum_{n=0}^{m} L_{m|n} P_m(n)$, then, we obtain a finite dimensional linear system of the form

$$L_m = 1 + \sum_{n=0}^{m} (L_n + L_{m-n})\, P_m(n) - P_m(0) \tag{2.16}$$

The probability $P_m(0)$ results from (2.15b) when none of the users in the initial collision has counter value 0.

Table 2.2: CRI length giving m packets in the first slot

m	0	1	2	3	4	5	6	7
L_m	1	1	4.5	7	9.66	12.32	14.98	17.65

Solving for L_m we obtain the following recursion for $m \geq 2$

$$L_m = \frac{1 - P_m(0) + \sum_{n=0}^{m-1} L_n\big(P_m(n) + P_m(m-n)\big)}{1 - P_m(0) - P_m(m)} \tag{2.17}$$

The initial values are given in (2.15a).

Table 2.2 contains the first few values of L_m resulted from solving (2.17). This table is quite revealing in several ways:

- First, the CW values in Table 2.1 are defined so that $CW \leqslant$ the actual CRI length, hence by comparing the data from the two tables we notice the following. The minimum m value that satisfy the corresponding CW value for the Safety-of-life class is $m = 1$, for Safety class is $m = [2, 3]$ and for Non-safety classes, i.e., AC_1, AC_0 is $m = [5, 6]$. These values show the tight region for the defined CW values in the protocol. The results and the discussion in the upcoming section clearly show the limitations for using such CW tight values especially for AC_3 class; as soon as several nodes contend using AC_3, a collision becomes very likely and the successful throughput reduces significantly.

- Second, from Table 2.2, it can be easily seen that every odd number is a possible value of L_m. This observation allows us to find a simplified form for the computation of the conditional distribution of CRI length $P(l \mid m)$ which is unrewardingly tedious to compute without this simplification. This conditional distribution will be used in Chapter 3 to build a description model for the output process (i.e., the departure process of the successfully transmitted packets) of IEEE 802.11p MAC protocol.

- Finally, from Table 2.2 we can see that $L_m - L_{m-1} = 2.66$, which implies the existence of a constant γ, i.e.,

$$L_m = \gamma m - 1 \qquad \text{for } m \geq 3,\ \gamma = 2.66 \tag{2.18}$$

The latter expression represents an upper bound on the CRI length L_m which shows the coarse dependence of L_m on the user density m. In Chapter 3 we develop a technique for obtaining a tight upper bound on L_m.

2.5.2 On the Relation Between the User Model and Stability of IEEE 802.11p

Although expression (2.13) along with (2.14) and (2.18) show how the delay process intimately interwoven with the algorithm's dynamical behavior and consequently provides a fair perception for how the delay process impact the overall system stability, there remain some technical issues that need to be examined. The peculiarity of the user model under which the algorithm is employed and how good delay characteristics and stability could be guaranteed. These issues are addressed in the following lemma which characterizes the trade-off among the Key Performance Indicators (KPIs) of IEEE 802.11p, namely latency, reliability, and throughput, and defines the inter-relationships among them under the two user models.

lemma 2. *Let L_i denotes the length of i-th CRI as induced by the algorithmic system, from (2.3) the sequences $\{L_i\}_{1\leq i<\infty}$ is clearly a Markov chain. Let μ to be the input rate of IEEE 802.11 MAC algorithmic system and $E\{y(\infty)\}$ to be the first moment of the steady state delay process as defined in Lemma (1). Then, the system throughput $\overset{\star}{\lambda}$ is defined as*

$$\overset{\star}{\lambda} = \sup\left(\mu \colon E\{y(\infty)\} < \infty\right) \tag{2.19}$$

The latter throughput definition is meaningful to capture the system stability under the two user models as follows:

1. For the Finite user population model described in (2.1), given $m <$

∞, provided that $\mu < 1$ then the conditions in (2.1) is sufficient to guarantee the boundness of F. Since $\mu < 1$ then necessarily p_T in (2.3) is such that $p_T > 0$ and then the Markov chain L_i is aperiodic and ergodic. The ergodicity of the Markov chain guarantees the boundary condition for Γ in (2.14) and so is then the mean packet delay D is bounded, i.e., $\lim_{m\to\infty} E\{y(\infty)\} < \infty$.

2. As the number m of the users increases and the quantities η_m and σ_m^2 become infinitely small so that the arrival process is Poisson such that $m\eta_m = \mu \ \forall m$, $\mu > \overset{\star}{\lambda}$. The Infinite model in (2.6) implies that $p_T \to 0$ as $m \to \infty$, then the boundary condition of (2.14) is violated and the random variable $y(\infty)$ will assume infinite values, i.e., $\lim_{m\to\infty} E\{y(\infty)\} = \infty$.

Remark 1. *Since mixing implies ergodicity [48], the ergodicity of Markov chain L_i is legitimate as long as the ϕ mixing conditions in (2.1) are valid. Therefore, for any finite number of independent and identical users in the system, and any arrival process per user as this in (2.1), the IEEE 802.11p MAC protocol is stable provided that the total input rate is less than one.*

2.6 Model Validation and Performance

Apart from speed and dynamic patterns of the deployed nodes, density is the third key property of vehicular mobility as vehicles in mutual radio range may vary from dozens to hundreds [49]. We have developed a simulator in Matlab for the simulation scenario. For the Finite model the number of vehicles is set to 30. The traffic is modeled as Bernoulli process, which stratifies the Φ mixing conditions in (2.1), with the parameters $\eta_m = 0.1$ and $\sigma_m^2 = 0.09$. While the Infinite model traffic is modeled as Poisson process with $\lambda = 0.4$ and 300 vehicles. The speed of each vehicle is modeled as a Gaussian random variable with mean value $70km/hr$. Empirical studies have shown that the vehicle speed in the flow state follows a Gaussian distribution [50].

As previously mentioned, the stability of IEEE 802.11p MAC protocol is determined by its throughput in the presence of the Infinite model when applied for real-time safety applications. Therefore, the rest of this section will

Table 2.3: Parameters setting for simulation scenario

Parameter	Value	Parameter	Value
Traffic rate	Variable (0.1 to 0.4)	CW_{min}	15
Vehicle speed	$70\,km/hr$	Attempt limit	7
TR	$500\,m$	Back-off slot	$16\,\mu s$
Packet Length	$500\,byte$	Propagation delay	0

be devoted to further investigate IEEE 802.11p MAC performance under the Infinite model. The packet abandons the system if its waiting time exceeds given threshold, i.e., CW_{max}^{AC}, and the attempt limit, we consider the delay to be infinite for the rejected packets. Since the transmission range (TR) of IEEE 802.11p at data rate of $3\,Mbps$ is up to $1000\,m$ and less than $200\,m$ at $27\,Mbps$, the value of $500\,m$ as a transmission range is rational. $500\,byte$ is a reasonable packet size including data and security information. Table 2.3 shows a summary of the parameters used in the simulation scenario.

Figure 2.3 validates the results of Lemma 2, it shows that the IEEE 802.11p is stable under the Finite model as the average delay for the four access classes is modestly increased. Whereas the Infinite model induced delay is significantly increasing for each access category with AC_0 having the highest induced delay. We expect that such delay increase will then be much higher for input rates above 0.4.

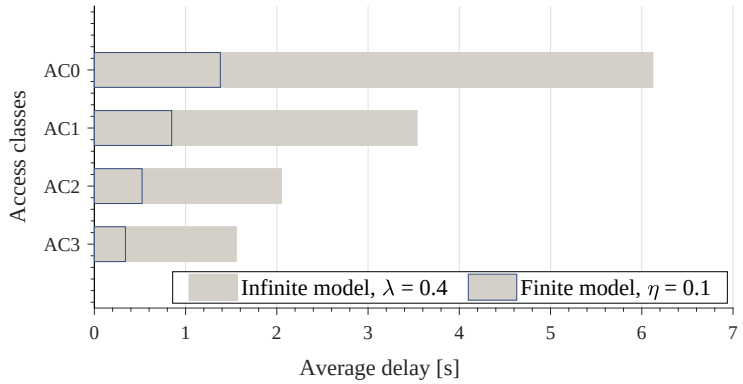


Figure 2.3: Average delay of Finite and Infinite model for different access classes

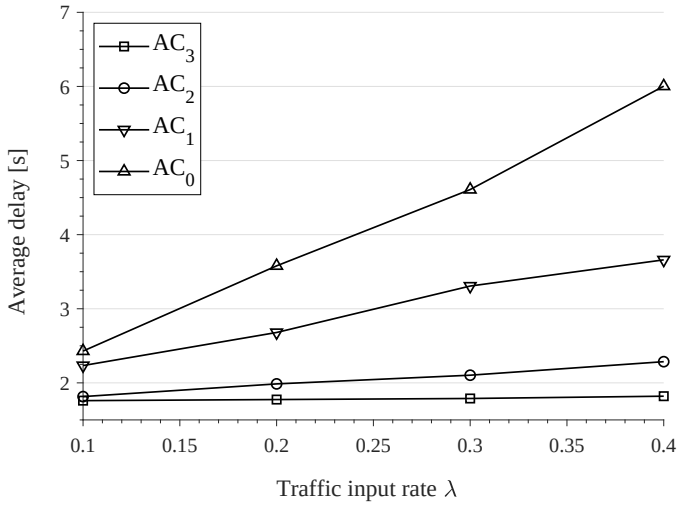


Figure 2.4: Average delay for messages of different access classes

In Figure 2.4 the average delay for the four ACs is plotted. The delay process as induced by (2.13) is shown to be a monotonically increasing with input rate λ. The low priority packets in AC_1 and AC_0 are suffering from an exponential increase of the average delay, primarily due to the large CW values and long AIFS times. Although this contention scheme clearly gives privilege for safety classes, the delay of the safety messages also goes up and the latter increase is noticeable for AC_2 at input traffic rates above 0.3.

Figure 2.5 demonstrates the shortcomings of IEEE 802.11p MAC protocol. AC_3 users are experiencing packet drop of almost 40% as the traffic rate increases, mainly due to the shorter contention cycles which produce more collisions and force the packets to reach the maximum number of attempts quickly and hence abandon the system early. This can be seen in greater detail in Figures 2.6 and 2.7. Figure 2.6 shows that for all the access classes the average number of sending attempts is exponentially increasing, this can be explained by the increasing number of collisions on the channel as the traffic rate increases. While Figure 2.7 illustrates that the majority of packets who attempted up to the maximum number of attempts are those who generated from the higher input rate, i.e., 0.4.

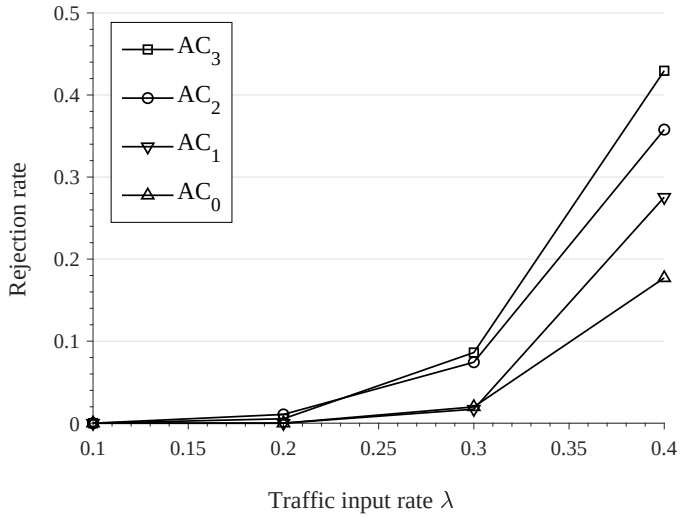


Figure 2.5: Rejection rate for messages of different access classes

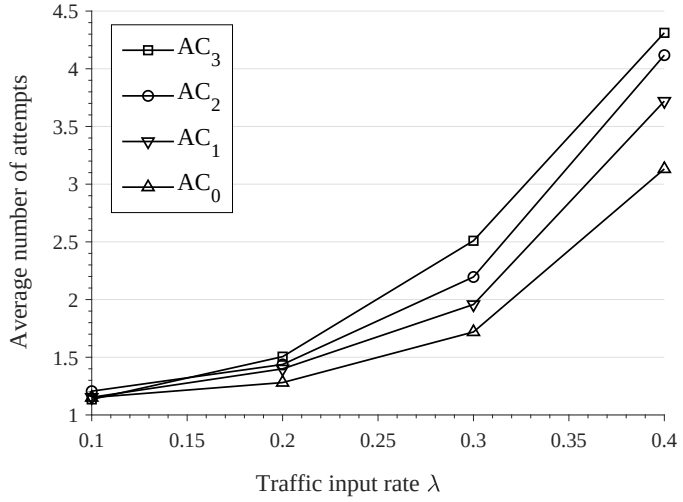


Figure 2.6: Average number of sending attempts for different access classes

It can be observed that IEEE 802.11p can prioritize groups of messages over others. Even though the delay of Safety-of-life messages in AC_3 is not affected that severely by the increase in the traffic rate. The average value of $1.5s$ is relatively high, considering that collision warning messages should have a maximum delay of $100\,ms$ to be able to provide a reliable service [51].

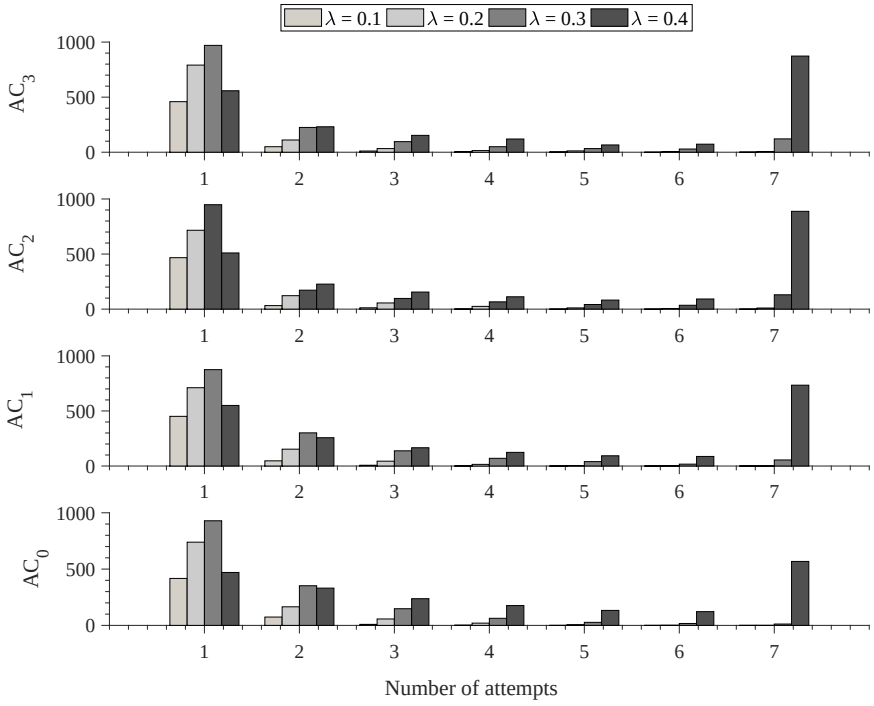


Figure 2.7: Attempts' distribution for various input rates

The results, as shown in the previous figures, indicate that to reduce the probability of collisions the CW size has to be increased; however, this leads to a further increase in the average delay and consequently to a throughput reduction.

2.7 Conclusions

For the dissemination of safety messages in Vehicular Networks (VANETs), the Medium Access Control (MAC) protocol of the enabling communication standard, IEEE 802.11p, becomes the dominant component that determines the transmission efficiency of the emergency messages. For example, emergency messages may experience unpredictable delays due to medium access contention mechanism, and long medium access delay is intolerable for safety applications in VANETs. Besides delay, packet rejections induced by the collisions is another serious problem for emergency message disseminations at the MAC layer where a single message loss due to the increased rejection rate

could result in the loss of life. Consequently, evaluating the IEEE 802.11p MAC protocol is of a great importance in order to assess the capacity of the protocol to provide high reliability and low latency for the dissemination of safety messages in VANET. One accurate and highly effective way to study the performance of IEEE 802.11p standard is by developing an accurate analytical model that translates its actual operation and functionality into mathematical equations.

In this chapter, we presented User Model-based Method for evaluating and enhancing IEEE 802.11p MAC protocol in VANET. The proposed method utilizes different approach than those taken in the existing literature; it reduces the problem of defining a Markovian model to the problem of determining the steady-state moments of the induced delay process. Its simplicity, together with its operational properties provide the means for the stability analysis of IEEE 802.11p MAC protocol which is far more difficult to obtain when a Markovian model is adopted. This stability analysis can provide us opportunities to further investigate the design parameters of IEEE 802.11p MAC, leading to proposed reconfigurations for improved performance. The analytical results verified through extensive simulations revealed that IEEE 802.11p MAC is stable under the Finite user model, providing sufficient quality of service (QoS) for safety messages delivery. However, in the presence of the Infinite user model, IEEE 802.11p MAC protocol fails to satisfy the required QoS for the safety messages. The results advise increasing the contention window size of safety messages class to enhance the reliability; however, this leads to a further increase in the average delay. Our results show that IEEE 802.11p MAC has a tradeoff between the acceptable delays and the acceptable loss in traffic and this tradeoff is only determined by the peculiarity of the safety application.

Chapter 3

Efficient Modeling of IEEE 802.11p Output Process for V2X Large-scale Enhancement

Since V2X must be deployable in the near term and extended to the future, it must provide the necessary high interworking performance to meet use cases of today while being futureproof.

3.1 Introduction

One of the main challenges inherent to the deployment of large-scale vehicular networks VANETs is operability. This issue arises due to the limitations of DSRC, which is the main enabling technology for communications in VANET. The first limitation originates from the inherent short range characteristic of DSRC which is around $300\,m$ for V2V communications. Another major limitation of DSRC results from the Medium Access Control (MAC) protocol employed by the DSRC standard IEEE 802.11p. In Chapter 2 we addressed this limitation in detail, the results showed that with high traffic density, the increase in collision among the transmitted packets in the shared communication channel results in an increase in the packet rejection rate leading to a considerable degradation in IEEE 802.11p performance, especially for safety messages dissemination.

A solution to the scalability issue in V2V communications necessitates the use of pre-existing network infrastructures, called Road-Side Units (RSUs). Depending on the origin of the transmission, infrastructure-related schemes can be classified as Vehicle-to-Infrastructure (V2I) or Infrastructure-to-Vehicle (I2V) schemes. Under V2I scheme, vehicles contact the RSU to report their conditions or request information. This kind of application can be easily implemented as the RSU position is stored in Wave-based Basic Service (WBSS) advertisement frames and self-positioning awareness of all the vehicles (equipped with GPSs) allow vehicles to dynamically select the data rate for unicast transmission towards the RSU. By contrast, in I2V scheme, the RSU provides customized pushing services by contacting a specific vehicle; the RSU can notify a vehicle about specific conditions, such as an accident on the vehicle's planned route, or a parking lot at its destination that has vacancies. It is quite clear that I2V has the potential but the two schemes present challenges that limit their ability to provide reliable data transmission for large-scale networks. These challenges could be summarized as follows:

- Firstly, the dwell time of a vehicle inside an RSU area is small, hence blind spots may exist in which vehicles lose the connection to the infrastructure, particularly if the vehicle is moving with a high speed. To maximize the availability of RSUs, RSUs should be densely deployed which can be very expensive.

- Secondly, vehicles' mobility induces dynamics in the traffic density which leads to uneven distribution of traffic loads on different RSUs. When the number of requests is increased, an important challenge is to implement a suitable scheduling algorithm which serves as more requests as possible.

- Finally, extending the coverage range of vehicles' radios may widen connectivity area of the network, however, this solution is associated with several drawbacks such as smaller data rates and increased packet collision which may result in unbounded delivery delays. Furthermore, this may result in high levels of energy consumption, especially by RSUs.

With the development of wireless communications, the concept of co-operative systems has gained further acceptance, as the revolution and the plethora of wireless communications has captured the interest of infrastructure owner-operators, as well as vehicle manufacturers. The availability of heterogeneous access networks at any geographic area arises as a key solution to the short-range VANET issues and to provide means for further revolutionary applications in intelligent transportation systems. This situation translates into Vehicle-to-anything (V2X) communications which enable information exchange among vehicles and other components of the ITS system, i.e., infrastructure components like RSUs, traffic lights/signs and pedestrian handled devices [4]. V2X is a promising communication technology which expected to revolutionize the ground transportation system by improving traffic safety and efficiency for people on roads.

The future deployment of V2X requires interworking between different access technologies, i.e., DSRC and cellular networks. These wireless access technologies have characteristics that perfectly complement each other. Cellular systems provide wide coverage areas, full mobility and roaming, but due to the centralized architecture, cellular networks offer low bandwidth connectivity and limited support for data traffic particularly for safety applications that have very strict latency requirements. On the other hand, DSRC provides high data rate at low cost, but only within a limited area. A primary concern in achieving an efficient V2X DSRC-cellular interworking is the multi-hop packet transmission issue, mainly originating from V2X hybrid architecture. The multi-hop issue is defined as the capability of the mobile nodes (vehicles) to provide connectivity to a variety of access technologies in the interconnected hybrid network. The main challenge to resolve the multi-hop issue is characterizing the output process of IEEE 802.11p-based DSRC standard that is employed in the network mobile nodes. This output process is the input traffic process to the other nodes (i.e., cellular Base Stations (BSs) and RSUs) in the interconnected network and affects considerably its operation.

The analytical tractability inherent to the memoryless Poisson model has tempted many researchers to adopt this model for the description of the interconnected network traffic processes; however, its validity for modeling the

bursty real-time traffic has often been questioned [52, 53]. In the high time-varying nature of vehicular networks we believe that the output process of IEEE 802.11p exhibits considerable changes under different traffic intensities, as we have seen in Chapter 2 that the network induced packet delay is a function of the traffic intensity rate. On the other hand, as the traffic intensity increases, the output process flow tends to be bursty which makes the Poisson model unsuitable for modeling the output process of IEEE 802.11p. This claim is investigated in the following subsection in detail.

3.1.1 Motivation

The network induced packet delay is defined as the time difference between its generation time and the end of its successful transmission. The distance between two successful transmissions in the delay process constitutes the interdepature output process of IEEE 802.11p. The change in the traffic intensity has an impact on the network connectivity and on the likelihood of congestion on the shared communication channel which induces dynamics in the delay process of IEEE 802.11p mainly at high traffic intensity. In a high traffic scenario, the intensity of channel contention among the transmitted packets increases significantly due to a high transmission collision rate, resulting in a large induced packet delay. Since the interdeparture process is regenerative with respect to the delay process, the output interdeparture distribution will be affected by the changes in traffic intensity.

This effect of traffic intensity on the induced packet delay process and the regenerative interdepature process is visualized in Figure 3.1. In this figure, one dimensional vehicular network and a slotted shared communication channel with no propagation delays are considered. The input traffic rates in (packet/slot) are $\lambda = 0.1$ and $\lambda = 0.4$. The simulations were run for the four access categories ACs each with its defined contention parameters. In the first Subfigure (a), the delay process is shown to be monotonically increasing with the traffic input rate. The delay for the ACs is modestly increased at low rate, i.e., $\lambda = 0.1$ as the intensity of channel contention among the transmitted packets is not severe. As the input traffic rate increases, i.e., $\lambda = 0.4$, the induced delay is significantly increasing for each

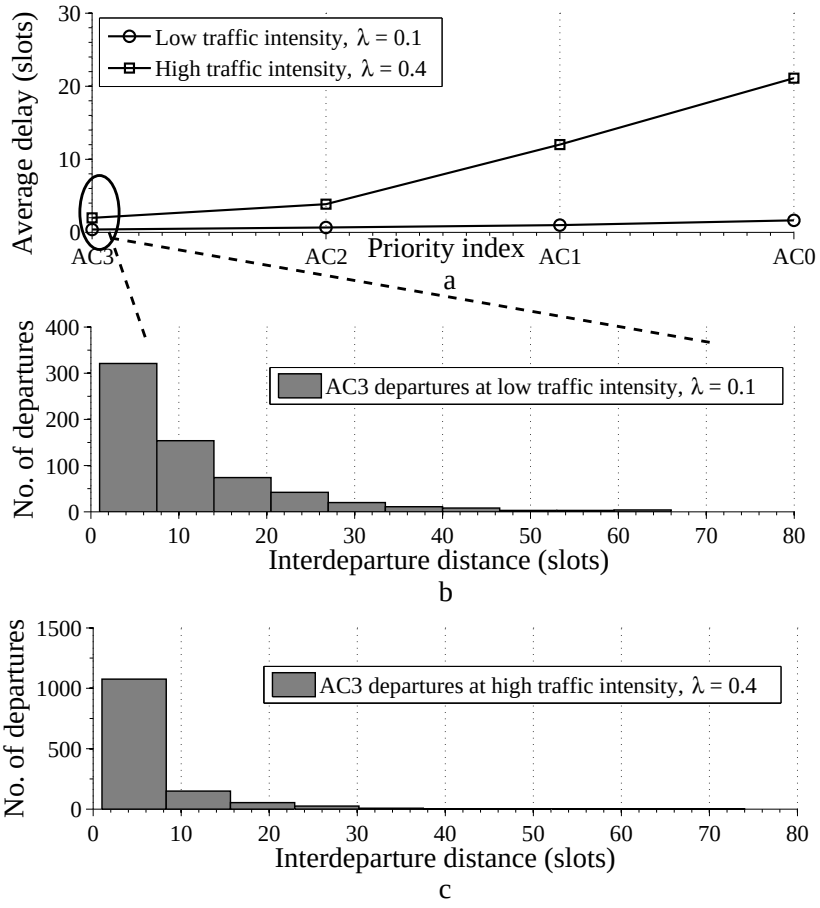


Figure 3.1: Average packet delay and departure distribution
(a) Average packet delay of different priority classes
(b) AC_3 departures distribution at low traffic intensity
(c) AC_3 departures distribution at high traffic intensity

access category. The detailed Subfigures (b) and (c), show the clear impact of traffic intensity on the related interdepauture process for the high priority category AC_3. While Subfigure (b) exhibits an exponential distribution at low traffic rate, the interdepauture distribution seems to deviate further from the exponential distribution at high rate in Subfigure (c). From the latter subfigure, it is interesting to note how the departures tend to group together at small range. This accumulation indicates the existence of burstiness as well as strong memory in the induced output process.

In such scenarios mentioned above and owing to the burstiness and mem-

ory characteristics of IEEE 802.11p output process, the memoryless Poisson model is not suitable for the description of IEEE 802.11p-based DSRC output traffic. In order to resolve the multi-hop issue in V2X interworking and consequently to allow large-scale operability, an accurate model for description of IEEE 802.11p output process should be developed that is able to capture the deviations in the output process under different traffic intensity.

3.1.2 Main Contribution

In Chapter 2, we developed User model based on a systematic method to find the delay characteristics of IEEE 802.11p-based DSRC MAC protocol. The obtained results from this method establish the main block for our motivations in this chapter as already detailed in the previous subsection. In this chapter we extend our systematic user method to incorporate more design parameters in IEEE 802.11p MAC protocol in order to define the interdeparture distance which constitutes the output process of IEEE 802.11p. In this chapter we present stochastic Regenerative model to provide a complete description of IEEE 802.11p-based DSRC output process, leading to traffic flow optimization in the future V2X communications. To our best knowledge available, there is no work that provides a complete model for the output process of IEEE 802.11p and its description. Due to its regenerative property, the model incorporates several design parameters including, MAC contention window size, packet generation rate and the service rate, so that important insights can be gained about IEEE 802.11p configuration and its functionality to support efficient V2X communications. Furthermore, As compared to the widely adopted Poisson model, the proposed model ability to capture the deviations of the actual output process of IEEE 802.11p when employed under different traffic intensity is superior to that of Poisson model.

The rest of this chapter is structured as follows: In Section 3.2, a review of V2X hybrid architectures and discussion on a selection of related works are given. In Section 3.3, the proposed Regenerative model is detailed. The performance evaluation of the proposed model is offered in Section 3.4. In Section 3.5, complete description models for the output process are defined. In Section 3.6, the Regenerative model is incorporated in the enhancement

of V2X cellular-DSRC interworking. Finally, the chapter is concluded in Section 3.7.

3.2 V2X Hybrid Interworking and Related Works

3.2.1 V2X Hybrid Architectures

As an important first step toward the future V2X deployment, Hierarchical and Flat hybrid architectures have been proposed for V2X communications. In the Hierarchical architecture, the type of mobile nodes belonging to each level of the hierarchy is arranged in a fixed or homogeneous hierarchy. In the fixed hierarchical architecture, the mobile nodes belonging to each level of the hierarchy are preselected and do not change with time. For example, public vehicles, such as buses and taxis, may belong to a certain hierarchical level, whereas the private vehicles may be assigned to a lower level in the hierarchy [54]. In contrast, the network nodes in the dynamic hierarchy architecture are not defined based on their type and are assumed homogeneous which provide more flexibility and robustness to the network dynamics as compared to the fixed architecture [55, 56]. Apart from the Hierarchical architecture, in the Flat architecture, the choice of which technology to employ for V2X communications does not depend on the type of the nodes, but it is based on the type of transmitted data or on certain performance QoS metrics like network data load, or network coverage capability. For instance, the transmission of control messages may be restricted to the cellular networks, while the forwarding of data traffic is achieved using DSRC [57, 58]. A detailed classification of V2X hybrid architectures presented here is given in [16].

More broadly, some ITS projects involving governments, car manufacturers and cellular networks providers have even gone further by creating and promoting V2X solutions to provide open and collaborative architectures for V2X communication. During 2012 to 2015, the CONVERGE project in Europe has defined the organizational and technical foundations of an open and collaborative architecture for V2X communication aiming to provide service

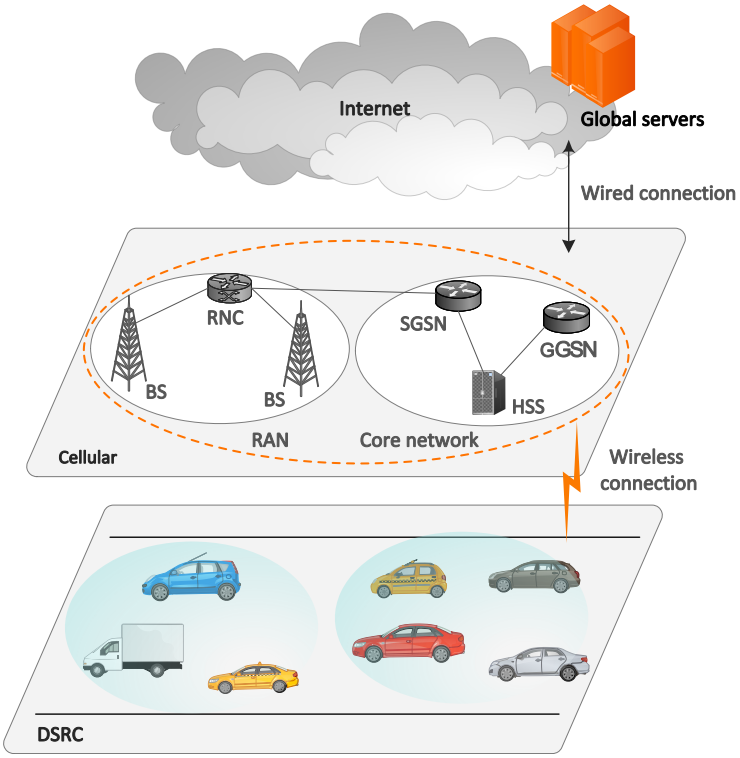


Figure 3.2: DSRC-cellular hybrid architecture

diversity following the example of the Internet [59]. In 2015, the Department of Transportation (DOT) in U.S has announced that it is investing up to $42 million in new V2X projects in three U.S. cities. New York City is installing the DSRC technology in up to 10000 public vehicles, while some traffic signals in both Manhattan and Brooklyn are equipped with DSRC technology along with a number of RSUs on major highways in these cites [60].

As previously mentioned, dynamic hierarchy architecture enables robustness and flexibility to the network variations which make it well suited for large-scale networks. Hence, in this chapter we adopt the dynamic architecture where we implement the proposed Regenerative model for performance enhancement of V2X DSRC-cellular hybrid interworking in a dynamic hierarchy scheme, as illustrated in Figure 3.2. One way to implement the dynamic architecture is by a clustering scheme, which groups vehicles into group of clusters. Each cluster has a Cluster Head (CH) that is responsible for maintaining the cluster and managing its resources. The other vehicles are called

Cluster Members (CMs) which communicate with their CHs by using IEEE 802.11p. The CHs then aggregate the data collected from their CMs and transmit it to the static nodes in the network, i.e., cellular Base stations (BSs) and Road-Side Units (RSUs) [55, 56].

3.2.2 Related Works

This subsection is dedicated to a brief tour of the relevant literature with the goal of relating our work in this chapter to the field. We aim to enable large-scale V2X deployment through providing efficient and adequate interworking scheme. In particular, we focus on the problem of defining the interconnected DSRC output traffic process.

Since IEEE 802.11p is the main communication standard which support DSRC communications, many analytical models and corresponding performance evaluations have been proposed in literature, [28], [38, 39] and [61, 62]. The majority of these studies have focused on modeling the induced MAC protocol delay process and improving its throughput, the output process has only been considered in simulation results in terms of the packet reception rate or in departures' probability distribution. In general, modeling the output process of a MAC protocol is a much harder problem since it is intimately interwoven with the dynamical behavior of the algorithmic system of the protocol. Because of this fact, it is not surprising that results concerning the output process of IEEE 802.11p MAC characteristics are limited and obtained only through simulations, which are usually based on special assumptions [63, 64].

Several works have studied the hybrid solutions that exploit the beneficial consequences of integrating DSRC and cellular technologies towards an efficient V2X communications. Vinel [9] provided a theoretical framework which compares the basic patterns of IEEE 802.11p standard and the cellular Long Term Evolution (LTE) technologies in the context of Safety-of-life vehicular scenarios. The authors of [57] showed that broadcast, multicast modes can reduce the load on cellular downlink, while the uplink channel becomes a bottleneck in dense vehicular scenarios since the uplink transmissions are always achieved using unicast mode. In [65], the authors used a Markovian

model to evaluate the cellular LTE for safety services, where the data service user arrivals at the uplink was modeled to be Poissonian. In summary, the accurate performance evaluation of V2X communication solutions need to account for the actual DSRC output traffic, which is generally ignored in existing studies.

3.3 Regenerative Model

In this section, we develop Regenerative model to compute the output traffic interdeparture distribution of IEEE 802.11p MAC protocol. Particularly, we find analytically the steady-state distribution of the distance between two consecutive successful transmissions. We consider a vehicular network with independent and identical (i.i.d) users. Time will be measured in slot units. The integer T will denote slot indexes, slot T occupies the transmission interval $(T, T+1)$. In slot T each user possesses the following attributes:

- The user generates a number N_T of packets. The random variables N_T are i.i.d with distribution

$$P(N_T = m) = P_m, \quad N_T \sim P_m(\eta_m, \sigma_m^2) \tag{3.1}$$

  where η_m and σ_m^2 are the finite mean and variance of the distribution respectively.

- Once a packet is generated the user will retain it in an infinite size buffer.

- As m increases, P_m converges to Poisson with rate λ packets per slot.

Our methodology in developing the proposed model utilizes the regenerative character of the output process $\{\beta_i\}_{i\geq 1}$ that IEEE 802.11p MAC protocol generates. By observing the contention resolution algorithmic system of IEEE 802.11p MAC as described in Chapter 2 Section 2.3, it is relatively easy to identify the regeneration points at which the output process probabilistically restarts itself. If $\{R_i\}_{i\geq 1}$ represents a sequence of successive collision resolution time points on the most ending edges of slots containing successful

transmissions and at which the lag equals one, then $\{R_i\}_{i\geq 1}$ is the sequence of the regeneration time points associated with output process $\{\beta_i\}_{i\geq 1}$. An important quantity in analyzing the proposed model is the Contention Resolution Interval (CRI) length. As previously described in Chapter 2, IEEE 802.11 MAC protocol utilizes a backoff value which is chosen randomly from a Contention Window (CW). The CW values in Table 2.1 are defined so that $CW \leq$ the actual CRI length. As it will become clear later, the CRI length L_m is determined by the number of collided packets in its first slot. The regenerative property of the induced output process leads to the following lemma

lemma 3. *If $d(n), n \geq 1$ is a discrete time process representing the distance between two consecutive successful transmissions in the output process $\{\beta_i\}_{i\geq 1}$ of IEEE 802.11p MAC algorithm, then there exist a random variable $d(\infty)$ such that the process $d(n), n \geq 1$ converges in distribution to $d(\infty)$. Given a sample function $\mathbb{1}_{\mathbb{n}}(r)$ of the process $d(n)$, then $d(\infty)$ represents the steady-state interdeparture distance induced by the algorithm and its distribution satisfies the equality*

$$P(d(\infty) = r) = \frac{1}{\lambda L_m} E\left\{\sum_{n=1}^{\tau_1} \mathbb{1}_{\mathbb{n}}(r)\right\}$$

Proof. Let the algorithmic system of IEEE 802.11p starts at time T_0 and define the sequence $\{R_i\}_{i\geq 1}$ such that $T_0 \leq R_1 \leq R_2 \leq \ldots$ to be the collision resolution time points on the most ending edges of slots containing successful transmissions and at which the lag equals one. Let $S_i, i \geq 1$ to be the number of successful transmissions in the interval $(T_0, R]$, $\forall R \in \{R_i\}_{i\geq 1}$ then

$$S_i = \sum_i 1(R_i \leq R) \quad \forall R \in \{R_i\}_{i\geq 1}; i \geq 1 \tag{3.2}$$

S_i is a renewal counting process where the inter-renewal times ζ_j^i, $1 \leq j < i$ are identically distributed random variables (i.i.d). If $d(n)$ denotes the distance between the $(n-1)$-th and the n-th successful transmission, then for the process $\{S_i, d_i(n)\}$ with inter-renewal times ζ_i^j the following regenerative

theorem holds [47]

For the process $\{S_i, d_i(n)\}, \quad i \geq 1, n \geq 1$ with iner-renewal times $\zeta_j^i, \quad 1 \leq j < i$, its sample path τ_j in the time interval $(R_j, R_{j+1}]$ is described by:

$$\tau_j = \left(\zeta_j^i, d_j(n) \colon 1 \leq j < i, n \geq 1\right) \tag{3.3}$$

This τ_j is the j-th segment of the process which represents the number of successful transmissions in the interval $(R_i, R_{i+1}]$. Expression (3.3) states that, the process $d_i(n)$ is regenerative with respect to S_i. Hence the process $d(n)$ is regenerative over all the renewable points $\{R_i\}_{i\geq 1}$ as its segments $\tau_i, i \geq 1$ have lengths l_i that are i.i.d. Giving that the sequence $\{\tau_i, i \geq 1\}$ is i.i.d, then

$$E\left\{l_i\right\} = E\left\{l_1\right\} = l \tag{3.4}$$

$$E\{\tau_i\} = E\{\tau_1\} = \Gamma \tag{3.5}$$

Where l and Γ are the mean segment length and throughput respectively. If the mean segment throughput is bounded, i.e.,

$$\Gamma < \infty \tag{3.6}$$

then from the renewal theory the following theorem holds [47]

For the discrete time process $d(n), n \geq 1$ which is regenerative with respect to $S_i, i \geq 1$ with τ_i as the i-th regeneration segment. If its sample function $\{f(d(n), n \geq 1)\}$ is a measurable nonnegative real-valued function then the function $\{f(d(n), n \geq 1)\}$ is also regenerative over all $\{R_i\}_{i\geq 1}$.

Define F to be the expected value of the sample function $\{f(d(n), n \geq 1)\}$ in the first segment τ_1 such that

$$F = E\left\{\sum_{n=1}^{\tau_1} f\big(d(n)\big)\right\} < \infty \tag{3.7}$$

then, by invoking the law of large numbers the first equality in the following

expression holds with probability one.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\Big\{f\big(d(n)\big)\Big\}=\lim_{N\to\infty}\frac{1}{N}E\left\{\sum_{n=1}^{N}\Big\{f\big(d(n)\big)\Big\}\right\}=\frac{1}{\Gamma}E\sum_{n=1}^{\tau_1}\Big\{f\big(d(n)\big)\Big\} \tag{3.8}$$

The expression in (3.8) shows how to establish the existence of the stationary distribution of the interdeparture process $d(n)$ by appropriately selecting the function f. Let us define $f\left(d(n)\right)$ as the indicator function $\mathbb{1}_{\mathbb{n}}(r)$

$$\mathbb{1}_{\mathbb{n}}(r)=\begin{cases}1, & \text{if } d(n)\leq r\\ 0, & \text{if } d(n)>r\end{cases} \tag{3.9}$$

This choice for the function $\mathbb{1}_{\mathbb{n}}(r)$ will permit the computation of the empirical distribution of $d(n)$, to see this let us rewrite (3.8) using (4.6)

$$\lim_{N\to\infty}\frac{1}{N}E\left\{\sum_{n=1}^{N}\Big\{\mathbb{1}_{\mathbb{n}}(r)\Big\}\right\}=\frac{1}{\Gamma}E\sum_{n=1}^{\tau_1}\Big\{\mathbb{1}_{\mathbb{n}}(r)\Big\} \tag{3.10}$$

At any fixed value of r, the expectation of the empirical distribution in (3.10) equals the cumulative distribution, which implies the existence of a real valued random variable $d(\infty)$ such that the sequence $d(n)$ converges in distribution to $d(\infty)$. Then, $d(\infty)$ is the steady-state of the interdeparture distance of the output process $\{\beta_i\}_{i\geq 1}$ with distribution defined as follows:

$$P(d(\infty)=r)=\frac{1}{\Gamma}E\left\{\sum_{n=1}^{\tau_1}\mathbb{1}_{\mathbb{n}}(r)\right\}=\frac{F}{\Gamma} \tag{3.11}$$

Thus, under the conditions stated in (3.6) and (3.7), the steady state distribution of the interdeparture process exist and its value is given in terms of the per segment parameters; the mean cumulative distance F and mean segment throughput Γ.

3.4 Numerical Evaluation

In this section we exploit the dynamics of the IEEE 802.11p contention resolution algorithmic system to evaluate the quantities F and Γ in (3.11).

3.4.1 Mean Segment Throughput

The computation of the mean segment throughput Γ in (3.11) depends on the input traffic rate λ; $\Gamma = \lambda l$, where l is the expected value of segment length as defined in (3.4). Since the multiplicity of successive segments are i.i.d random variables, the expected segment length l is approximating L_m for sufficiently large m. L_m is the expected value of the CRI length given that it starts with multiplicity of m packets in the first slot, then

$$\Gamma = \lambda L_m \tag{3.12}$$

A proof of the last assertion is given in Appendix A. In the following we compute the expected value of the CRI length.

Expected Value of CRI Length

Let T corresponds to a starting slot of some CRI. Let $L_{m|n}$ to be the expected length of the CRI conditioned on having n users with counter value 0. Then, from description of the algorithm the following equations hold

$$L_m = 1 \quad \text{for } m = 0, m = 1 \tag{3.13}$$

$$L_{m|n} = \begin{cases} 1 + L_n + L_{m-n} & \text{for } \ 1 \leq n \leq m \quad \text{(3.14a)} \\ 1 + L_m & \text{for } n = 0 \quad \text{(3.14b)} \end{cases}$$

Expressions (3.14a) and 3.14b can be explained as follows:

- For $m \geq 2$, there is a collision in the first slot of the CRI, the 1 corresponds to the slot of the initial collision among the m users. Then the CRI could be regarded as a partition of two subsets. The first subset is the expected number of slots needed to resolve the collision in slot 2

among n users whose backoff timers decreased to zero. The probability that exactly n users will transmit in slot 2 after the collision slot is

$$P_n = \binom{m}{n} 2^{-m} \tag{3.15}$$

- The second subset is formed by the multiplicity of $(m-n)$ holding users whose backoff timers retained them from transmitting in slot 2, which will be initiated after the end of the previous subset.
- Expression (3.14b) results when none of the users in the initial collision has counter value 0, which occurs with probability P_0.

Since

$$L_m = \sum_{n=0}^{m} L_{m|n} P_n \tag{3.16}$$

then, from (3.14a) and (3.14b) we obtain the finite dimensional linear system

$$L_m = 1 + \sum_{n=0}^{m} \left(L_n + L_{m-n}\right) P_n - P_0 \tag{3.17}$$

Solving for L_m we obtain the following recursion with initial conditions given by (3.13).

$$L_m = \frac{1 + 2\sum_{n=0}^{m} L_n P_n - P_0}{1 - (2)^{1-m}}, \quad m \geq 2 \tag{3.18}$$

Table 3.1 contains some of the computed values of L_m along with the corresponding service rate m/L_m.

Table 3.1: Expected CRI length and the service rate given m packets in the first slot

m	0	1	2	3	4	5	6	7
L_m	1	1	4.5	7	9.6	12.3	15	17.6
m/L_m	0	1	0.44	0.428	0.416	0.406	0.4	0.397

Bounds on CRI Length

The computation of the quantity Γ in (3.12) requires that L_m to be finite for $m \geq 0$ and, moreover, it should be bounded. Our approach to determine bounds on L_m is based on the observation of the coarse dependence of L_m on m as induced by (3.18). This observation allows us to assume that $m = 2m$ is very large, reformulating (3.14a) using this assumption gives

$$L_{2m} \approx 1 + 2L_m, \quad m >> 1 \tag{3.19}$$

Considering as an equality, (3.19) is a recursion whose solution is

$$L_m = \varepsilon m - 1, \quad m >> 1 \tag{3.20}$$

Since we assume that m is very large, the desired upper bound for L_m should guarantee a strictly positive service rate (m/L_m). If $(m/L_m) > 0$, then for every arrival rate that is smaller than (m/L_m), the algorithmic system is stable.

Hence the desired upper bound for L_m should be of the form

$$L_m \leq \varepsilon_k m - 1, \quad m >> 1 \tag{3.21}$$

for an arbitrary positive integer k such that $\varepsilon_k > 0$.

Table 3.1 shows that: $L_m - L_{m-1} \approx 2.7$ for $m \geq 3$. This indicates that the constant ε_k in (3.21) is about 2.7. In Appendix B we proof that $L_m \leq 2.7m - 1$ can be optimized for best ε_k value, so that

$$L_m \leq 2.68m - 1 \tag{3.22}$$

is tightly accurate for $m \geq 3$.
We note that the obtained value in (3.22) is closer to one obtained with the Aloha-based binary protocol, this is true since IEEE 802.11p is a modified version of IEEE 802.11a which is Aloha-based random access scheme as previously discussed in the beginning of Chapter 2.

Up to this point, the conditional expected value of the CRI length given that it starts with multiplicity of m packets, L_m, and its bounds have been calculated. The latter obtained values will be used to compute the mean segment throughput in (3.12). The objective is to evaluate the interdparture distribution in (3.11). As a last step before this evaluation, we calculate the quantity F, namely the mean cumulative interdparture distance over a segment

3.4.2 Mean Cumulative Distance Over a Segment

In order to evaluate the mean cumulative interdeparture distance F, we need to compute the value of τ_1, i.e., the number of packets that are successfully transmitted in the first segment. To that end, we first notice that the algorithm induces a sequence of consecutive CRIs. If L_i denotes the length of the i-th CRI, then from (3.18) the sequence $\{L_i\}_{1\leq i<\infty}$ forms a Markov chain. The limiting distribution of the interdeparture distance in (3.11) fails to exist when this chain is periodic, hence for the chain to be aperiodic, the first segment should be in the first partition of the first CRI. To see this let use define the following quantities:

L_d: is the conditional expectation of the next CRI length, giving the length of the previous one equals d

$$L_d \triangleq E\left\{L_{i+1} \mid L_i = d\right\} \tag{3.23}$$

$P(m \mid d)$: is the probability that the number of packets (arrivals) at the beginning of the $(i+1)$-th CRI is m given that the length of previous one is d.
If the total number of the generated packets in the system is M and the packet generating process as this in (3.1) then

$$P(m \mid d) = \binom{M}{m}(1-P_1)^{(M-m)d}(P_1)^{md} \tag{3.24}$$

where P_1 is the probability of having single arrival in a slot time. Thus, the conditional expectation in (3.23) can be expressed as

$$L_d = \sum_{m=0}^{M} E\left\{L_{i+1} \mid L_i = d, m \text{ arrivals at the start of } L_{i+1}\right\} P(m \mid d) \quad (3.25)$$

Since

$$E\left\{L_{i+1} \mid L_i = d, m \text{ arrivals at the start of } L_{i+1}\right\} = L_m \quad (3.26)$$

then the expression in (3.25) transforms to

$$L_d = \sum_{m=0}^{M} L_m P(m \mid d) \quad (3.27)$$

where L_m is the expected CRI length given m packets in its first slot as defined in (3.18).

For the Markov chain $\{L_i\}_{1 \leq i < \infty}$ to be aperiodic, P_1 in (3.24) should be such that $P_1 > 0$ which implies that τ_1 should lay on the first partition of L_1. The chain can also be irreducible and hence ergodic by an appropriate selection of its state space as follows:

1. If $M < \infty$ and the input rate $m\eta_m < 1$, then necessarily $P_1 > 0$ and the chain is also irreducible and ergodic. Hence the system is stable.

2. If $M \to \infty$ and the quantities η_m, σ_m^2 become infinitely small so that $P(m \mid d)$ converges in distribution to Poisson such that

$$L_d = \sum_{m=0}^{\infty} L_m \left(\lambda d\right)^m \frac{e^{-\lambda d}}{m!} \quad (3.28)$$

   then, as we discussed in Section 3.4.1, the system is stable if and only if the Poisson input rate is such that $\lambda < m/L_m$. That is for small Poisson rates, $P_1 > 0$ and the chain is ergodic. As the Poisson input rate increases, the Poisson theorem states that $P_1 \to 0$ as $M \to \infty$. Then, the ergodicity of Markov chain is not valid and the system becomes unstable.

In each cases, in finite or infinite state space above, whenever $P_1 > 0$ the

first successful transmissions in τ_1 guarantee the ergodicity of the Markov chain and consequently the existence of the steady state distribution of the interdeparture process.

From (3.22) we can see the linear growth of the CRI mean L_m with m. However its variance can also be proven (by analogous procedure to this we used to L_m) to grow linearly with the number of collision multiplicity m, hence by Markov's inequality, the i-th CRI length L_i will be close to its mean L_m with high probability for a sufficiently large m. As a result, the following simple and clear bound on τ_1 arises

$$1 \leq \tau_1 < S_n \tag{3.29}$$

where S_n is the expected number of packets that are successfully transmitted in first partition of the CRI.

To compute S_n we must compute the rate of successful transmissions during the CRI. To that end, let S_m be the expected number of packets that are successfully transmitted during CRI given that it started with m packets and let $S_{m|n}$ be the expected number of packets that are successfully transmitted during the CRI conditioned on having n packets in the first partition. Then, the operation of the algorithm yields the following relations for $S_{m|n}$:

$$S_{m|n} = \begin{cases} S_m & n = 0 \\ 1 + S_{m-1} & n = 1 \\ S_n & 2 \leq n \leq m \end{cases} \tag{3.30}$$

Denoting, as in (3.15), by P_n the probability that n arrivals occurred in an interval of length L_n, we have

$$S_m = \sum_{n=0}^{m} S_{m|n} P_n \tag{3.31}$$

Based on (3.30) and (3.31), we can write a recursion for S_m with initial values

$S_0 = 0, S_1 = 1$ as follows

$$S_m = \frac{(1 + S_{m-1})P_1 + \sum_{n=2}^{m-1} P_n S_n}{1 - P_0 - P_m}, \qquad m \geq 2 \tag{3.32}$$

3.4.3 Model Validation

In this subsection, we validate the proposed analytical model by simulation experiment. In order to verify the coarse dependence of the output process on the traffic intensity λ as induced by (3.12). We report in Table 3.2 the analytically computed upper bounds P_r on the distribution $P(d(\infty) = r)$ when the packet generation process is Poisson with rates $\lambda = 0.1, 0.3$ and 0.4.

Table 3.2: Upper bounds on the interdeparture distribution

	$\lambda = 0.1$	$\lambda = 0.3$	$\lambda = 0.4$
r	P_r	P_r	P_r
1	0.1443	0.2749	0.3781
2	0.0928	0.2268	0.2189
3	0.0825	0.1478	0.1517
4	0.0801	0.1065	0.0995
5	0.0722	0.0653	0.0522
6	0.0695	0.0378	0.0299
7	0.0619	0.0344	0.0274
8	0.0515	0.0275	0.0149
9	0.0513	0.0241	0.0075
10	0.0318	0.0240	0.0075
11	0.0309	0.0069	0.0050
12	0.0206	0.0068	0.0025

Since many traffic safety applications rely on the Beaconing mechanism, in which vehicles periodically broadcasting messages containing their current state (e.g., position, speed), we have developed a simulator in Matlab where each CM vehicle in the dynamic clustering scheme of Section 3.2 sends position Beaconing messages to its CH. This allows the CH to update and manage its cluster. The Beaconing messages generated according to Poisson process with different rates (0.1, 0.3, 0.4) which are within the required Beaconing generation rate specified in [66]. At the receiver CH, we observe the transmitted messages and we compute the interdeparture distance as the difference between two consecutive successful transmissions. We used the AC_3 parameters as defined in Table 2.1 to contend the messages for the CCH channel.

The obtained results from Table 3.2 and the simulation are graphically reported in Figure 3.3. From this figure we notice the following:

1. When the input rate is small, i.e., $\lambda = 0.1$, the interdeparture distance is approximately Geometrically distributed with $P_r \approx P(1-P)^{(r-1)}$ where $P \approx \lambda e^{(-\lambda)}$.

2. As λ gets larger, the interdeparure distribution tends to accumulate at relatively small values. For $\lambda = 0.3$ and $\lambda = 0.4$ we have $\sum_{r=1}^{12} P_r = 1$, which makes the output distribution in this case deviates further from the distribution in 1.

The above results demonstrate the ability of the proposed Regenerative model to capture the deviations of the output process of IEEE 802.11p under different traffic intensity. A complete description of this process is essential in analyzing V2X interconnected systems as we will see later. Hence, the computation of the steady state interdeparture distance in Section 3.3 together with these results will be used to build description models for the actual output process of IEEE 802.11p. A procedure for the calculation of the parameters of the description models under different traffic scenarios is detailed in the following section.

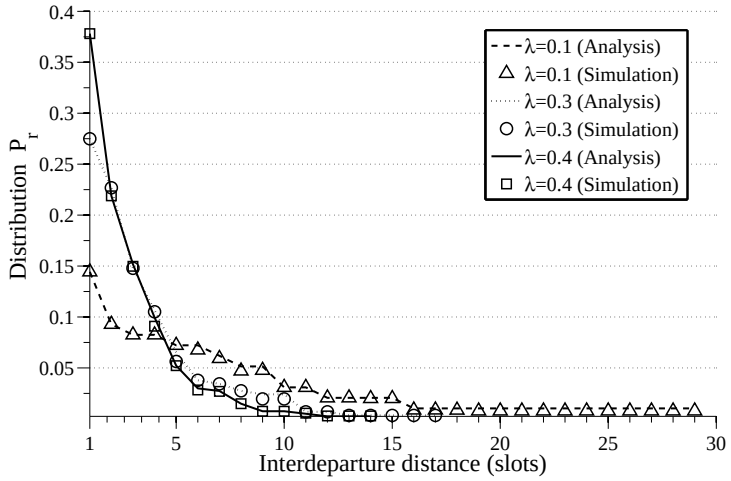


Figure 3.3: Interdeparture distribution for different input traffic rates

3.5 Description of the Output Process

Since the Control Channel (CCH) status process is in a direct interaction with the employed IEEE 802.11p (this should be qualitatively clear from the description of the algorithm in Chapter 2), then the evolution of the channel status process determines completely the output process. This implies the following lemma, for which the proof is given in Appendix C.

lemma 4. *Let $\{Ch_i\}_{i\geq 1}$ to be the status process of the shared channel CCH with a set of states $S = \{s_1, s_2, s_3\}$ such that $Ch_i \in S$ and define the output process $\{\beta_i\}_{i\geq 1}$ as a discrete binary process associated with slots of the channel CCH. Then, the output process can be considered as a two state channel status process, that is*

$$\{\beta_i\}_{i\geq 1} = \{Ch_i\}_{i\geq 1} \; : Ch_i \in \{s_1, s_2\} \tag{3.33}$$

Lemma 4 shows that the meaningful procedure for the calculation of the parameters of the description models would be to equate their stochastic parameters to those in the actual output process where certain corresponding events occur.

3.5.1 The Output Process in Low Traffic Scenario

From Figure 3.3 and for small input rates, the output distribution is close to the Bernoulli distribution. hence from Lemma 4 we have

$$\{\beta_i\}_{i\geq 1} \sim \text{Brn} = \begin{cases} P(\beta_i = s_1) = P \\ P(\beta_i = s_2) = 1 - P \end{cases} \tag{3.34}$$

The only parameter of the Bernoulli description model in (3.34) is P which is equal to the probability of a successful packet transmission in the actual output process. The probability of success equals the packet input rate under stable algorithmic operation. Hence, the interdeparture distance distribution is given by

$$P_r = P(1-P)^{(r-1)} \tag{3.35}$$

Remark 2. *An interesting interpretation of expression (3.35) is that approximating $\{\beta_i\}_{i\geq 1}$ by a Bernoulli process leads to the following assumptions regarding the channel status $\{Ch_i\}_{i\geq 1}$: the state of the channel in the slot T is independent from the previous slot $T-1$, this independency conflicts with the contention resolution mechanism in IEEE 802.11p. The intuitive explanation of the latter phenomenon is as follows: In a spares density model each vehicle in the network can occasionally generate safety related packets and compete for the channel to transmit them hence IEEE 802.11p works in a light traffic environment were the packets' collision is rarely happen. Now, given that the employed IEEE 802.11p MAC protocol is the responsible for bringing in the dependencies among the consecutive slots, this implies that Bernoulli is a reasonable description for IEEE 802.11p output process in low traffic scenario.*

This issue of the Bernoulli model parameter will be revisited when we consider the system probabilities in the following subsection.

3.5.2 The Output Process in High Traffic Scenario

Considering the Bernoulli process in 3.35 as a description for the output process in a highly loaded traffic model is intuitively not appealing. In a high traffic scenario, the traffic rate is heavy and bursty, hence IEEE 802.11p introduces strong dependency among the consecutive slots. As a result, we expect the IEEE 802.11p to generate output traffic with memory. In fact, the accumulation in the interdeparture distribution for $\lambda = 0.4$ in Figure 3.3 puts into evidence the memory feature of the actual output process. One way to capture this memory, would be describing the resulting process by a First-Order Markov Process (FOMP) whose parameters related to those of the actual output process. The validity of the Markovian property follows from the underlying regenerative character of the actual output traffic process that the algorithm generates as proven in Lemma 3. Since the actual output process is to be described by FOMP with parameters λ and $\boldsymbol{b}$; λ is the traffic rate and $\boldsymbol{b}$ is traffic burstiness coefficient, then it is suitable to work on the steady state distributions.

From Lemma 4, if $\Pi(s_1), \Pi(s_2)$ are the steady state probabilities of the channel status process $\{Ch_i\}_{i\geq 1}$ in state s_1 and s_2 respectively, then under the stable algorithmic operation, it is evident that $\Pi(s_1) = \lambda$ and $\Pi(s_2) = 1 - \lambda$. The FOMP transition probabilities are given by

$$P(s_1 \mid s_1) = 1 - P(s_2 \mid s_1) \tag{3.36}$$

$$P(s_2 \mid s_2) = 1 - P(s_1 \mid s_2) \tag{3.37}$$

By invoking Bayes' theorem, we have

$$P(s_2 \mid s_1) = \frac{P(s_2, s_1)}{\Pi(s_1)} \tag{3.38}$$

$$P(s_1 \mid s_2) = \frac{P(s_2, s_1)}{\Pi(s_2)} \tag{3.39}$$

The burstiness coefficient $\boldsymbol{b}$ is defined by

$$\boldsymbol{b} = P(s_1, s_1) - P(s_2 \mid s_1) \tag{3.40}$$

In order to evaluate the above transitional probabilities we need to find the joint probability $P(s_2, s_1)$, for this purpose we notice the following:

From the description of the algorithm it is evident that a CRI which is ending with a successful transmission is followed by an idle slot. This gives rise to a joint pair (s_2, s_1) of successive slots in the channel statues process and consequently the joint probability $P(s_2, s_1)$ can be expressed as

$$P(m_{i+1} = 1 \mid m_i = m) = P(s_2, s_1) \tag{3.41}$$

The transitional probability $P(m_{i+1} = 1 \mid m_i = m)$ takes the general form

$$P(m_{i+1} = \acute{m} \mid m_i = m) = \sum_{l=1}^{\infty} P(m_{i+1} = \acute{m} \mid L_i = l) P(L_i = l \mid m_i = m) \tag{3.42}$$

The first term on the right hand side of the equality (3.42) is the conditional probability of the $(i + 1)$-th CRI with multiplicity m_{i+1}, given that the expected length of the i-th CRI is l. The second term is the conditional probability of the i-th CRI.

Given that the data arrival process is a homogeneous Poisson of rate λ, from (3.28) and for $\acute{m} = 1$, (3.42) can be rewritten as

$$P(m_{i+1} = 1 \mid m_i = m) = \sum_{l=1}^{\infty} (\lambda l)\, e^{-\lambda l}\, P(L_i = l \mid m_i = m) \tag{3.43}$$

Because of (3.13), the conditional CRI probability $P(L_i = l \mid m_i = m) = 1$ for $m_i = 0, 1$. From (3.18) and Table 3.1, it can be easily seen that every odd number is a possible value of L_i, hence $P(L_i = l \mid m_i = m)$ could be written as

$$P((2N + 1) \mid m_i = m), m \geq 2 \tag{3.44}$$

Computing (3.44) for $m = 2$ is sufficient for the joint probability pair $P(s_2, s_1)$ that we are interested in. With $m = 2$, we have $P((2N+1) \mid 2) = 2^{-N}, N \geq 1$, hence in view of (3.43) with $m = 2$, the desired joint probability of the actual

resulting output process in (3.41) is given by

$$P(m_{i+1} = 1 \mid m_i = 2) = \sum_{N=1}^{\infty} \lambda(2N+1)e^{-\lambda(2N+1)}2^{-N} = \frac{3}{2}\,\lambda\, e^{-3\lambda} \qquad (3.45)$$

The transitional probabilities of FOMP model is then calculated from (3.38) and (3.39) and since the steady state probabilities are also computed, the description First Order Markov Process (FOMP) output process is completely determined.

Remark 3. *Let* $P_{\acute{m}m} \triangleq P(m_{i+1} = \acute{m} \mid m_i = m)$. *Then,* $P_{10} = \lambda e^{-\lambda}$ *is the parameter of the Bernoulli output process, as previously noted from Figure 3.3. This indicates that for low Poisson rates, Bernoulli distribution is a suitable description for the output traffic of IEEE 802.11p. In the actual output process and for small input rates, single arrivals in two successive slots occur with probability* $P_{10}^2 \approx \lambda^2$ *while the probability to have a collision slot* P_{21} *is then equals to* $\frac{1}{2}\lambda^2 e^{-\lambda} \approx \frac{1}{2}\lambda^2$. *This explains the increase in the interdeparture distance probability* P_r *for* $r = 1$ *above the Bernoulli parameter* P_{10}.

3.5.3 Evaluation of the Description Models

In this subsection, we evaluate the accuracy of the description models using the same simulation scenario of Subsection 3.4.3. Figure 3.4 shows the actual interdepatrure process and the description interdepatrure processes for low and high traffic scenarios. The figure clearly shows how the interdeparture distribution is close to Bernoulli at low input rates, it also shows that the First Order Markov Process FOMP provides a good description for the output process as the input rate increases.

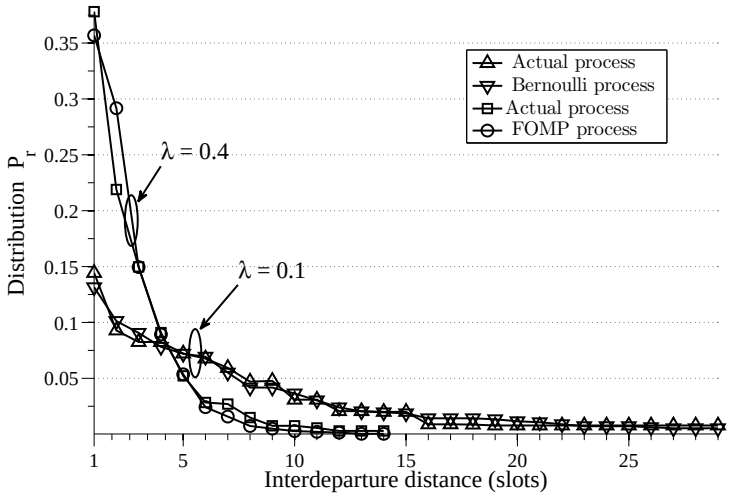


Figure 3.4: Actual, Bernoulli and FOMP at low and high traffic rates

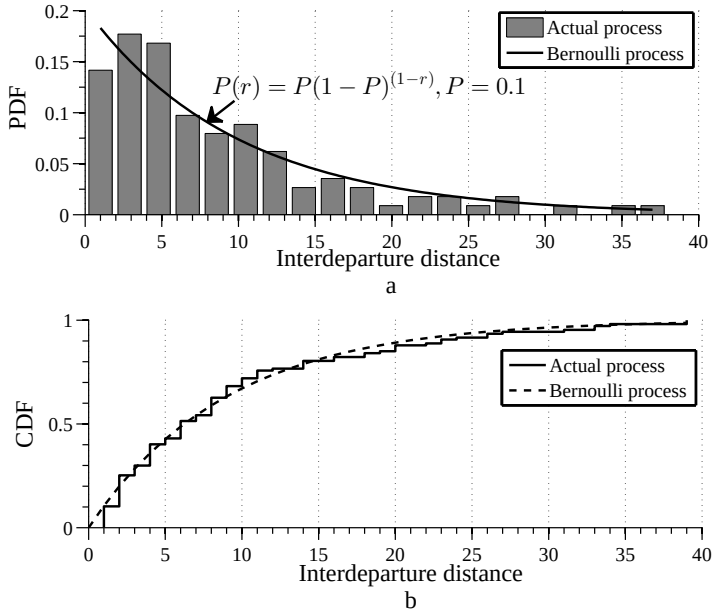


Figure 3.5: Bernoulli interdeparture process vs. actual process
(a) probability density function (PDF)
(b) cumulative distribution function (CDF)

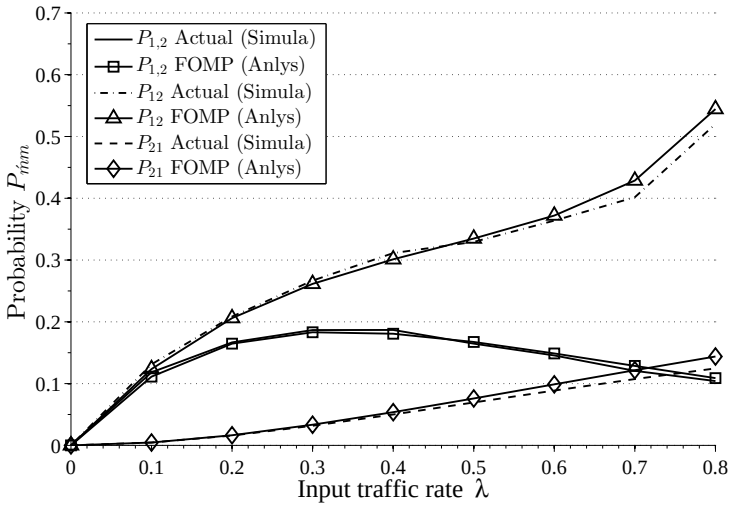


Figure 3.6: System probabilities $P_{\acute{m}m}$ vs. input traffic rate λ

A more detailed examination of Bernoulli description model is depicted in Figure 3.5. The figure shows how the pdf and cdf of the interdeparture distance in Bernoulli process are well fitted to the actual output process. In Figure 3.6, we plot the system transition probabilities $P_{\acute{m}m}$ of the actual process along with those computed analytically from FOMP description process. From the figure we see how the joint probability increases with the input rate, however for rates above 0.4 the joint probability starts to decrease. This is due to the fact that for high rates IEEE 802.11p introduces strong dependency but as the input rate increases above 0.4 the packet rejection rate increases leading to a drop in the joint probability. The latter increase in the rejection rate is due to the increase in the collision probability P_{21} for which the corresponding transition probability P_{12} increases as well with the increasing input rate. Most importantly, however, we can see that there is good agreement between the transition probabilities of First Order Markov Process and the actual system.

3.6 V2X Application Scenario

In this section the output traffic modeling and the corresponding results presented before are incorporated in the performance enhancement of V2X

interworking in the dynamic clustering scheme of Subsection 3.2.1. Particularly we focus on the associated message uplink from CHs to a cellular Base Station (BS) where each input flow to the BS represents an output process from the employed 802.11p in each cluster. The mean uplink delay D is an essential measure of the performance of V2X interworking. In order to derive D a queuing model has been applied to the uplink path of the BS.

More specifically, we consider a queuing traffic model with M cluster flows, λ_j be the j-th cluster output rate in (packets/slot). Since we assume a slotted time system with fixed-length data packets, then the same constant amount of service will be required at the base station which implies that the input (output) processes $\{\beta_i^j\}_{i\geq 1}$, $j = 1, 2, \ldots, M$ are synchronized.

If the interworking is within a small number of clusters, then the employed IEEE 802.11p works in a low traffic scenario. In this case, the output process is Bernoulli process. Thus by using Queuing Theory [67, 68], the average number of packets S_B in the cellular uplink is given by

$$S_B = \frac{\sum_{j=1}^{M} \sum_{k>j}^{M} \lambda_j \lambda_k + \Lambda(1-\Lambda)}{1-\Lambda} \tag{3.46}$$

where

$$\Lambda = \sum_{j=1}^{M} \lambda_j \tag{3.47}$$

From the well known Little theorem, the mean packet delay, D_B is given by

$$D_B = S_B/\Lambda. \tag{3.48}$$

As the number of the clusters increases, the resulted output process from the employed 802.11p is FOMP. The average number of packets S_K in this case is

$$S_K = \Lambda + \frac{\sum_{j=1}^{M} \sum_{k>j}^{M} \lambda_j \lambda_k \left[1 + \frac{\boldsymbol{b}_j}{1-\boldsymbol{b}_j} + \frac{\boldsymbol{b}_k}{1-\boldsymbol{b}_k}\right]}{1-\Lambda} \tag{3.49}$$

where $\boldsymbol{b}$ is the burstiness coefficient as defined in (3.40)

Then, the mean packet delay D_K is given by

$$D_K = S_K/\Lambda. \tag{3.50}$$

The induced mean uplink delay was computed from the expressions 3.48 and 3.50 for $M = 3$ and $M = 5$ respectively. The obtained values are shown in the Figures 3.7 and 3.8 along with the values resulted from simulating the actual queuing system. Figure 3.7 shows that both of the output description models perform well as the queuing problem is not significant when $M = 3$. Even though the delay induced in the Bernoulli model for $\lambda = 0.1$ is relatively high, its performance outperforms Markov as the output rate increases, i.e., $\lambda \geqslant 0.3$. In fact, the Bernoulli model induced delay is more closer to the actual system delay. The observed increase in the Bernoulli delay for $\lambda = 0.1$ is attributed to the fact that the Bernoulli output process has interdeparture probability P_r at $r = 1$ which exceeds its mean parameter P as previously explained in Remark 3.

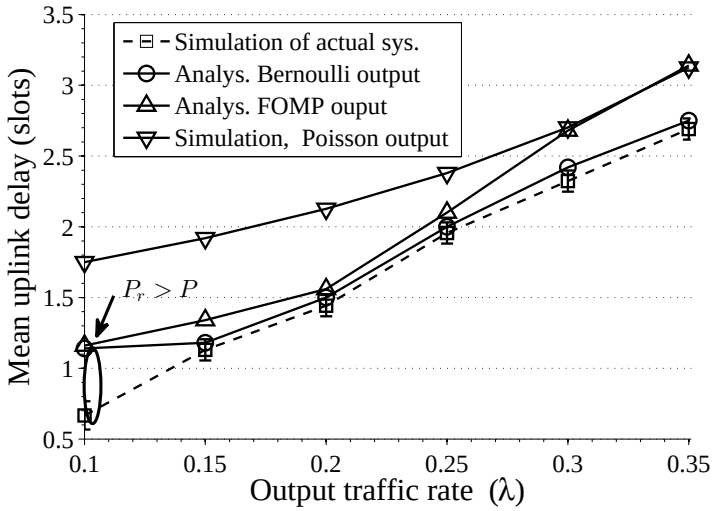


Figure 3.7: Mean uplink delay as a function of the output rate, $M = 3$

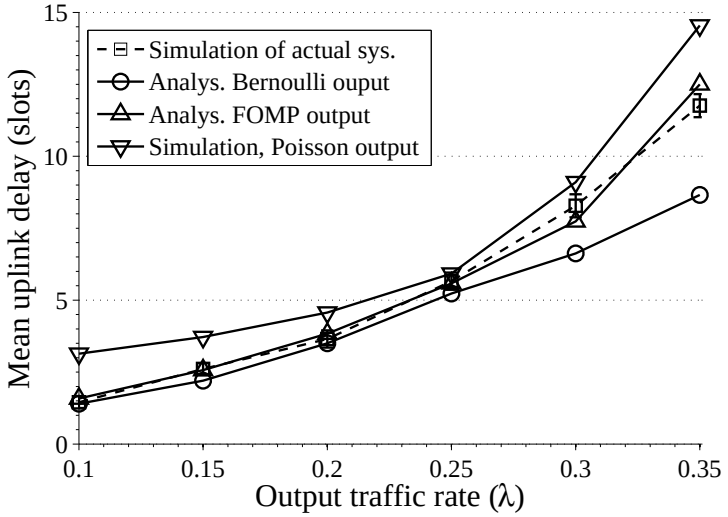


Figure 3.8: Mean uplink delay as a function of the output rate, $M = 5$

As expected for $M = 5$, FOMP performs better than Bernoulli. This is clearly shown in Figure 3.8 as the actual system induced delay is closer to the induced delay under FOMP model since the latter captures some of the dependency introduced by the algorithmic system of IEEE 802.11p. The interworking induced average packet delay is shown in Figure 3.9; it is the average time between the packet generation time and the end of its successful transmission. It is provided here to indicate the total average delay that the packet undergoes in the cluster network and the uplink path. As expected from the previous results the induced total average delay is less when $M = 3$, as compared to $M = 5$.

As we already mentioned in the beginning of this chapter, due to its tractability the Poisson model is generally adopted to model the interconnected network traffic processes. We compared our Regenerative model with the Poisson model in the evaluation of V2X interworking scheme discussed in this section. As clearly shown from the results in Figure 3.7 and 3.8, the performance of the Regenerative model is superior to that of Poisson because the latter fails to capture the real variations in the traffic intensity. Our results show clearly that the adoption of Poisson model results in erroneous packet delay calculations which lead to inaccurate identification of the bottlenecks in V2X interworking.

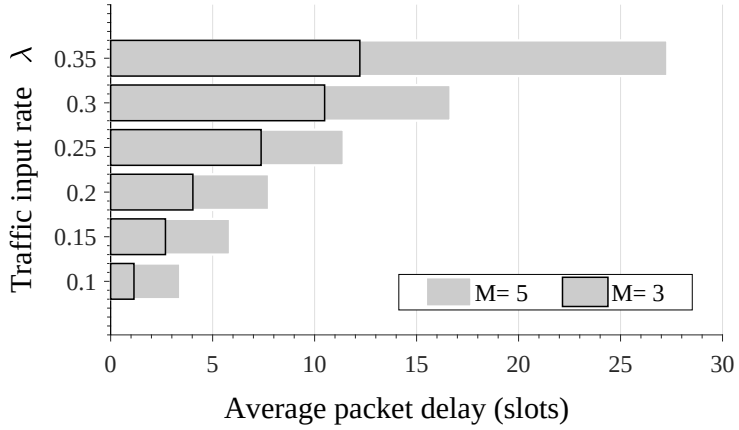


Figure 3.9: The total interworking average packet delay

3.7 Conclusions

Due to their analytical tractability, the memoryless models are widely used in the literature for the description of interworking traffic processes; however, the ability of such models to describe bursty traffic has always been questioned. Owing to burstiness and memory nature of the data traffic in vehicular environment, the adoption of the memoryless models in this case could lead to erroneous identification of the bottlenecks of the interconnected system and to erroneous packet delay calculations which cannot be tolerated especially for real-time safety applications. In the future V2X complex interworking systems, the lack of an accurate description of the output process of IEEE 802.11p-based DSRC communication standard presents the major difficulty in evaluating the interworking performance. This is due to the fact that the output process of IEEE 802.11p is closely attached with the dynamical behavior of the contention resolution mechanism of the MAC protocol which makes results concerning the output process characteristics to be limited and difficult to obtain. Until now, the evaluation of such characteristics has been based only upon simulation studies that do not give precise description of the actual induced output process.

In this chapter, we presented Regenerative model to completely provide an accurate description for IEEE 802.11p output process under different traffic intensities. The motivation behind the proposed model is to capture

the dependencies in the actual output process which are introduced by the contention resolution mechanism of IEEE 802.11p MAC protocol. Besides tractability, another attractive feature of the proposed model is its applicability; since the regenerative property is also encountered in the induced delay process, the model provides important insights about IEEE 802.11p MAC design parameters and its capability to provide efficient V2X communications. The analytical results verified through extensive simulations show the accuracy of the proposed model in describing the actual output process of IEEE 802.11p. Moreover, the proposed model is compared with the memoryless Poisson model in hybrid V2X interworking enhancement and a relevant queuing system has been studied for this purpose. As compared to Poisson model, the Regenerative model ability to capture the deviations of the actual output process of IEEE 802.11p when employed under different traffic intensity is superior to that of Poisson model.

Chapter 4

QoS-based Sequential Detection Algorithm for Jamming Attacks in VANET

The unique characteristics of VANET; high mobility, network topology and its unbounded scalability, make it an eye-catching field for attackers.

4.1 Introduction

Wireless networks make use of shared transmission medium; therefore, they are inherently susceptible to security problems. The intrusion on the transmission medium is easier than for wired networks and it is possible to conduct several malicious attacks. An attacker with a radio transceiver could intercept the transmission, injects spurious packets, and blocks or jams the legitimate transmissions in the network. Being a type of wireless communication networks, Vehicular Ad hoc Networks (VANETs) are vulnerable to all of these attacks. As a key component of V2X technology, supporting V2V and V2I communications, VANET plays an important role in enabling life-critical safety applications, such as cooperative collision warning, intersection collision avoidance and road conditions (e.g., slippery road, work zone area) [19]. Hence, security is the most required feature for VANET since attacking and misusing such network could cause destructive consequences. Besides

the general wireless networks security issues, unique security challenges rises because of the distinct characteristics of VANET which can be summarized as follows:

- High Mobility: The vehicles in VANET are usually moving at high speed. This makes the prediction of vehicle's position and the protection of its privacy harder to achieve.

- High dynamic topology: Due to the high mobility, the position of a vehicle changes frequently. Hence, the possibility of having long-lived communication context in VANET is small; applying securing approaches depending on verifying identities is hard.

- Unbounded scalability: The number of vehicles in VANET is not always known and, more importantly, cannot be restricted. Thus, VANET may contain a huge number of vehicles and it can be implemented for one city, several cities or even for countries. Therefore, applying a robust confidential system which has the ability to distribute cryptographic keys for that large number is unfeasible.

- Frequent and short connection: The ad hoc nature of VANET requires each vehicle to gather real-time information from its neighboring and from the RSUs. This information is included in periodically exchanged packets called Beacons which is at the heart of safety applications in VANET. This requires efficient security techniques that take into consideration the Quality of Service (QoS) requirements and constraints for such vital applications in VANET.

These unique features along with the open wireless nature of communication lead to the most critical and challenging security issues that could severely disrupt the network operation [69–72]. The wireless communication in VANET is based on the DSRC technology which is achieved over reserved radio spectrum band allocated in the upper 5 GHz range. The main enabling communication standard in DSRC is IEEE 802.11p which supports V2V and V2I communications. In IEEE 802.11p MAC protocol, different QoS classes are obtained by prioritizing the data traffic. Therefore, application messages

are categorized into different Access Classes ACs, with AC_0 has the lowest and AC_3 the highest priority, where each AC has different contention parameters to contend its messages for the shared communication channel. Our studies presented in the previous chapters provide evidence about the vulnerability of IEEE 802.11p standard to security threats. In particular, the obtained results from the analysis of IEEE 802.11p MAC protocol reveal that the MAC layer in IEEE 802.11p possesses various vulnerabilities to Denial of Service (DoS) attacks. Such attacks are a vexing problem in all wireless networks, but they are particularly threatening in VANET. Jamming is one of the harshest types of DoS attacks in which the jammer (attacker) can disable the whole network by continuously or selectively jamming important transmissions like ACKs and Beacons. Since VANET is a real-time communication system, consequences of losing ongoing transmissions could be fatal. In Section 4.3 we discuss in detail jamming attacks and how they affect the transmissions in VANET.

4.2 Related Works and Contributions

In this Section, we provide a review of selected related works in the literature followed by the main motivations which lead to the new contributions that this study makes to knowledge beyond the existing literature.

4.2.1 Related Works

In order to detect jamming in conventional wireless networks (e.g., mobile networks, sensor networks) different detection and countermeasure methods have been proposed in the literature. The existing detection methods are mainly based on observing packet/network measures, such as packet delivery ratio (PDR), signal strength (SS) and carrier sensing time (CST) in normal and abnormal (jamming) network conditions. In [73–75] jamming attacks are evaluated at the packet level utilizing packet send/delivery ratio, while the authors of [76] and [77] evaluated the jamming at the network level by establishing lower bounds on the network saturated throughput under arbitrary jamming attacks. However, there are certain drawbacks associated with

the use of such detection methods. More importantly, packet/network level measures do not directly reflect QoS requirements imposed in time-critical applications (e.g., latency constraints). For instance, a high transmission reliability presented in the packet delivery ratio does not necessarily guarantee that the needed latency requirement for the delivery of time-critical messages is satisfied. Hence, these detection methods are not feasible for VANETs in which time-critical applications are of a fundamental importance.

Several attempts have been made to provide countermeasures that can be used to mitigate jamming attacks. Wood *et al.* [78] introduced a detection and mitigation algorithm which maps out the jammed area in a wireless sensor network and routes packets around the affected region. On the other hand, the authors in [79] proposed a multipath routing which requires multiple paths to exist between every network node and base stations assuming that there is at least one non-jammed path between them. An adaptive approach to anti-jamming for sensor networks is proposed by Li *et al.* in [80], the proposed approach combines anti-jamming techniques, which enables each node to adaptively select the optimal anti-jamming technique for different jamming conditions. Different from the conventional wireless networks, vehicular networks have strike characteristics, as previously mentioned, that require adaptation in design whenever we apply detection or mitigation technical solutions from conventional wireless networks to the vehicular environment. For instance, the unbounded scalability of VANET, in particular, makes the possibility of applying the countermeasures techniques unfeasible, especially for large-scale vehicular networks.

Unfortunately, while research on jamming attacks in conventional wireless networks is active and prolific, we have seen very few efforts specifically targeting vehicular networks. Radio Frequency jamming attacks on VANETs were studied experimentally in indoor and outdoor in [81]. Lyamin *et al.* [82] proposed a jamming detection method that can detect a missing of one beacon from a vehicle in a platoon, i.e., group of vehicles. Based on the number of received beacons, the proposed detector divides the vehicles into groups whose beacons only collide to beacons sent from members of the same group. Whenever there is a missing of one beacon in one group, a detection alarm will be raised. A broader perspective to the work of Lyamin *et al.* has

been adopted by Benslimane and Nguyen-Minh in [56] where they proposed a MAC-based detection method for multiple beacon jamming attack. The major disadvantage of Beacon detection method is that the network is only evaluated for one running application, i.e., safety application. In real-time VANETs, the jamming attack would affect not only the safety messages but also other messages generated from various categories of applications as well.

Besides jamming attack detection methods, mitigation techniques trying to avoid jamming attacks have been also proposed for VANETs. In the works of Biswas *et al.* [83] and Sharma *et al.* [84], verification check algorithms have been proposed to detect the malicious node in VANET. In reviewing the literature, we notice that most of the reported jamming detection methods in VANETs focus on a particular jamming attack and consider only one type of applications running in the network. This indicates a need to investigate the effect of different jamming attacks on the network performance when different application messages are exchanged between its nodes. In addition, these studies investigate only the case of communication between two nodes and no medium access contention is considered. Obviously, in order to achieve high detection efficiency, the reference value (i.e., detection threshold) that is used in differentiating a jamming attack and normal network conditions should be accurate. However, this cannot be achieved without the consideration of medium access contention mechanism which is generally overlooked by existing studies.

4.2.2 Motivations and Contributions

While preventing jamming attacks in VANETs is not feasible due to its unbounded scalability, the detection of such attacks is of paramount importance. In this chapter, we deal with IEEE 802.11p MAC vulnerabilities related to jamming attacks and we propose a novel jamming detection algorithm that is able to detect three common types of jammers: Constant, Random and Intelligent jammer [83]. There are two key observations that drive our detection method.

1. The QoS requirements imposed by different access classes ACs and how they are closely attached to the contention mechanism design parame-

ters of IEEE 802.11p MAC. This relation allows us to define detection threshold value that can be used in differentiating a jamming attack from normal network conditions.

2. Vehicles in VANET which are moving in free-flow conditions form interconnected blocks of vehicles where vehicles within the same transmission range are considered to be part of a cluster. The links between vehicles within the same cluster tend to be more stable, this stability supports QoS requirements of the different classes ACs, and consequently the threshold value in (1) can be obtained accurately.

Motivated by the two observations, we propose a QoS-based Sequential Detection Algorithm (QoS-SDA) that can effectively detect jamming attacks, while false detections occur infrequently. Specifically, our main contributions in this work include

1. We develop an optimization methodology for IEEE 802.11p MAC which ties QoS requirements of the application messages in the access classes ACs with the contention mechanism design parameters. Utilizing this methodology, we define IEEE 802.11p MAC *stability region* from which we decide on the detection threshold value.

2. In contrast with the previous studies where the defined detection threshold values do not reflect the QoS requirements imposed in real-time applications. Our QoS-based approach allows us to accurately determine a detection threshold value, which in turn enhances the performance of the proposed detection algorithm in term of the probability of detection.

3. We integrate the sequential detection of change method with the developed optimization methodology and we propose the QoS-based Sequential Detection Algorithm (QoS-SDA).

4. We provide comprehensive analytical and simulation analyses to prove the validity of the develop methodology and the efficiency of the proposed algorithm.

The major objective of this chapter is to present a jamming detection algorithm that is more suitable for vehicular networks while in the same time providing an important opportunity to advance the understanding of IEEE 802.11p MAC protocol and its reconfiguration for enhanced performance. First, in the upcoming section, we investigate the vulnerability of IEEE 802.11p MAC to jamming attacks and describe briefly three common types of jamming attacks in wireless networks. Second, we present the network architecture and the problem formalization in Section 4.4. Then, in Section 4.5 we identify the QoS requirements of application messages for each access class and present our optimization methodology for IEEE 802.11 configuration. Section 4.6, introduces the proposed detection algorithm in its general and special memoryless case, followed by a discussion on the simulation model and the corresponding obtained results. Finally, the chapter is included in Section 4.8.

4.3 Jamming Attacks in VANET

Due to its inherited distributed contention resolution mechanism, the MAC protocol in IEEE 802.11p is more susceptible to jamming attacks. At IEEE 802.11p MAC, a vehicle being jammed will defer its next transmission following a backoff decrease process and after a few successive jams the vehicle would virtually stop transmissions. This is a strong incentive for other malicious attacks like eavesdropping and selfish node attacks which trying to gain an unfair share of the transmission channel without having to reveal their wrongdoings. This context shows the severity of the threats posed by jamming attacks in the vehicular environment, particularly intelligent jamming as we will see in the sequel of this section. In the following we investigate how jamming attacks exploit vulnerabilities of MAC protocol in IEEE 802.11p.

4.3.1 Vulnerability of IEEE 802.11p MAC to Jamming Attacks

IEEE 802.11p uses the Enhanced Distributed Channel Access (EDCA) as Medium Access (MAC) method. The EDCA uses CSMA with collision

avoidance (CSMA/CA) while traffic prioritization is provided by four Access Classes with AC_0 has the lowest priority and AC_3 the highest priority [85]. For each newly generated packet, the vehicle senses the channel activity before it starts the transmission. If the channel is sensed idle for a time period greater than or equal to an arbitration interframe space (AIFS), the packet can be directly transmitted. If the channel is busy or becomes busy during AIFS, the vehicle must wait until its backoff timer decreases to zero to be able to transmit again. If a malicious attacker deliberately transmits interfering random packets during AIFS, the vehicle will sense the channel busy and then starts the backoff process. The Backoff Timer (BT) is chosen randomly from a discrete uniform distribution and drawn from a Contention Window (CW) with values from the interval $(0, CW_{min})$.

Moreover, the MAC protocol of 802.11p is a stop-and-wait protocol and therefore the sender vehicle awaits an acknowledgment (ACK) from the receiver. If no ACK is received due to being deliberately discarded by a malicious attacker, the sender will falsely believe that there exists congestion and then enter a retransmission state. For every retransmission attempt, the BT value will be doubled from its initial value until reaching CW_{max} and the packet who reached the maximum number of attempts will be rejected out of the system. Hence, if the attacker launched successive constant jams, the vehicle being jammed would experience an increased rejection rate due to constantly sensing a busy channel and virtually stop transmissions.

The CSMA/CA procedure in IEEE 802.11p, in unicast and broadcast modes is presented in Figure 4.1. The contention parameters for the control channel (CCH) are previously discussed in Chapter 2 and shown in Table 2.1 in the same chapter. Those parameters are defined to meet different QoS requirements for each access class. While AC_3 and AC_2 have strict QoS requirements, such requirements are loosened for AC_1 and AC_0, as we shall discuss further in Section 4.5. Therefore, we only consider three types of messages in a vehicle which are set priorities with AC_3 for Safety-of-life messages, AC_2 for Safety messages, and we lump both AC_1 and AC_0 into one priority class AC_1 for Non-safety messages.

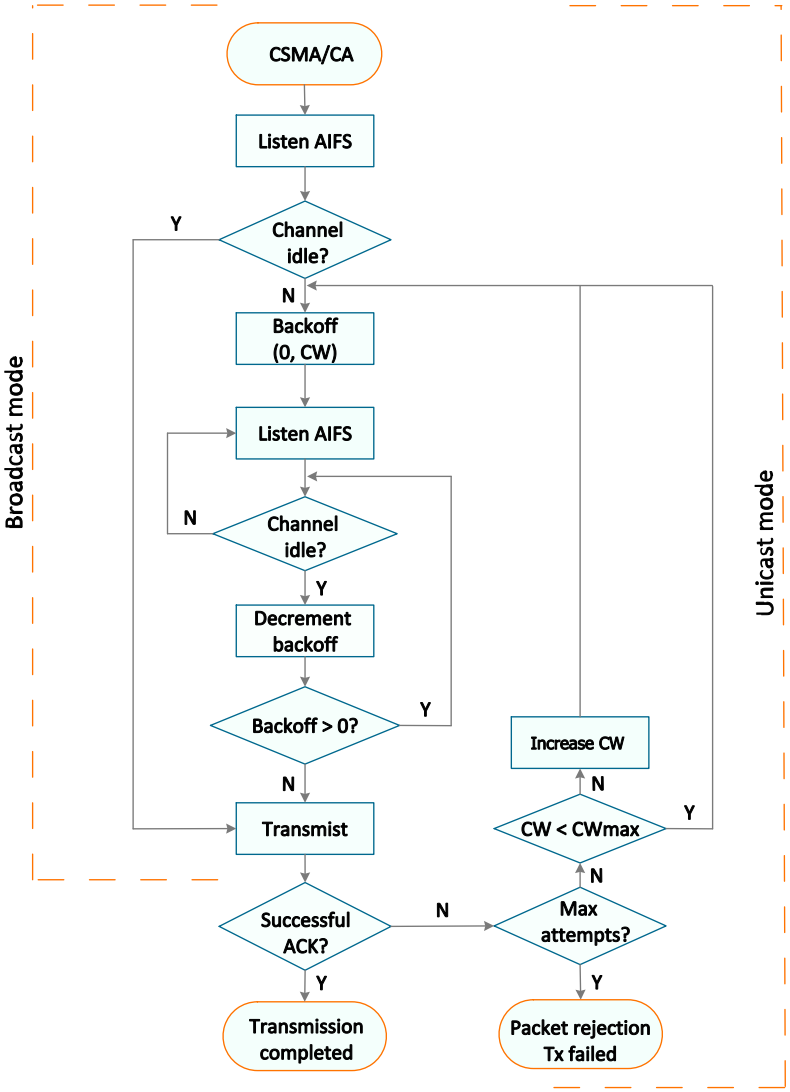


Figure 4.1: CSMA/CA procedure in IEEE 802.11p

4.3.2 Attacker Model

Jamming attacks is one of the most serious DOS attacks in vehicular networks. The specific characteristics of vehicular environment contribute to the scenarios' diversity to perform such attacks. In jamming attacks, the attackers may transmit random messages to jam the channel aiming to reduce the efficiency and performance of the network while being stealthy against

detectors or cause a completely denial of service so that the total network is no longer available to the legitimate users or being protocol aware so that they are less likely to detect. The above mentioned metrics in characterizing jamming attacks lead to the following three common types of jammers in vehicular networks; Constant jammer, Random jammer, and Intelligent jammer [86].

- A Constant jammer continuously transmits random interfering packets to make the communication channel always busy. Whenever a legitimate node attempts to access the channel, it finds the channel busy then enters to backoff process. If the constant jammer launches successive attacks it could lead to a completely denial of service which results in a zero data rate at the receiver side.
- A Random jammer operates according to a random sequence of active (ON) and sleep (OFF) periods. It sleeps regardless of any activity on the network, and during the jam interval, it acts as a constant or intelligent jammer.
- An Intelligent jammer is a protocol-aware jammer that conforms easily to legitimate transmissions. This jammer transmits interfering packets with the knowledge of the MAC protocol, hence it is activated only when it senses activity in the transmission channel which makes it less likely to detect.

4.4 System Model and Problem Formalization

4.4.1 Network Architecture

Due to different vehicular traffic scenarios, i.e., regular, dense or sparse, vehicles in VANETs moving on the same directed pathway form interconnected blocks of vehicles [50]. Additionally, vehicles that are within the same transmission range and maintain V2V connectivity are said to be part of a cluster.

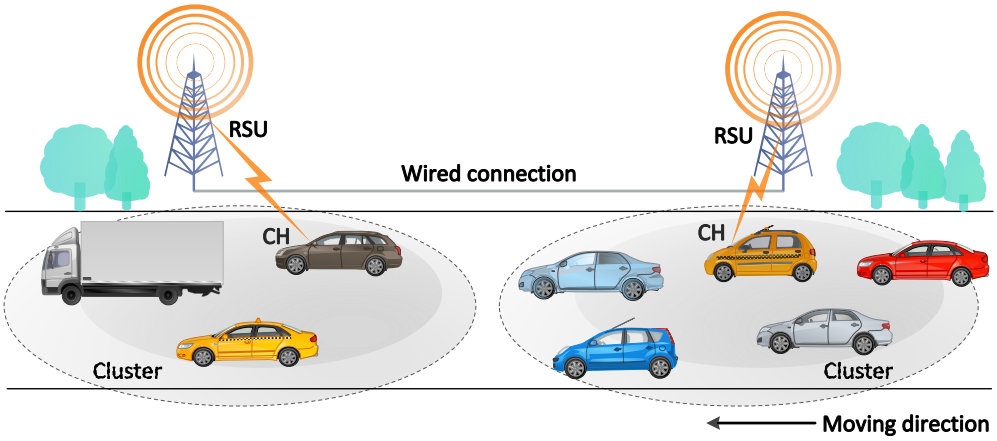


Figure 4.2: Envisioned network architecture

We consider clustered network architecture, as shown in Figure 4.2, the components in the architecture are Cluster Heads (CHs), Cluster Members (CMs) and a V2I backbone network of cluster heads and RSUs. The neighboring vehicles within the transmission range of a CH become a CM and directly communicate with their corresponding CH via IEEE 802.11p. In this scenario, each vehicle is equipped with a positioning device and the local cluster connectivity information is received by CH through periodic Safety messages (Beaconing) carrying information on vehicle position and velocity. On the other hand, the RSUs are connected with each other using wired communication line and periodically send their existence announcement packets to indicate their availability in their service coverage. The CH then aggregates the data from its local CMs and send it to the RUS in its range in periodic time intervals. The RSU is then responsible for disseminating the received data to the other RUSs in the network.

Several VANET research studies in the literature have focused on developing clustering techniques, we choose to adopt a technique that is best suited for the characteristics of our envisioned V2X architecture [87]. Even though the average speeds of vehicles in different paths vary, speeds of vehicles in the same directed path have almost identical mean and variance, moreover as these vehicles move across in the same path, the change in the neighborhood is small. This restriction of mobility to one dimension in a confined path,

almost static neighborhood conditions around a vehicle and in addition to the presence of the RSUs eliminate the effect of mobility and consequently reduce the need for periodic election of cluster heads which makes the links among vehicles within the same cluster to be more stable. Thus, links stability provides us an opportunity to define IEEE 802.11p *stability region* which will be further used to define a threshold value on the per cluster input rate generated by its CMs. To make this fundamental concept concrete, in the following we proceed with a full description of the problem statement.

4.4.2 Problem Formalization

Consider a cluster C comprised of a Cluster Head (CH) and a set S of Cluster Members vehicles (CMs), $S = 1, 2, ..., n$. Then, a number m of RSUs are displaced in the network scenario such that $m < n$. Within the cluster C each CM generates messages for the three traffic classes $AC_i\,, i = 1, 2, 3$, with the actual combination of traffic classes in the corresponding CM depending on the applications running at this CM. Each class AC_i imposes different QoS requirements (e.g., delay and rejection rate constraints) while simultaneously presenting traffic rates λ_i, $i = 1, 2, 3$ which may vary dynamically. These variations in the rates λ_i along with contention resolution mechanism in IEEE 802.11p induce changes in the data rate accessing the corresponding cluster head CH. If the rate accessing the cluster head is λ_{Ci}, then the main problem can be formulated as follows:

- Given the rates λ_i, $i = 1, 2, 3$ and given the statistical descriptions of the traffics, then there exists an upper and lower bounds on the cluster data rate λ_{Ci} such that the QoS requirements for each traffic class AC_i are satisfied. The method for determining these bounds which represent the cluster *stability region* will be discussed in detail in Section 4.5.

- If the changes in the data rate λ_{Ci} are within the cluster *stability region*, then the cluster data rate is maintained; meaning that the QoS requirements of each class are satisfied and the resulted rejection rate is due to normal operation of the contention resolution mechanism (no jamming). Otherwise, the rate λ_{Ci} in no longer maintained and the rejections are highly probable due to a jamming attack.

- To detect the changes in the cluster data rate, a proposed QoS-based Detection Algorithm will be devised that traces consecutive λ_{Ci} changes and declares a jamming attack whenever this change falls outside the predefined bounds interval.

4.5 Optimization Methodology for IEEE 802.11p Configuration

4.5.1 Traffic Classes and Quality of Service Criteria

Obviously, a jamming attack results in an increase in the number of packet collisions observed in the affected cluster and consequently leads to a rejection among the transmitted packets. An important quality measure which differentiates between the rejection under normal operation and the rejection due to jamming in this case is the lower bound on the fraction of the successfully transmitted traffic L_s. The induced rejection rate leads to changes in the traffic rates $\lambda_i, i = 1, 2, 3$ in each cluster. Our target will be to trace those changes in traffic rates and to detect a jamming attack whenever this change falls outside the *stability region* of the per cluster IEEE 802.11p MAC protocol. This *stability region* is obtained via an optimization methodology which relates the traffic rate maintenance, in terms of the satisfaction of the lower bound L_s and the other corresponding QoS, with the contention mechanism design parameters. Below, we identify and state the traffic QoS requirements for each class as taken from [51].

QoS of Safety-of-life Class, AC_3

1. Each generated Safety-of-life message imposes a strict finite upper bound U_d of 100 ms on the transmission delay it may tolerate; that is, if the message does not reach its intended recipient in this time period then the data is less or more useless and the missed upper bound will have more severe consequences on the system performance.

2. Communication range is between 50 and 300 meters. Every Safety-of-

life message must reach any vehicle within this specified range and in less than its specified latency in 1.

3. Each Safety-of-life message should have 99.9% probability of successful transmission for the application to be effective. Hence the lower bound L_s on the successful transmission of each Safety-of-life message should be such that $L_s \geqslant 0.99$, meaning that it tolerates no more than 0.1 probability of rejection, where rejection occurs if one of the previous constraints is violated.

QoS of Safety Class, AC_2

Qualitatively speaking, the QoS requirements per Safety message are parallel to those for Safety-of-life. An upper bound, U_d of 1000 ms on the delay per message along with 99.9% probability of successful transmission apply here as well with a communication range that may extend up to 1000 m.

QoS of Non-safety Class, AC_1

Non-safety messages do not impose specific constraints on transmission delays, while they have shorter communication range (up to 90 m). It is desirable, however, that delays be finite with high transmission reliability.

4.5.2 EDCA Quality of Service Support

As mentioned in Section 4.3, the MAC layer in IEEE 802.11p adopts the Enhanced Distributed Channel Access (EDCA) for QoS support for the traffic classes ACs. This enables each AC with an independent MAC queue that can be differentiated by channel contention parameters including Contention Window (CW) and Arbitration Inter-Frame Space (AIFS) as shown in Table 2.1. The Contention Window (CW) is a basic design parameter that is chosen so that the *stability region* of IEEE 802.11p is maximized while maintaining the QoS requirements of each traffic class even under congestion conditions. This leads to the following lemma for which the proof is in the Appendix D.

lemma 5. *Given a lower bound on the successful transmissions L_s and an upper bound U_d on the transmission delay as defined in QoS requirements*

of IEEE 802.11p-based DSRC, the Contention Window size (CW) should be determined from the following constrained optimization problem: Find the CW value such that the input rate λ is maximized while the fraction of the successfully transmitted traffic S remains greater than or equal to L_s. That is, the required system throughput, which attains the stability region, at this CW value is

$$\lambda^*_{U_d,Ls}(CW) = \sup\big(\lambda\colon S \geq L_s\big) \tag{4.1}$$

We applied this optimization method for the three access classes, i.e., AC_1, AC_2 and AC_3, each with its defined CW value. Table 4.1 reports the obtained results for Poisson input rate $\lambda \in [0.1, 0.4]$, from this table we observe the following important findings:

- We observe that IEEE 802.11p is relatively insensitive to the alteration of CW in the interval $[CW_{AC_3}, CW_{AC_2}]$. This is due to the fact that, the CRI constant, i.e., ε_k in (3.21) allows only one increment for CW in the defined interval, which is from CRI length L_2 to L_3.

- We also observe that for a fixed CW value, the attainable $\{S, \lambda^*{}_{U_d,Ls}\}$ value of (4.1) is an increasing function of the delay constraint U_d.

- An interesting observation is that only for small input rates $(0.1, 0.15)$, the 802.11p MAC meets the required reliability when a high delay constraint is imposed. When such constraint is loosened for AC_2, the performance is improved; for small input rates $(0.1, 0.25)$, the fraction of the successfully transmitted traffic S meets the lower bound L_s. This finding further supports the results obtained in Chapter 2 which demonstrated the limitations of 802.11p MAC to support safety messages dissemination.

- For non-safety class with no delay constraint and for input traffic rates within $(0.1, 0.35)$, the fraction S of the successfully transmitted traffic almost equals one, and the throughput then represents the maximum maintainable rate for the input traffic.

The combination of these findings defines the *stability region* which represents the case where the traffic is maintained for the access classes under normal

Table 4.1: Traffic stability region

CW_{AC}	U_d	L_s	λ	S
$CW_{AC_3} = 3$	100	0.99	0.10	0.9961
			0.15	0.9910
			0.20	0.9777
			0.25	0.9062
			0.30	0.8151
			0.35	0.7417
			0.40	0.6411
$CW_{AC_2} = 7$	1000	0.99	0.10	1.0000
			0.15	1.0000
			0.20	0.9971
			0.25	0.9931
			0.30	0.9679
			0.35	0.8114
			0.40	0.7260
$CW_{AC_1} = 15$	NA	0.99	0.10	1.0000
			0.15	1.0000
			0.20	1.0000
			0.25	1.0000
			0.30	0.9970
			0.35	0.9954
			0.40	0.7781

operation (i.e., no jamming). Hence, we may subsequently select on the upper and lower bounds on the cluster rate that to be monitored as, $\lambda_u = 0.35$ and $\lambda_l = 0.15$ respectively. These bounds encompass the contention resolution mechanism, whose operation is explained in Section 4.3, thus any change in the cluster rate which falls outside this interval is due to a jamming attack. However, as first stated in this section, the jamming attack causes an increase in the packet rejection rate and subsequent reduction of cluster input rate, hence the detection algorithm will monitor λ_u to λ_l possible shifts and declares a jamming attack whenever the cluster rate shifts below the lower bound λ_l.

It is worth mentioning that when the traffic is maintained, the contention

resolution process induced by the deployed IEEE 802.11p changes the traffic statistics. When the input traffic to IEEE 802.11p from CMs in each cluster is Poisson, the output traffic to the corresponding CH is not Poisson then, while it maintains the input rate and can be closely approximated by a Poisson process. We also point out that when the traffic is maintained for small input values ($\lambda \leqslant 0.1$), the clustering mechanism is considered wasteful as it adds complexity to the backbone network.

Figure 4.3 results from simulating the clustered network, as previously detailed in Section 4.4, with the basic IEEE 802.11p MAC layer parameters in Table 2.1. The figure illustrates the traffic rates $\lambda_i, i = 1, 2, 3$ for the access classes ACs under normal network conditions, i.e., in the absence of jamming attacks. As clearly shown, the data rates are maintained within the defined *stability region* bounds ($\lambda_u = 0.35, \lambda_l = 0.15$). This result corroborates Lemma 5 and the corresponding analytically obtained results in Tabel 4.1.

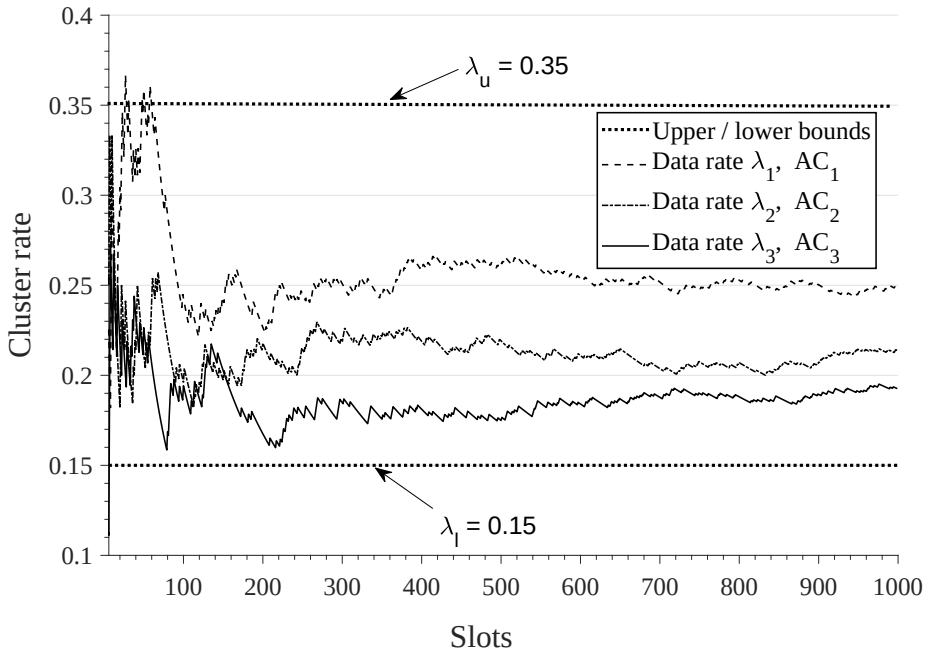


Figure 4.3: Cluster data rate under normal network conditions; no jamming

4.6 QoS-based Sequential Detection Algorithm (QoS-SDA)

After the decision about the detection rate interval is made as detailed in Section 4.5, the objective is to trace possible cluster rate shifts from λ_u to λ_l and declare a jamming attack whenever this shift falls below the detection threshold λ_l. In the following we propose a QoS-based Sequential Detection Algorithm (QoS-SDA) which implements the optimization methodology with the sequential detection of change method that was first presented in Bansal *et al.* [88] and has been used in various networks applications [89–91]. The proposed algorithm operates sequentially on the observed arrival sequence of the cluster data rate λ_{C_i} utilizing a reflective barrier at 0 and a decision threshold ζ. The algorithmic operational value is updated only at the beginnings of equally spaced time instants called frames $\{n_i\}_{i\geqslant 0}$. Initially, QoS-SDA starts with some generated cluster data rate and with its operational value sets to zero $T_0 = 0$. After the algorithm is initialized, it operates in three phases; Observation phase, Updating phase and Detection Phase as follows:

1. Observation phase: Given $\lambda_i, i = 1, 2, 3$ of the traffic classes ACs with known distribution P_i, let $P_i(m_1^n)$, where $m_1^n = (m_1, \cdots, m_n)$ denote its n-th dimensional distribution in frames lengths. Then, the algorithm starts observing the cluster data arrival sequence as follows: given that λ_i is the active rate throughout, m_1 data arrivals occur in the first frame, and so on, with m_n data arrivals lie in the n-th frame.

2. Updating phase: Allowing algorithmic adaptations only at the beginnings of frames and for stationary, memory distribution P_i, the QoS-SDA takes the general form

$$T_n(m_1^n) = max\left[0, T_{n-1}(m_1^{n-1}) + log\left(\frac{P_l(m_n \mid m_1^{n-1})}{P_u(m_n \mid m_1^{n-1})}\right)\right] \qquad (4.2)$$

3. Detection Phase: The algorithm continues updating its operational value until it stops the first time n when it crosses the decision threshold

ζ. Then it is decided that a shift in the cluster rate is outside the predefined bound interval and a jamming attack has occurred.

4.6.1 QoS-SDA for Memoryless Model

As explained in Section 4.5, the traffic accessing the cluster head, while not Poisson it can be approximated by a Poisson process, with rate λ_{Ci} packet/time unit. Since Poisson is stationary memoryless process, QoS-SDA utilizes no memory in this case, hence the conditional distributions in the updating step of (4.2) then collapse. In order to establish the memoryless sequential evolution of the general algorithm in (4.2), it is necessary to define a new set of variables: L is frame length in slot time units, N_n is the number of data arrivals within the n-th frame from the beginning of time.

Then, QoS-SDA uses its per frame observed data arrivals N_n and the detection rate interval to update its operational value as follows

$$T(n) = max\left[0, T(n-1) + L\left((\lambda_u - \lambda_l) + N_n\, log\left(\frac{\lambda_u}{\lambda_l}\right)\right)\right] \tag{4.3}$$

Even though the implementation of QoS-SDA in (4.3) involves minimal complexity comparing to the general algorithm in (4.2), as no memory is required in its operation, the decision threshold value ζ may not be a positive integer. To circumvent this difficulty, we define the constant $\Lambda_{u,l}$ such that

$$\Lambda_{u,l} \triangleq (\lambda_u - \lambda_l) \,/\, log\left(\frac{\lambda_u}{\lambda_l}\right) \tag{4.4}$$

Since the cluster data rate is bounded by rational values, i.e., (λ_u, λ_l), we may further define this constant by two integers b and t as follows:

$$\Lambda_{u,l} = b/t \quad \text{for two integers } b \text{ and } t:\ b < t \tag{4.5}$$

Using the expression in (4.5) and with appropriate scaling by $\mathbb{1}(\lambda)$ where

$$\mathbb{1}(\lambda) = \begin{cases} 1, & \text{if } \lambda_l < \lambda_u \\ 0, & \text{if } \lambda_l > \lambda_u \end{cases} \tag{4.6}$$

with initial $T(0) = 0$, the QoS-SDA in (4.3) then transforms to

$$T(n) = max\left[0, T(n-1) + (-1)^{\mathbb{1}(\lambda)}\big(N_n t - Lb\big)\right] \tag{4.7}$$

The following Pseudocode summarizes the operating phases for QoS-SDA.

Algorithm QoS-based Sequential Detection Algorithm (QoS-SDA)

Initialization
Define the detection rate interval (λ_u, λ_l)
Based on (λ_u, λ_l), define the integers t, b such that $\lambda_l < \frac{t}{b} < \lambda_u$.
Define the number of time slots per frame L
Select a decision threshold ζ , $\zeta > 0$
Set the operational value $T(0) = 0$

Phase 1 – Observation phase

procedure OBSERVATION PHASE
    Let at some slot, λ_u be decided as just starting.
    Let the generating process of λ_u to be Poisson.
    Observe the arrivals in frame lengths.
    Count the number of arrivals in n-th frame (N_n).
end procedure

Phase 2 – Updating phase

procedure UPDATING PHASE
    for each frame **do**
        update $T(n)$ as follows
        $T(n) = max\left[0, T(n-1) + (-1)^{\mathbb{1}(\lambda)}\big(N_n t - Lb\big)\right]$
    end for
end procedure

Phase 3 – Detection phase

procedure DETECTING PHASE
    if $T(n) \geqslant \zeta$ **then**
        Stop at time n
        Cluster rate $\lambda_{Ci} < \lambda_l$
        Declare a jamming attack detection
    end if
end procedure

4.6.2 Decision Threshold Selection

QoS-SDA induces correct detection decisions as well as false alarms whose relative relationship is controlled by the value of the selected threshold ζ. Thus, the performance of the algorithm is basically characterized by two probability measures:

1. $P_D(n)$: The probability that a shift in the cluster date rate below the lower bound λ_l is decided before or at time n given that $\lambda_u \rightarrow \lambda_l$ shift has occurred, named Detection probability.

2. $P_{FA}(n)$: The probability that before or at time n it is decided that the cluster data rate has shifted below the lower bound λ_l, while $\lambda_u \rightarrow \lambda_l$ never changed, named False Alarm probability.

From the description of QoS-SDA in (4.7), it can be easily seen that the above probabilities are monotonically nondecreasing with increasing n. As functions of n, these probabilities represent correct detection and false alarm curves, while the correct detection curve converges to one, the latter converges to values that are generally less than one. These curves can then be used for the appropriate selection of the decision threshold ζ. Qualitatively speaking, we are seeking a threshold value for relatively small n sample sizes such that the probability $P_D(n)$ is sufficiently large, while $P_{FA}(n)$ is be below a specified desirable level. Toward this end, we evaluate QoS-SDA for several given threshold values, then we compare the correct detection and false alarm curves induced by the algorithm at these threshold values to decide on the appropriate threshold value.

Figure 4.4 shows the behavior of the detection and false alarm curves, for four different threshold values. From the figure we note how the two curves are decreasing with increasing given threshold value. The threshold selection for QoS-SDA may then be based on a required detection lower bound and a required false alarm upper bound, at a given time n. From the same figure we observe the better performance for the threshold value 200 and especially for time values $n \leqslant 80$. This is true since larger differences in the false alarm set at different threshold values , i.e., $\{P_{FA}^{\zeta_i}(n) - P_{FA}^{\zeta_j}(n)\ ;\ i \neq j\}$ represent improved algorithmic performance.

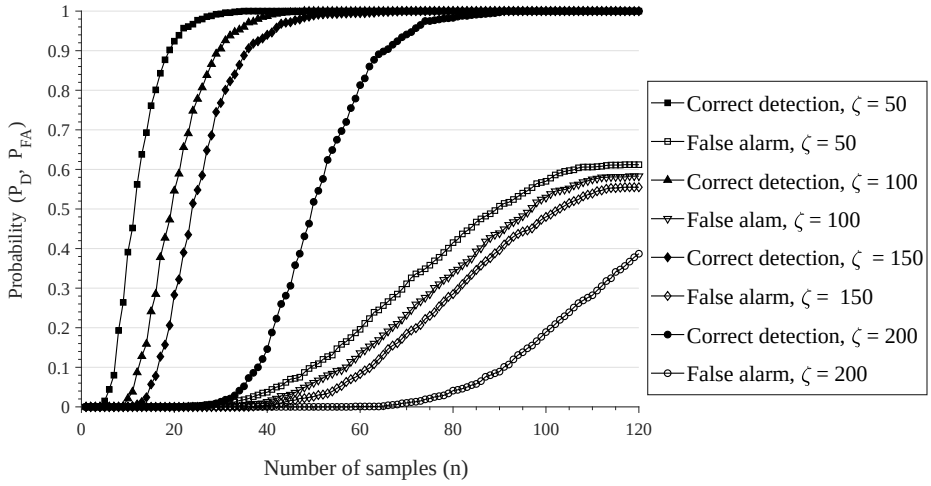


Figure 4.4: Power and false alarm curves for different threshold values

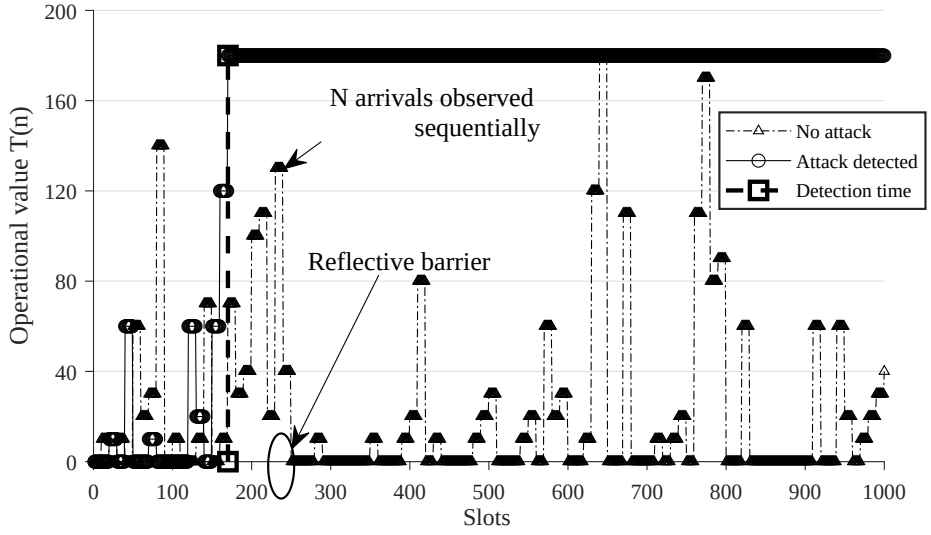


Figure 4.5: Time evolution of QoS-based sequential detection algorithm (QoS-SDA)

By selecting the decision threshold value equals to (200) and utilizing the observed data sequence for non-safety traffic class AC_1, the sequential operation of QoS-SDA is depicted in Figure 4.5. The figure shows two cases;

the first in the presence of Constant jamming attack which was successfully detected and the latter case in the absence of the attack in which the algorithm continues operating sequentially via the use of reflective barrier at zero and the decision threshold. The data in Figure 4.5 clearly demonstrates the ability of the proposed algorithm to detect jamming attacks in a short detection time while false detections are minimized.

4.7 Simulation Model and Results

The simulations were performed using network simulator in Matlab that we developed with the basic IEEE 802.11p MAC layer operation as previously explained in Section 4.3. The used EDCA parameters are those in Table 2.1 with the attempt limit set to seven attempts. We considered the Poisson Model and focused on a single cluster. In addition, we modeled the data rates $\lambda_i, i = 1, 2, 3$ transmitted by each CM as exponentially distributed in frame lengths. We simulated QoS-SDA with monitored cluster rates within the detection interval ($\lambda_u = 0.35, \lambda_l = 0.15$), selected frame length L equals to 20 time slots and with the integers b and t values set to 11 and 50 respectively. In order to let the jammer have time to react, specifically Random jammer, we selected the average message length equals to a frame length. Following the threshold selection method explained in Section 4.6, algorithmic decision threshold was selected to be 200.

Figure (4.6) shows different manifestations of jamming attacks as mentioned in Section 4.3, in the three Subfigures the attacker launches the attack in the first 100 slots of the transmission with rate 0.1 packet/slot, the attack rate was set to this small value to measure the ability of the algorithm to track and detect very small changes in the normal network conditions. Subfigure (a) shows the Constant jammer, where the attacker transmits continues random packets with rate 0.1 packet/slot. The three traffic rates have been affected with more noticeable rate drop for AC_3. This is mainly due to the small CW value used in AC_3 class, more discussion on CW values and their effect on the detection probability is described in the sequel.

Subfigure (b) shows the Random jammer where a packet arrives in each of the time slots of the ON state, following a Bernoulli (0.5) distribution.

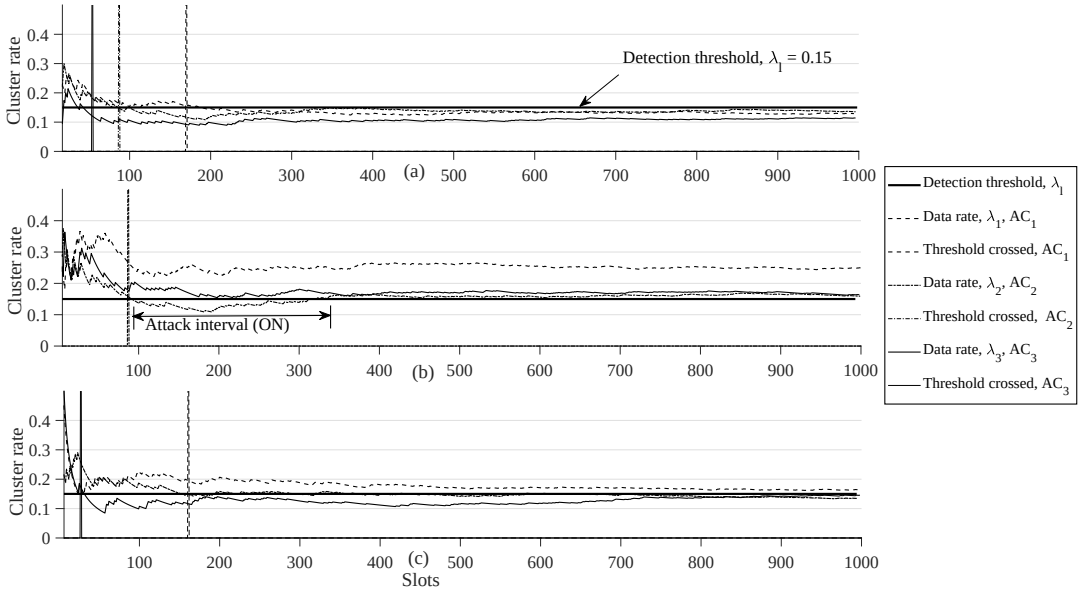


Figure 4.6: The algorithmic performance under different attacker models (a) Constant jammer (b) Random jammer (c) Intelligent jammer

In Subfigure (c), an intelligent jammer, who is aware of the target communications, attacks the legitimate transmissions of the messages in AC_2 and AC_3 utilizing the corresponding contention parameters to inject its interfering packets. As we can see, the algorithm only needed a few samples, at this small value of attacking rate for the three jamming types, to detect the cosponsoring attack. Almost all the detection times, where the detection threshold λ_l has been crossed, fall in the first 100 slots where the attack started.

Detection probability and the detection delay are used as metrics to evaluate QoS-SDA. To illustrate the influences on the attack rate and contention window size CW, we consider the Intelligent jammer as it conforms to the contention mechanism in IEEE 802.11p MAC. Figure 4.7 depicts the detection probability and the detection delay versus the attack rate for different contention window sizes. In Subfigure (a), when $CW = 15$, QoS-SDA performs better as the attack rate increases comparing with the case when $CW = 3$. This decrease in detection probability for AC_3, as compared to AC_1, is due to the fact that shorter contention cycles and shorter AIFS times

would produce more collisions and force the packets to reach the maximum number of attempts quickly and hence abandon the system early. As a result, this induces more rejections and the monitored rates (λ_u, λ_l) are becoming significantly close in Kullback-Leibler numbers which affects the detection accurate decisions in QoS-SDA.

When the attack rate reaches 1, i.e., the malicious attacker jams all the activity in the transmission channel, QoS-SDA can detects up to 70% of attack cases for AC_3 class with $CW = 3$, while it detects almost all the attack cases for AC_1 with $CW = 15$. In Subfigure (b), we plot the detection delay versus the jamming attack rate. As a consequence of the discussion in Subfigure (a), the detection delay is a decreasing function of the attack rate with obviously improved detection performance for traffic class AC_1 with $CW = 15$, primarily due to the larger CW value and long AIFS time comparing with AC_3.

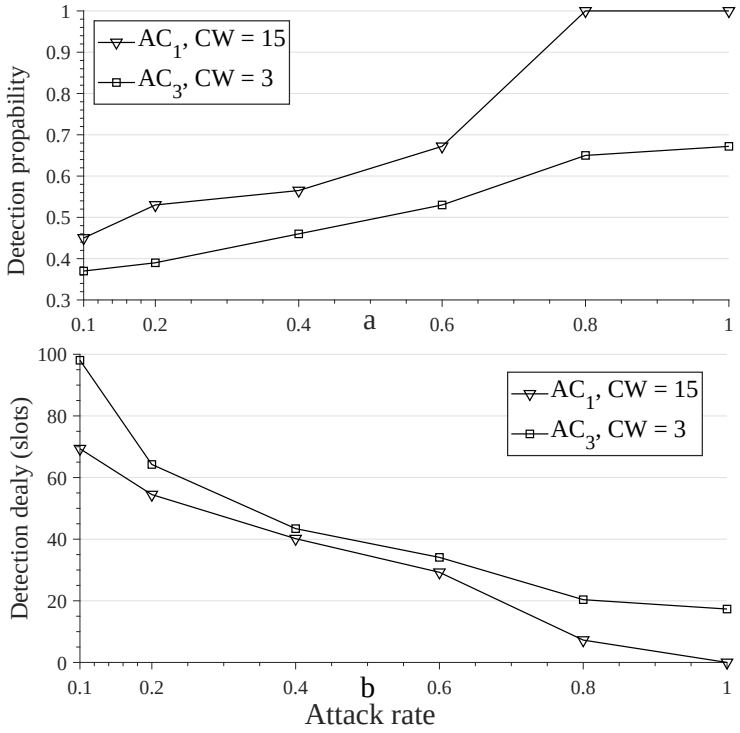


Figure 4.7: Detection probability (a) and delay (b) as a function of the attack rate

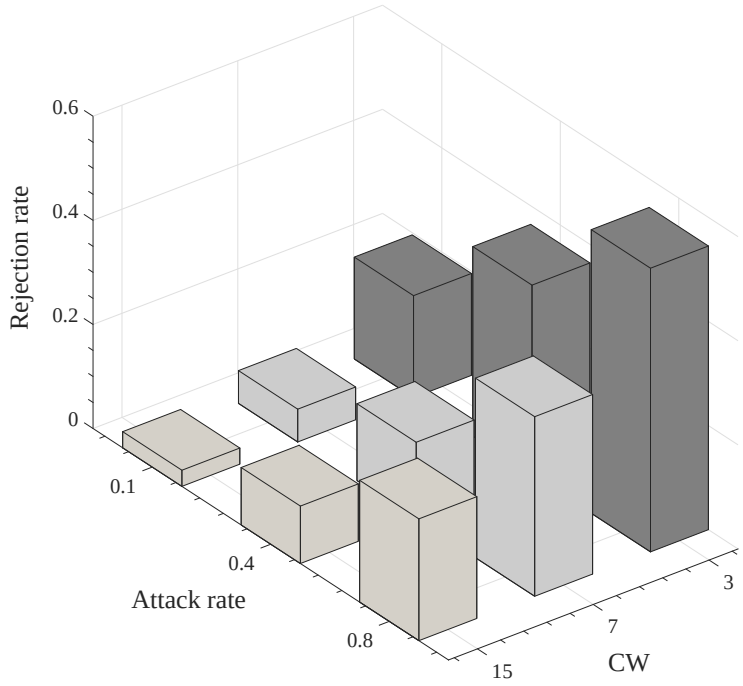


Figure 4.8: Rejection rate as a function of CW size and the attack rate

The effect of the Contention Window size (CW) on the detection probability is further detailed in Figure 4.8. The figure shows a clear trend of increasing rejection rate with increasing attacking rate, which is more noticeable for small contention window values, i.e., $CW = 3$. This is due to the fact that small CW values produce more collisions leading to an increase in the rejection rate which affects the detection correct decisions.

4.8 Conclusions

Jamming attacks are very serious of risk for VANETs which play an important role in enabling life-critical safety applications. Due to the network nature, i.e., rapid changes in topology, high mobility and unbounded scalability, jamming attacks became a concern since countermeasure solutions are not feasible in VANET. Most of the jamming detection techniques that have been proposed in the literature are based on methods primary designed for general wireless networks. However, when it comes to vehicular networks,

certain constraints will be introduced on the adoption of these methods, since the network nature in the vehicular environment is a lot different from general wireless networks. As a result, these methods are not applicable to VANET, especially for real-time safety applications. One important constraint is the diversity of the QoS requirements imposed by different application messages in VANET. In addition, the MAC layer in IEEE 802.11p, which is the main enabling communication standard in VANET, provides access for different QoS classes by prioritizing the data traffic. This added feature which is extensionally designed for vehicular communication should be taken into consideration in any proposed jamming detection method.

In this chapter, we provided an in-depth study of the vulnerabilities of IEEE 802.11p to jamming attacks and focused on three common types of jamming. Drawing upon our observation of IEEE 802.11p MAC layer vulnerabilities to jamming attack, we proposed a novel detection algorithm that takes in consideration the QoS requirements and constraints imposed by different application messages in VANET which makes it more suitable for the vehicular environment. The proposed QoS-based Sequential Detection Algorithm (QoS-SDA) operates sequentially on the observed data sequence in the *stability region* of IEEE 802.11p and declares a jamming attack whenever a shift in this data sequence falls outside the predefined *stability region*. In order to define the *stability region* of IEEE 802.11p, an optimization methodology for IEEE 802.11p MAC configuration under normal operation is developed. The proposed methodology allows to clearly differentiating the jammed network operation from normal operations for various types of jamming attacks. In addition, it offers important insights into IEEE 802.11p MAC layer basic design parameters for enhanced performance. The reported results for different jamming attacks, verified the accuracy and the efficiency of QoS-SDA to detect jamming attacks even under a small attacking rate. When the malicious attacker jams all the activity in the transmission channel, QoS-SDA can detects up to 70% of attack cases for Safety class messages, while it detects almost all the attack cases for Non-safety class.

Chapter 5

General Conclusions

Undoubtedly, the future will bring more challenges for the vehicular networks field, as changes in the available technologies and needs make it more worthy of study.

The growing advances in wireless communication technologies and automobile industry have paved the way for vehicular communication. Vehicle-to-anything (V2X) technology has emerged as a promising solution to improve both road safety and driving comfort. Even though research in the field of vehicular networks has made tremendous progress in the last few years, there are still issues that deserve further consideration. Here, in this thesis, we consider two of the most prominent ones; reliability and security of vehicular communications. This chapter summarizes the thesis, discusses its findings and contributions, and also outlines directions for future research. The chapter is divided into three sections. Section 5.1 is a summary of the thesis. Section 5.2 provides a resume of our contributions and gives a brief overview of the developed methods and techniques in this thesis. Finally Section 5.3 presents and discusses the future work.

5.1 Summary of the Thesis

More than 1.2 million people die on the roads every year. Safe, automated driving supported by Vehicle-to-anything communications, or V2X, will enhance traffic safety and driving comfort aiming to provide maximum casualty

reduction. V2X technology enables vehicles to communicate with their surroundings via Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P) communications. V2X communications enable active safety systems that can help to reduce fatalities and injuries on the roads. In addition to improving safety, V2X holds great potential for traffic management and reducing road transport emissions.

There are two potential solutions to support V2X communications; Dedicated Short-Range Communications (DSRC) and cellular network technologies. During the years 2005 to 2010 an adapted version of the IEEE 802.11 based-DSRC standard for vehicular communication was developed. This 802.11p amendment defines the medium access (MAC) and the physical (PHY) communication layers, which collectively with the family standard IEEE 1609 constitute the Wireless Access in Vehicular Environment (WAVE) communication protocol. Cellular technologies, on the other hand, have witnessed incredible development in the past 25 years making it an off-the-shelf potential solution for V2X communications. Despite their advantages, the centralized nature of the cellular networks jeopardizes their ability to support real-time V2X safety applications. Consequently, DSRC remains an essential technology for realizing V2X communications.

This thesis, therefore, studies the DSRC communications with great potential given to the MAC layer of IEEE 802.11p, the main enabling DSRC communication standard in V2X, so that it will be able to support reliable and secure V2X communications, either in pure V2X DSRC communications or in hybrid DSRC-Cellular V2X communications. A primary concern in realizing V2X communications is the design of MAC protocol that is able to satisfy the Quality-of-Service (QoS) of different supported applications, especially safety applications. In this part, the aim of this thesis is twofold. Firstly, to analyze and assess the capacity of IEEE 802.11p/WAVE protocol to provide a reliable and efficient V2X communications and secondly to investigate the design parameters of IEEE 802.11p MAC protocol for proposed enhanced performance. Toward this end, a User Model-based Method is then proposed to render the above objectives possible.

Another major concern, from V2X reliability perspective that this thesis is addressing, is the operability challenge in large-scale V2X deployment. In

order to ensure efficient and adequate large-scale operability, an interworking between DSRC and cellular technologies in this case is more viable. However, the DSRC and cellular interworking in itself poses also several challenges, such as hybrid architecture and mobility management. A common factor in addressing those design challenges and consequently to achieve large-scale operability is to determine a complete and an accurate description for the output process of IEEE 802.11p-based DSRC communication standard. This output process is the input to other nods in the interconnected system and greatly influences its performance. For this purpose, a novel Regenerative model is introduced to provide a complete description of IEEE 802.11p output process. To be more precise, the model exploits the regenerative character of IEEE 802.11p actual output process and by observing the dynamics of the contention resolution scheme and its direct interaction with the shared transmission channel defines description models for IEEE 802.11p output process under different traffic intensities.

The analysis of IEEE 802.11p standard undertaken here, has extended our knowledge about the standard's configurations leading to develop an optimization methodology which aims to enhance its performance. On the other hand, this analysis explored IEEE 802.11p vulnerabilities to security threats. Taken together, the last two findings motivated our research to go step further toward addressing the security issue in the vehicular environment. Apart from the mentioned reliability issues, security issue is another main concern in vehicular networks which must be fully considered in order to have an efficient and secure communication. Accordingly, from the security perspective, this research seeks to enhance V2X communication security by means of a new detection algorithm especially tailored for the vehicular environment. Specifically, by integrating the developed optimization methodology with the sequential detection of change method, the proposed QoS-based Sequential Detection Algorithm is designed to detect jamming attacks with high detection probability even under small attacking rates.

5.2 Summary of the Results

This section concludes the results by synthesizing the key findings of the thesis. In this section, each subsection begins by an introductory context restating the research problem underpinning our study in each chapter followed by a brief analysis of the outcomes obtained in the corresponding chapter.

5.2.1 User Model-based Method for IEEE 802.11p MAC Performance Evaluation

In Chapter 2, we first proposed User Model-based Method for evaluating the capacity of IEEE 802.11p standard to provide reliable and efficient V2X communications. In reviewing the literature, most of the presented methods are based on Markovian models which, besides their intractability, usually give insufficient information on IEEE 802.11p MAC protocol stability. The proposed method in this research represents a systematic method which reduces the problem of defining a Markovian model to the problem of determining the steady state moments of the induced delay process. Moreover, the method defines a relation between the Finite and the Infinite population user models so that the capacity of IEEE 802.11p can be assessed under the saturated and unsaturated traffic conditions. The obtained analytical and simulation results prove the validity of the proposed method, and demonstrate its ability to effectively model the actual functionality of IEEE 802.11p as compared to the Markovian models.

The results from applying this method revealed that IEEE 802.11p is stable under the Finite user model, providing sufficient QoS for all the supported application classes including safety applications. However, under the Infinite user model, the standard fails to satisfy the required QoS for safety messages delivery. The obtained results from this study indicate shortcomings in the design parameters of the contention resolution mechanism which is at the heart of IEEE 802.11p MAC protocol operation. In particular, the obtained results advise increasing the Contention Window (CW) parameter size to enhance the transmission reliability; however, this could lead to an increase in the induced average delay. The findings observed in this study

are what motivated our research to propose a new optimization methodology aiming to enhance the performance of IEEE 802.11p MAC protocol. The proposed optimization methodology has been further used in enhancing the security part of V2X communications.

5.2.2 V2X Interworking Enhancement

The possibility of incorporating other design parameters along with the contention window in the systematic User method of Chapter 2 is the subject of our motivation in this part of the research. In Chapter 3, the method has been extended by introducing new parameters and analytical techniques, in the interest of defining the interdeparture distance which constitutes the output process of IEEE 802.11p standard. For this purpose, Regenerative model has been proposed to provide complete description for the output process of IEEE 802.11p under different traffic intensities. Defining this output process is a key issue in any envisioned V2X hybrid interworking system, and plays a fundamental role in determining its performance. An efficient and adequate interworking is an essential component in achieving large-scale operability for V2X deployments.

Unfortunately, the generalisability of much published research on this issue is problematic. What we know about IEEE 802.11p output process is largely based on simulation studies that do not provide a complete or an accurate description of the process. On the other hand, any attempt to address this issue is tempted to adopt the memoryless models; however, the ability of such models for the description of the interworking traffic processes in general wireless networks has been always questioned. Thus, the adoption of such models in the vehicular environment, with its strike characteristics, could lead to erroneous identification of the bottlenecks of the interconnected hybrid system.

The analytical and the simulation results presented in this study verified the accuracy of the Regenerative model and its ability to capture the deviations in the output process of IEEE 802.11p when employed under different traffic intensities. In addition, the proposed model is compared with the Poisson memoryless model in V2X interworking enhancement of a DSRC-

cellular dynamic architecture. The resulted analytical and simulation data, evidently show that the performance of the Regenerative model is superior to that of Poisson model as the latter fails to capture the real deviations in the actual output process of IEEE 802.11p. The obtained results clearly show how the adoption of memoryless models leads to erroneous delay calculations that cannot be tolerated for real-time safety applications. Overall, realizing efficient and adequate interworking is a major challenge in general wireless networks as well. The proposed Regenerative model for the vehicular environment may be applied to general wireless networks, the technique used in developing the model is believed to be a fairly general and could be modified to match the peculiarities of the specific wireless network at hand.

5.2.3 Optimization Methodology for IEEE 802.11p Reconfiguration

In vehicular networks, traffic safety applications set the benchmarks for the functional requirements with respect to the communication in terms of satisfying strict QoS requirements such as; low latency, high transmission reliability and communication range. However, our analysis for IEEE 802.11p-based DSRC communication standard, revealed that the standard's MAC layer cannot ensure time critical message dissemination (e.g., safety collision warnings), especially in dense traffic scenarios. Therefore, it is of considerable interest to design MAC protocol that will operate efficiently and reliably under the strict QoS constraints of safety applications. For this purpose, an optimization methodology is developed which ties the QoS requirements of the application classes with the basic contention mechanism design parameters in IEEE 802.11p MAC protocol.

The results of a preliminary application of the methodology using the defined design parameters are promising. One interesting result is that no significant improvement in the standard's performance is observed by increasing the Contention Window (CW) value within the defined interval of Safety-of-life and Safety applications, i.e., $[AC_3, AC_2]$. This result indicates that CW value, that attains the QoS of safety messages, should be increased out the range of this interval. Another observation from this result is as fol-

lows: since IEEE 802.11p MAC is insensitive to the alteration of CW value in the safety applications' interval, then, we could define one queue for both safety applications in the multichannel operation of IEEE 802.11p by setting one CW value for both. This will lead to appropriate channel utilization which will further save the limited bandwidth. The latter is a crucial bottleneck that reduces and slows down the scalability of the applied information dissemination scheme in vehicular networks.

Another important result of the developed methodology is the determination of IEEE 802.11p *stability region* for which the traffic rate is maintained (in terms of satisfying the QoS requirements) for all the application classes. Based on the defined *stability region*, we determined a detection threshold value. We further used this threshold value in developing a new detection algorithm for jamming attacks in vehicular networks, which we review its key findings in the upcoming subsection. Moreover, defining the *stability region* of IEEE 802.11p can be further exploited in the dynamic architectural reconfigurations of vehicular networks, which defines one of our future research interests.

5.2.4 Securing VANET Against Jamming Attacks

In Chapter 4, we proposed a new detection algorithm for jamming attacks in vehicular networks, QoS-based Sequential Detection Algorithm (QoS-SDA). The proposed QoS-SDA mainly relies on the developed optimization methodology and the sequential detection of change method. The algorithm utilizes a detection threshold value which is obtained from applying the optimization methodology on IEEE 802.11p communication standard when employed in V2X dynamic architecture. This threshold value is used as a boundary to distinguish the network's normal operation from its operation under jamming attacks. By integrating the sequential detection of change method, the algorithm observes sequentially the data arrivals and declares a jamming attack whenever arrivals' rate falls below the detection threshold value. We applied QoS-SDA to detect three common types of jammers; Constant, Random and Intelligent jammer when safety and non-safety applications are running in the network.

The obtained results not only demonstrated the ability of the proposed algorithm to effectively detect jamming, but also validated the accuracy of the developed methodology and its arguments. From the results, a better detection performance is noticeable for non-safety applications as compared to safety applications, which is mainly due to the utilized CW values in each application class. This result confirms the results of the optimization methodology which proved the necessity to increase CW values to enhance the reliability of safety messages dissemination. The results show a monotonic increase in the detection probability with the attacking rate. When the attacking rate reaches one, QoS-SDA detects up to 70% of attacks in safety applications while it detects almost all the attack cases for non-safety applications. This monotonic tendency holds for the detection delay as well, which is shown to be a monotonically decreasing function of the attacking rate. According to the results, we conclude that the presented analysis and simulations confirm the capability of QoS-SDA algorithm to effectively detect jamming attacks, even at a small value of attacking rate.

5.3 Future Work

Given the limited time and the scope of the research carried out for this thesis, extensive experiments have not been conducted for all the studies. For some of them, only preliminary results are presented. In this section, we discuss future research directions and perspectives with respect to research studies conducted in this thesis.

IEEE 802.11p MAC Protocol Enhancement: In this thesis, we have proposed an optimization methodology for IEEE 802.11p configuration that can assist in improving the performance of the standard. The main idea is to maximize the *stability region* of IEEE 802.11p MAC protocol while at the same time satisfying the QoS constraints of each application class in the protocol. Even though the preliminary findings from applying the methodology for security enhancement in the vehicular environment were encouraging, further investigation regarding the effect of transmission delay upper bound U_d on the protocol throughput would be worthwhile. In fact,

for large U_d values (as for non-safety applications), the throughput is not completely determined by the constraint on the fraction of the successfully transmitted traffic L_s, an appropriate determining factor in this case, is the constraint on the expected delays for successfully transmitted packets.

In addition to the security application, we are exploring the possibility to build a reconfigurable vehicular network architecture facilitated by a *dynamic architectural reconfiguration algorithm* which exploits the optimization methodology results for optimal overall network performance. The idea is to consider a clustered topology (since vehicles on the same directed path tend to form clusters) in which the cluster data rates are all bounded from above by bounds determined by the *stability region* of the deployed IEEE 802.11p in each cluster. The envisioned *dynamic architectural reconfiguration algorithm* works as follows: First, the aggregate network data rate at time T_i and subsequently the expected number of clusters N_i in the network are computed. Then, as compared to the network architecture at time T_{i-1}; if $N_i = N_{i-1}$ then the architecture of the backbone network remains unchanged. If $N_i < N_{i-1}$, then some clusters are eliminated and this induces dynamic reallocation for the survived cluster heads. The eliminated clusters are those who possess the lowest rates according to the *stability region* bounds. Clearly, for the operation of the *dynamic architectural reconfiguration algorithm*, two underlying algorithms should be deployed simultaneously in the original network architecture; a routing protocol that works on aggregating the overall network data rate at predefined time intervals, and an efficient monitoring algorithm that observes the clusters data rates.

Development and Application of the Regenerative Model: The Regenerative model proposed is Chapter 3 has a huge impact on V2X hybrid interworking enhancement. The proposed model is developed to overcome the problem of the interconnected-traffic process characterization in V2X interworking. The model provides complete description of IEEE 802.11p-based DSRC output process under different traffic scenarios, where a Bernoulli and a First-order Markov models are proposed. Due to the bursty nature of the vehicular data at high traffic rates, the First-order description model performs better than Bernoulli for moderate and heavy traffic description, with re-

spect to the interworking fundamental delay issue. Further experimentation into the performance of the Regenerative model is strongly recommended, it would be interesting to assess the effects of the model on the performance enhancements and evaluations of other interworking issues, such as mobility management and network selection issues.

In fact, the high dynamic vehicular network topology along with the trend of small-cell deployment in next generation cellular networks (i.e., 5G), which requires effective mobility management and network selection schemes, adds to the complexity of the eventual interconnected system and makes an efficient interworking quite challenging. To efficiently achieve such DSRC-cellular interworking, we need to account for the actual DSRC output traffic, which is only obtained through the Regenerative model. In this context, we are currently working on extending the Regenerative model using Second-order Markov description model. The Second-order model is intuitively more pleasing than First-order, since it captures better the dependency in IEEE 802.11p output process which is introduced by the contention resolution process of IEEE 802.11p MAC protocol. However, the analytical calculations of the Second-order Markov model (i.e., transition probabilities), in this case involve some complexity as compared to the First-order model. To minimize the computational complexity of the Second-order model, the previously defined First-order Markov model could serve as an underlying process for the determination of the parameters of the Second-order model.

Publications

The publications directly stemming from this thesis work are the following:

Journal Papers

F. Salem, Y. Elhillali and S. Niar, "Efficient modeling of IEEE 802.11p MAC output process for V2X interworking enhancement," IET Networks, Online ISSN 2047-4962, 2018.

Refereed Conference Proceedings

F. Salem, Y. Elhillali and S. Niar, "User model-based method for IEEE 802.11p performance evaluation in vehicular safety applications," 2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Austria, Vienna, 2017.

F. Salem, Y. Elhillali and S. Niar, "Stochastic modeling of IEEE 802.11p output process for efficient V2X large-scale interworking," 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT), Belgium, Leuven, 2017.

F. Salem, Y. Elhillali and S. Niar, "QoS-based Sequential Detection Algorithm for Jamming Attacks in VANET," International Conference on Future Network Systems and Security (FNSS), France, Paris, 2018.

Appendix A

Proof of the Assertion Given in (3.12)

Let us define

- CW: The contention window size.
- $P_m(\eta_m, \sigma_m^2)$: The distribution of the traffic formed by the arrival packets with mean η_m and variance σ^2.
- P: The probability that a single transmission occurring in an interval of expected length l.
- λ : Poisson arrival rate.
- S : The expected number of successful packets in a CRI of expected length L.

Let m represents the total number of arrivals in the interval l with rate η_m. If the contention resolution process, induced only a single successful transmission in the interval l, then the probability $P = CW/\,l$. However, under stable operation of the algorithmic system (m is small), the probability of having a single packet (successful transmission) is also equals the input rate , i.e., $P = \eta_m$. Now let m to increase and the quantities η_m and σ^2 in the arrivals' distribution P_m simultaneously to decreases so that

$$\eta_m m = \lambda \qquad \text{for} \;\; \lambda > 0, m >> 1 \tag{A.1}$$

A.1 is basically states the Poisson theorem, hence P_m converges in distribution to Poisson process.

Since $P = \eta_m$ and $\eta_m \triangleq m/l$, then (A.1) can rewritten as

$$CW/\, l \cdot \eta_m l = \lambda \tag{A.2}$$

The Poisson process has an interesting property that given a number of arrivals in an interval, the arrival points in this interval is uniformly distributed. Hence, if a fraction $S/\lambda CW$ of the packets are successfully transmitted in a CRI it means that $S/\lambda CW$ is the fraction of the interval resolved. Therefore, $(S/\lambda CW)CW = S/\lambda$ represents the average portion of the resolved interval, which takes on the average L slots to be resolved. Thus, in view of the CRI recursion in (3.18), the algorithm remains stable, even when it is highly loaded (m is large), whenever it is able to resolve collisions at the rate in which the arrival process progresses in time, i.e.,

$$L = \frac{S}{\lambda} \tag{A.3}$$

Substitution of (A.1) and rearranging

$$L = \left(\frac{S}{\Gamma}\right) l \tag{A.4}$$

Γ is the expected number of successful transmissions in the interval l.

The infinite random sequence $\{\tau_i, i \geq 1\}$ as defined in (3.5) is independent identically distributed (i.i.d) with common finite mean, i.e., $E\{\tau_i\} = \Gamma$. Hence, if we were to observe the values of this random sequence, $\tau_1, \tau_2, \ldots$, sequentially in time till a random time point N, then from the algorithmic operation the following equality holds

$$S_N = \sum_{i=1}^{N} \tau_i$$

S_N is the total number of successful transmissions observed till the random stopping time N.

Let us define

$$T_N \triangleq \sum_{i=1}^{N} E\{\tau_i\} \tag{A.5}$$

then by Wald's theorem we have

$$E\{S_N\} = E\{T_N\} \tag{A.6}$$

$$S = \Gamma \tag{A.7}$$

The last equality is in the stopping time sense and consequently (3.12) holds which proves the validity of the given assertion.

Appendix B

Bounds on the Expected Value of CRI Length

In Chapter 3, we showed that the desired upper bound for L_m should be of form

$$L_m \leq \varepsilon_k m - 1, \quad m >> 1 \tag{B.1}$$

where the constant $\varepsilon_k \approx 2.7$ for $m \geq 3$.

In this Appendix, we demonstrate that this bound can be computed with high accuracy. Toward this end, we seek the smallest value for the constant ε_k for which the latter bound is true. The point of departure is the Kronecker delta function $\delta_{i,j}$ defined as

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \tag{B.2}$$

using (B.2), the inequality in (B.1) can be rewritten as

$$L_m \leq \varepsilon_k m - 1 + \sum_{n=0}^{k-1} \delta_{n,m}(L_m - \varepsilon_k m + 1) \tag{B.3}$$

$$L_m \leq \varepsilon_k m - 1 + (L_m - \varepsilon_k m + 1) \tag{B.4}$$

Since, the right hand side of (B.4) equals L_m, then substituting the obtained bound from (B.3) in (3.18) we get

$$L_m \leq \frac{\varepsilon_k m - 1 - P_0 + 2\left[\sum_{n=0}^{k-1}\Big(L_n - \varepsilon_k n + 1\Big)P_n\right]}{1 - (2)^{1-m}} \tag{B.5}$$

observing (B.5), it can be seen that (B.1) holds if we choose ε_k such that the summation quantity in (B.5) is non positive for $m \geq k$, i.e.,

$$\sum_{n=0}^{k-1} \Big(L_n - \varepsilon_k n + 1 \Big) P_n \leq 0 \tag{B.6}$$

$$\varepsilon_k \sum_{n=0}^{k-1} n P_n \geq \sum_{n=0}^{k-1} (L_n + 1) P_n \tag{B.7}$$

thus the required ε_k is given by

$$\varepsilon_k \geq \left[\frac{\sum_{n=0}^{k-1} (L_n + 1) P_n}{\sum_{n=0}^{k-1} n P_n} \right] \tag{B.8}$$

Recall that for the computation of (B.1) we assumed that m is very large such that $\varepsilon_k \geq (L_m + 1)/m$. Therefore (B.8) represents the supremum from which we can obtain the smallest ε_k

$$\varepsilon_k = \max \left((L_m + 1)/m, \sup_{m \geq k} \left[\frac{\sum_{n=0}^{k-1} (L_n + 1) P_n}{\sum_{n=0}^{k-1} n P_n} \right] \right) \tag{B.9}$$

For a given m, the value of L_m can be computed from (3.18), see Table 3.1, and hence determine ε_k as in (B.9). Thus it is a simple matter numerically to find that for $m \geq 3$, we have

$$L_m \leq 2.68m - 1 \tag{B.10}$$

Remark 4. *The obtained upper bound in (B.10) guarantees a positive service rate (m/L_m) for the stability of the algorithmic system as claimed in Subsection 3.4.1. To show this, we start with the fact that the expression in (B.8) represents the supremum. Hence the Poisson approximation is valid, then asymptotically, we have*

$$\sum_{n=0}^{k-1} (L_n P_n) \approx L_m \tag{B.11}$$

and

$$\sum_{n=0}^{k-1}(nP_n) \approx \lambda L_m \tag{B.12}$$

Making use of the latter approximations in (B.11) and (B.12), the inequality in (B.8) can be written as

$$\varepsilon_k \geq \left[\frac{L_m + 1}{\lambda L_m}\right] \tag{B.13}$$

Since $m/L_m = \lambda \quad as \quad m \to \infty$ *, then*

$$\frac{m}{L_m} \geq \frac{1}{\varepsilon_k} + \frac{1}{\varepsilon_k L_m} \qquad m \geq k \tag{B.14}$$

Hence the service rate m/L_m *is guaranteed to be larger than* $1/\varepsilon_k$*, if the arrival rate is smaller than the latter service rate, then the algorithm is stable.*

Appendix C

Proof of Lemma 4

Given m and η_m as in (3.1), the quantity $\mu = m\eta_m$ is the input rate of the algorithmic system. Define the output rate α such that $\alpha = \frac{1}{n}\sum_{i=1}^{n}\beta_i$, where $\beta_i = 1$ if the $i\,th$ slot is a success slot, i.e., one user transmitting and $\beta_i = 0$ otherwise. If $\overset{\star}{\lambda}$ is the system throughput, then the following simple throughput definition relates the output process with the channel status process

$$\overset{\star}{\lambda} = \sup\big(\mu\colon \mu = \alpha\big) \tag{C.1}$$

(C.1) implies that the channel is noiseless which is by definition allows us to partition the channel output into disjoint sets [92]. Hence, the shared channel (CCH) at slot T can be viewed in one of the following status: s_1 if only one user is transmitting at T, s_2 if more than one user transmitting at T hence a collision occurs and s_3 is idle if no user occupying the channel at T. Since the last two states do not result in an output, we can lump them both in one state s_2 and consider the channel status process as a two state process.

Since $\alpha = \frac{1}{n}\sum_{i=1}^{n}\beta_i$ and in viewing the noiseless channel mapping in (C.1), the output process $\{\beta_i\}_{i\geq 1}$ and a two state channel status process $\{Ch_i\}_{i\geq 1}, Ch_i \in \{s_1, s_2\}$ are identical, hence

$$\{\beta_i\}_{i\geq 1} = \{Ch_i\}_{i\geq 1} \,:\, Ch_i \in \{s_1, s_2\}$$

We note that the throughput definition in (C.1) applies for the infinite population model, m is large, as well. Hence we could have specified $\mu = \lambda$, where λ is Poisson input rate, in (C.1) and the Lemma would still hold.

Appendix D

Proof of Lemma 5

Let us define

- CW: The contention window size.
- $P_m(\mu, \sigma^2)$: The distribution of the traffic formed by the arrival packets with mean μ and variance σ^2.
- P: the probability of successful transmission
- k : the expected number of packets that are successfully transmitted during a time interval l given that it started with the transmission of m packets

When no constraints (i.e., delay or successful transmission bounds) on the transmitted traffic are imposed, the following definition of throughput is meaningful to capture IEEE 802.11p MAC algorithm stability

$$\lambda^* = \sup\big(\mu \colon \mu = \alpha\big) \tag{D.1}$$

Let us define the output rate α such that $\alpha = \frac{1}{n}\sum_{i=1}^{n}\beta_i$, in Chapter 3 it has been proven that the output process of IEEE 802.11p under stable conditions tends to follow a Bernoulli distribution. Hence

$$\{\beta_i\}_1^n \sim \text{Brn} = \begin{cases} P(\beta_i = 1) = P & \text{if the } i\text{-th slot is a success slot} \\ P(\beta_i = 0) = 1 - P & \text{otherwise} \end{cases} \tag{D.2}$$

The only parameter of the Bernoulli output distribution in (D.2) is P. To define P let us consider the following scenario: Let m represents the total number of arrivals (packets) in a time interval l with rate μ. If the contention

resolution in IEEE 802.11p, induced only a single successful transmission, then the probability of this event is $P = CW/\,l$. However, under stable operation of the algorithm (m is small) this value approaches the input rate i.e., $P = \mu$ and consequently (D.1) holds

Now let m to increase and the quantities μ and σ^2 in the arrivals' distribution P_m simultaneously to decreases so that

$$m\mu = \lambda \qquad \text{for} \;\; \lambda > 0, m >> 1 \tag{D.3}$$

the latter expression is the Poisson theorem, then P_m converges in distribution to Poisson process, i.e., $P_m \longrightarrow Pois(\lambda)$.

In the presence of constraints and give Poisson traffic rate λ, the expected number of packets transmitted in the first slot of a time interval l is λCW and therefore the fraction of packets that are successfully transmitted S during l is $S = k/\lambda CW$. In [93], recursions for computing the quantity k have been found.

In Poisson process, the arrival points in an interval are uniformly distributed. Hence, if a fraction S of the packets are successfully transmitted it means that S is also the fraction of the interval resolved. Therefore, $(k/\lambda CW)CW = k/\lambda$ represents the average portion of the resolved interval, which takes on the average N slots to be resolved. Thus, the algorithm remains stable, even under congestion conditions (m is large), whenever it is able to resolve collisions at the rate in which the arrival process progresses in time, i.e.,

$$N \leqslant \frac{k}{\lambda} \tag{D.4}$$

(D.4) defines the maximum value on the input rate λ at this specific CW value so that IEEE 802.11p throughput is maximized while the successfully transmuted packets are bounded by S; thus, the statement in Lemma 5 is a consequence of this.

Bibliography

[1] World Health Organization. Global status on road safety 2015. Technical report, Geneva, Switzerland, 2015.

[2] T. Lomax D. Schrank, B. Eisele and J. Bak. Urban mobility scorecard. Technical report, TX, USA, 2015.

[3] ERF, european road statistics. Technical report, Brussels, Belgium, 2011.

[4] P. Merias J. Meredith. Study on LTE-based V2X services (release 14), technical specification. Technical report, 2016.

[5] IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *IEEE Std. 802.11-2012 (Revision of IEEE Std. 802.11-2007)*, pages 1–2793, 2012.

[6] European profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 GHz frequency band. Technical report, 2010.

[7] Frequency allocation table 2 (annexes 8.8 and 11.3). Technical report, Tokyo, Japan, 2015.

[8] Fan Bai and H. Krishnan. Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications. In *2006 IEEE Intelligent Transportation Systems Conference*, pages 355–362, Sept 2006.

[9] A. Vinel. 3GPP LTE versus IEEE 802.11p/WAVE: Which technology is able to support cooperative vehicular safety applications? *IEEE Wireless Communications Letters*, 1(2):125–128, April 2012.

[10] Cisco visual networking index: Forecast and methodology, 2016-2021. Technical report, San Jose, CA, USA, 2016.

[11] Vehicle safety communications project task 3 final report, DOT HS 809 859. Technical report, Washington, DC, USA, 2005.

[12] R. Baldessari. Car-2-Car communication consortium manifestot. Technical Report Ver. 1.1, Braunschweig, Germany, 2007.

[13] Vehicle safety communications-applications (VSC-A) final report. Technical Report DOT HS 811 492A, Washington, DC, USA, 2011.

[14] Powell G. R. Yoon R. Fikentscher J. Doyle C. Sade D. Lukuc M. Simons J. Harding, J. and J. Wang. Vehicle-to-Vehicle communications: Readiness of V2V technology for application. Technical Report DOT HS 812 014, Washington, DC, USA, 2014.

[15] T. Kosch, C. J. Adler, S. Eichler, C. Schroth, and M. Strassberger. The scalability problem of vehicular ad hoc networks and how to solve it. *IEEE Wireless Communications*, 13(5):22–28, October 2006.

[16] K. Abboud, H. A. Omar, and W. Zhuang. Interworking of DSRC and cellular network technologies for V2X communications: A survey. *IEEE Transactions on Vehicular Technology*, 65(12):9457–9470, Dec 2016.

[17] Fatma Salem, Yassin elhillali, and Smail Niar. User model-based method for IEEE 802.11p performance evaluation in vehicular safety applications. In *2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, pages 63–68, June 2017.

[18] Ho Ting Cheng, Hangguan Shan, and Weihua Zhuang. Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mechanical Systems and Signal Processing*, 25(6):2020 – 2038, 2011.

[19] H. Hartenstein and L. P. Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 46(6):164–171, June 2008.

[20] DSRC implementation guide. a guide of users of SAE J2735 message sets over DSRC. Technical report, 2010.

[21] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. Technical Report ETSI TR 102 638 V1.1.1 (2009-06), F-06921 Sophia Antipolis Cedex - FRANCE, 2009.

[22] Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. Technical Report ETSI TS 102 637-2 V1.1.1 (2010-04), F-06921 Sophia Antipolis Cedex - FRANCE, 2010.

[23] C. Sacchiand A. Lyakhov M. Telek A. Vinel, B. Bellalta and M. Oliver. *Multiple Access Communications*. Springer-Verlag, Berlin Heidelberg, 2010.

[24] D. Malone, K. Duffy, and D. Leith. Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions. *IEEE/ACM Transactions on Networking*, 15(1):159–172, Feb 2007.

[25] O. Tickoo and B. Sikdar. Queueing analysis and delay mitigation in IEEE 802.11 random access MAC based wireless networks. In *IEEE INFOCOM 2004*, volume 2, pages 1404–1413 vol.2, March 2004.

[26] Mahanti A. Rao A., Kherani A. Performance evaluation of 802.11 broadcasts for a single cell network with unsaturated nodes. In *NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*, pages 836–847, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[27] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, March 2000.

[28] Marc Torrent-Moreno and Jens Mittag. Adjusting transmission power and packet generation rate of periodic status information messages in VANETs. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, VANET '06, pages 90–91, New York, NY, USA, 2006. ACM.

[29] F. Schmidt-Eisenlohr, M. Torrent-Moreno, T. Mittag, and H. Hartenstein. Simulation platform for inter-vehicle communications and analysis of periodic information exchange. In *2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services*, pages 50–58, Jan 2007.

[30] J. R. Gallardo, D. Makrakis, and H. T. Mouftah. Performance analysis of the EDCA medium access mechanism over the control channel of an IEEE 802.11p WAVE vehicular network. In *2009 IEEE International Conference on Communications*, pages 1–6, June 2009.

[31] Jose R. Gallardo, Dimitrios Makrakis, and Hussein T. Mouftah. Mathematical Analysis of EDCA's Performance on the Control Channel of an IEEE 802.11p WAVE Vehicular Network. *EURASIP Journal on Wireless Communications and Networking*, 2010(1):489527, Apr 2010.

[32] Jianhua He, Zuoyin Tang, Tim O'Farrell, and Thomas M. Chen. Performance analysis of DSRC priority mechanism for road safety applications

in vehicular networks. *Wireless Communications and Mobile Computing*, 11(7):980–990, 2011.

[33] Q. Yang, S. Xing, W. Xia, and L. Shen. Modelling and performance analysis of dynamic contention window scheme for periodic broadcast in vehicular ad hoc networks. *IET Communications*, 9(11):1347–1354, 2015.

[34] M. Khatua and S. Misra. D2D: Delay-aware distributed dynamic adaptation of contention window in wireless networks. *IEEE Transactions on Mobile Computing*, 15(2):322–335, Feb 2016.

[35] S. Cao and V. C. S. Lee. Improving throughput of multichannel MAC protocol for VANETs. In *2016 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, pages 1–6, July 2016.

[36] Y. Yao, L. Rao, X. Liu, and X. Zhou. Delay analysis and study of IEEE 802.11p based DSRC safety communication in a highway environment. In *2013 Proceedings IEEE INFOCOM*, pages 1591–1599, April 2013.

[37] M. J. Booysen, S. Zeadally, and G. J. van Rooyen. Performance comparison of media access control protocols for vehicular ad hoc networks. *IET Networks*, 1(1):10–19, March 2012.

[38] Wei-Yen Lin, Mei-Wen Li, Kun-Chan Lan, and Chung-Hsien Hsu. A comparison of 802.11a and 802.11p for V-to-I communication: A measurement study. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, pages 559–570, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[39] B. E. Bilgin and V. C. Gungor. Performance comparison of IEEE 802.11p and IEEE 802.11b for vehicle-to-vehicle communications in highway, rural, and urban areas. *International Journal of Vehicular Technology*, (971684):10, 2013.

[40] Raj K. Jaiswal and C. D. Jaidhar. An applicability of AODV and OLSR protocols on IEEE 802.11p for city road in VANET. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, pages 286–298, Cham, 2015. Springer International Publishing.

[41] R. Bala and C. R. Krishna. Scenario based performance analysis of AODV and GPSR routing protocols in a VANET. In *2015 IEEE International Conference on Computational Intelligence Communication Technology*, pages 432–437, Feb 2015.

[42] Specification for telecommunications and information exchange between roadside and vehicle systems 5 GHz band dedicated short range communications (DSRC) Medium access control (MAC) and physical layer (PHY) specifications. Technical report, 2010.

[43] IEEE standard for wireless access in vehicular environments (WAVE)-multi-channel operation, IEEE Std 1609.4. Technical report, 2016.

[44] Shuji Tasaka. *Performance Analysis of Multiple Access Protocols*. MIT Press, Cambridge, MA, USA, 1986.

[45] Unnikrishna Pillai S. Papoulis, A. *Probability, random variables, and stochastic processes*. McGraw Hill, New York, USA, 1965.

[46] L. Georgiadis, L. Merakos, and P. Papantoni-Kazakos. A Method for the Delay Analysis of Random Multiple-Access Algorithms Whose Delay Process is Regenerative. *IEEE Journal on Selected Areas in Communications*, 5(6):1051–1062, Jul 1987.

[47] Baum Dieter Breuer, L. *Renewal Theory in: An Introduction to Queueing Theory and Matrix-Analytic Methods*. Springer, Dordrecht, Netherlands, 2005.

[48] Harry Furstenberg. *Recurrence in Ergodic Theory and Combinatorial Number Theory*. Princeton University Press, Princeton, NJ, 1981.

[49] S. Yousefi, E. Altman, R. El-Azouzi, and M. Fathy. Analytical model for connectivity in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 57(6):3341–3356, Nov 2008.

[50] W. R. McShane and R. P. Roess. *Traffic engineering*. Prentice-Hall, Englewood Cliffs, N.J, 1990.

[51] Tony K. Mak, Kenneth P. Laberteaux, and Raja Sengupta. A multi-channel VANET providing concurrent safety and commercial services. In *Proceedings of the 2Nd ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '05, pages 1–9, New York, NY, USA, 2005. ACM.

[52] V. Paxson and S. Floyd. Wide area traffic: The failure of poisson modeling. *IEEE/ACM Transactions on Networking*, 3(3):226–244, Jun 1995.

[53] B. Melander, M. Bjorkman, and P. Gunningberg. A new end-to-end probing and analysis method for estimating bandwidth bottlenecks. In

Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE, volume 1, pages 415–420 vol.1, 2000.

[54] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu. Cloud-assisted safety message dissemination in VANET x2013; cellular heterogeneous wireless network. *IEEE Systems Journal*, 11(1):128–139, March 2017.

[55] S. Ucar, S. C. Ergen, and O. Ozkasap. Multihop-cluster-based IEEE 802.11p and LTE hybrid architecture for VANET safety message dissemination. *IEEE Transactions on Vehicular Technology*, 65(4):2621–2636, April 2016.

[56] A. Benslimane, T. Taleb, and R. Sivaraj. Dynamic clustering-based adaptive mobile gateway management in integrated VANET x2014; 3G heterogeneous wireless networks. *IEEE Journal on Selected Areas in Communications*, 29(3):559–570, March 2011.

[57] J. Calabuig, J. F. Monserrat, D. Gozalvez, and O. Klemp. Safety on the roads: LTE alternatives for sending ITS messages. *IEEE Vehicular Technology Magazine*, 9(4):61–70, Dec 2014.

[58] I. Lequerica, P. M. Ruiz, and V. Cabrera. Improvement of vehicular communications by using 3G capabilities to disseminate control information. *IEEE Network*, 24(1):32–38, Jan 2010.

[59] Communication network vehicle road global extension. Technical report, D-66117 Saarbruecken Germany, 2015.

[60] Connected vehicle pilot deployment program. Technical report, Washington, DC, USA, Fact Sheet, 2015.

[61] X. Ma, X. Yin, M. Wilson, and K. S. Trivedi. MAC and application-level broadcast reliability in VANETs with channel fading. In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 756–761, Jan 2013.

[62] N Etemadi and F Ashtiani. Throughput analysis of IEEE 802.11-based vehicular ad hoc networks. 5:1954 – 1963, 10 2011.

[63] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang. Modeling prioritized broadcasting in multichannel vehicular networks. *IEEE Transactions on Vehicular Technology*, 61(2):687–701, Feb 2012.

[64] S. Khan, M. Alam, N. Müllner, and M. Fränzle. A hybrid MAC scheme for emergency systems in urban VANETs environment. In *2016 IEEE Vehicular Networking Conference (VNC)*.

[65] W. Li, X. Ma, J. Wu, K. S. Trivedi, X. L. Huang, and Q. Liu. Analytical model and performance evaluation of long-term evolution for vehicle safety services. *IEEE Transactions on Vehicular Technology*, 66(3):1926–1939, March 2017.

[66] A. Vinel, D. Staehle, and A. Turlikov. Study of beaconing for Car-to-Car communication in vehicular ad-hoc networks. In *2009 IEEE International Conference on Communications Workshops*.

[67] Disney T. Ott J. Ralph, L. *Networks of Queues, in Applied Probability-Computer Science: The Interface*. Springer Science and Business Media, 1982.

[68] Thomas G. Robertazzi. *Computer Networks and Systems: Queueing Theory and Performance Evaluation*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 3rd edition, 2000.

[69] Fatih Sakiz and Sevil Sen. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks*, 61:33 – 50, 2017.

[70] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. VANEt security challenges and solutions: A survey. *Vehicular Communications*, 7:7 – 20, 2017.

[71] Sunilkumar S. Manvi and Shrikant Tangade. A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications*, 9:19 – 30, 2017.

[72] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design Test*, 34(4):7–17, Aug 2017.

[73] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the performance of IEEE 802.11 under jamming. In *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*.

[74] L. Sang and A. Arora. Capabilities of low-power wireless jammers. In *IEEE INFOCOM 2009*, pages 2551–2555, April 2009.

[75] Ali Hamieh and Jalel Ben-Othman. Detection of jamming attacks in wireless ad hoc networks using error distribution. In *Proceedings of the 2009 IEEE International Conference on Communications*, ICC'09, pages 4831–4836, Piscataway, NJ, USA, 2009. IEEE Press.

[76] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pages 46–57, New York, NY, USA, 2005. ACM.

[77] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pages 1307–1315, May 2007.

[78] A. D. Wood, J. A. Stankovic, and S. H. Son. JAM: A jammed-area mapping service for sensor networks. In *RTSS 2003. 24th IEEE Real-Time Systems Symposium, 2003*, pages 286–297, Dec 2003.

[79] G. Thamilarasu and R. Sridhar. Game theoretic modeling of jamming attacks in ad hoc networks. In *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, pages 1–6, Aug 2009.

[80] X. Li, Y. Zhu, and B. Li. Optimal anti-jamming strategy in sensor networks. In *2012 IEEE International Conference on Communications (ICC)*, pages 178–182, June 2012.

[81] O. Punal and C. Pereira and A. Aguiar and J. Gross. Experimental characterization and modeling of RF jamming attacks on VANETs. *IEEE Transactions on Vehicular Technology*, 64(2):524–540, Feb 2015.

[82] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo. Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks. *IEEE Communications Letters*, 18(1):110–113, January 2014.

[83] S. Biswas and J. Mîsicàand V. Mîsicˇ. DDoS attack on WAVE-enabled VANET through synchronization. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 1079–1084, Dec 2012.

[84] A. Singh and P. Sharma. A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA).

In *2015 2nd International Conference on Recent Advances in Engineering Computational Sciences (RAECS)*, pages 1–5, Dec 2015.

[85] IEEE. IEEE standard for wireless access in vehicular environments (WAVE)-multi-channel operation. IEEE Std 1609.4. Technical report, 2016.

[86] Nadeem Sufyan, Nazar Abbass Saqib, and Muhammad Zia. Detection of jamming attacks in 802.11b wireless networks. *EURASIP Journal on Wireless Communications and Networking*, 2013:208, Aug 2013.

[87] Shekhar Verma Ranjeet Tomar and Geetam Tomar. *Cluster Based RSU Centric Channel Access for VANETs*, pages 150–171. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[88] R. Bansal and P. Papantoni-Kazakos. An algorithm for detecting a change in a stochastic process. *IEEE Transactions on Information Theory*, 32(2):227–235, Mar 1986.

[89] A. T. Burrell and P. Papantoni-Kazakos. On-line learning and dynamic capacity allocation in the traffic management of wireless ATM networks. In *Universal Personal Communications, 1998. ICUPC '98. IEEE 1998 International Conference on*, volume 2, pages 1063–1066 vol.2, Oct 1998.

[90] Fatma Salem, Anthony T. Burrell, and P. Papantoni-Kazakos. Dynamic architectural reconfigurations of sensor networks. In *IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society*, pages 1117–1122, Nov 2010.

[91] Fatma Salem, Anthony T. Burrell, and P. Papantoni-Kazakos. Dynamic architectural reconfiguration algorithms and transmission protocols for clustered sensor network topologies with prioritized data. *ISRN Sensor Networks*, 2012:17, 2012.

[92] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2006.

[93] Fatma Salem, Yassin elhillali, and Smail Niar. Efficient modeling of IEEE 802.11p MAC output process for V2X interworking enhancement. *IET Networks*, Feb 2018.