Contribution to the Intelligent Transportation System : security of Safety Applications in Vehicle Ad hoc Networks

Huong Nguyen-Minh

UNIVERSITY OF AVIGNON

DOCTORAL THESIS

Contribution to Intelligent Transportation Systems: Security of Safety applications in Vehicular Ad hoc Networks

Author:
NGUYEN Minh Huong

Supervisor:
Abderrahim BENSLIMANE

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

Laboratoire Informatique d'Avignon

September 29, 2016

Declaration of Authorship

I, NGUYEN Minh Huong, declare that this thesis titled, "Contribution to Intelligent Transportation Systems: Security of Safety applications in Vehicular Ad hoc Networks" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

Abstract

Doctor of Philosophy

Contribution to Intelligent Transportation Systems: Security of Safety applications in Vehicular Ad hoc Networks

by NGUYEN Minh Huong

The development of transportation all over the world has been providing a lot of benefits for many aspects of human life. Intelligent Transportation Systems (ITS) are advanced applications that aim to make the transport networks safer, more convenient and smarter. According to their usages, they can be classified into two types of ITS applications, which are safety applications and non-safety applications.

Vehicular ad hoc network (VANET) is a key component of ITS since it enables communications among transportation units. These communications support different ITS applications with various properties. Between two types of applications, we are interested in safety applications which have tighter quality and security constraints. Depending on an applied scenario of a given safety application, the exchanged information among vehicles must be broadcast locally within one-hop communication and/or also be notified to vehicles in large range. The main objective of this thesis is to improve the performance of safety applications in term of the quality of service and security, in both one-hop communication and multi-hop communication. We focus on reliability, connectivity and Denial of Services (DoS) attack. We study and propose technical solutions coming from lower layers (Physical, MAC and network layers) which play a fundamental role in mitigation to challenges created by the nature of the vehicular environment.

Mainly, our contributions are three folds. Firstly, we consider efforts to enhance the reliability for communication in vehicular networks. These efforts are represented by proposed protocols aiming to assure the delivery of messages to recipient(s). Focusing on safety applications, we propose a reliable scheme to achieve the reliability for broadcasting. In our scheme, the safety messages are rebroadcast when the sender is requested. Our analysis shows that the implementation of our scheme in the standard IEEE 802.11p increases the percentage of vehicles receiving the messages while duplicated messages are limited compared to other related works. Secondly, we consider the fragmentation of the network. We study solutions that overcome the temporary disconnection in the network to bring the safety information to the recipients. Based on the social properties of vehicular networks, we propose a social-based forwarding protocol to support the communication between vehicles to points of interest that provide safety services with looser time constraints, such as search and rescue. Our

protocol outperforms in the studied scenario of poor connectivity. Finally, we investigate threats for safety applications in vehicular networks. Specially, we investigate jamming attack, a kind of DoS attacks, which is crucial for safety applications because of the adequate condition of the attack at the lower layers. We model jamming attack on broadcasting in order to study the degradation caused by the attack on network performance. The degradation at a certain level in network performance is an indication of a jamming attack presence in the network; therefore results from this analysis will allow us to determine network performance thresholds to distinguish between normal and attacked scenarios. However, according to our analysis, the method using the degradation as an indication to detect a jamming attack is not feasible for real-time applications. Hence, we propose methods to detect jamming attacks in real-time. Our methods allow real-time detection with high accuracy, not only at the central monitor but also at each vehicle. Therefore, vehicles are noticed about the attack soon enough to recover the communication and react for their safety.

Acknowledgements

I would like to express my deep gratitude to Prof. Abderrahim Benslimane for all his help, support and kindness during the course of my PhD.

I would like to thank the Laboratoire Informatique d'Avignon (LIA), the university of Avignon and the University of Science and Technology of Hanoi for sponsoring my PhD.

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

I would like to send special thanks to my family, my love and my friends for always being by my side.

Contents

Declaration of Authorship iii

Abstract v

Acknowledgements vii

1 Introduction 1
- 1.1 Motivations . . . 1
- 1.2 Research Methodology . . . 3
- 1.3 Thesis Contributions . . . 4
- 1.4 Thesis Structure . . . 5

2 Overview of ITS and Vehicular Ad hoc Networks 7
- 2.1 ITS Applications . . . 8
- 2.2 ITS Architecture and Vehicular Networks domain . . . 9
- 2.3 Enabling communication technologies . . . 12
  - 2.3.1 DSRC spectrum allocation . . . 12
  - 2.3.2 WAVE protocol stacks . . . 13
- 2.4 Challenges for communication in vehicular environment . . . 16
- 2.5 Fundamental protocols for vehicular networks . . . 17
  - 2.5.1 Medium access control protocols . . . 17
    - The standard 802.11p and Multichannel operation IEEE 1609.4 . . . 17
    - Concerns when designing MAC protocol in VANETs . . . 21
    - Proposed MAC protocols in VANETs . . . 22
  - 2.5.2 Multi-hop communication protocols in vehicular networks . . . 23
    - Challenges in multi-hop communication in VANETs . . . 24
    - Proposed multi-hop communication approaches for safety applications . . . 24
  - 2.5.3 Security in vehicular networks . . . 28
    - Wireless attacks in VANETs . . . 28
    - Security requirements . . . 30
    - Security proposals for vehicular networks . . . 31
- 2.6 Open issues on improving performance of safety applications . . . 33

3 Reliability in broadcasting for safety applications in Vehicular Networks 35
3.1 State of the art . . . 36
3.1.1 Problem Statement . . . 36
3.1.2 Reliable protocols for broadcasting in vehicular networks . . . 36
3.1.3 How to provide the reliability for safety applications? . . . 39
3.2 Polling scheme for reliable broadcasting . . . 42
3.3 Proposed polling scheme analysis . . . 46
3.3.1 Assumptions . . . 46
3.3.2 Basic model . . . 47
Probability of successful transmission . . . 48
Probability of failed transmissions . . . 49
Number of successful messages . . . 50
3.3.3 Extended model for prioritized broadcasting . . . 52
3.4 Reliable MAC protocol in dissemination of safety messages . . . 54
3.4.1 Local operation . . . 55
3.4.2 Forwarding mechanism . . . 56
3.4.3 Effect of MAC protocol to dissemination performance . . . 57
3.5 Performance Evaluation of proposed polling scheme . . . 59
3.5.1 One-hop communication . . . 60
3.5.2 Dissemination in urban and highway scenarios . . . 63
3.6 Conclusions . . . 66

4 Connectivity enhancement for safety applications in vehicular networks 69
4.1 Opportunistic forwarding approaches in Vehicular networks . . . 70
4.1.1 Overview of opportunistic forwarding protocols in VANETs . . . 70
4.1.2 Social aspect of vehicular networks . . . 71
Social properties of vehicular networks . . . 71
Utilizing social metrics in forwarding protocols in VANETs . . . 73
4.2 Social-aware forwarding approach for safety services in Vehicular network (SocVe) . . . 73
4.2.1 Beacon and SocVe header design . . . 74
4.2.2 Forwarding process . . . 75
4.3 Experiment Setup . . . 78
4.3.1 City map . . . 78
4.3.2 Connectivity analysis . . . 79
4.4 Simulation Results for the studied experiment . . . 81
4.5 Conclusions . . . 84

5 Security of safety applications against jamming attacks in Vehicular Networks 85
5.1 Jamming attacks in Vehicular Networks . . . 86
5.1.1 Classification of jamming attacks in Vehicular networks . . . 86
5.1.2 Related works and open issues of jamming detection for beacons 87

5.1.3 Our contributions . . . 88
5.2 Modeling reactive jamming attack for broadcasting in vehicular networks 90
5.2.1 Jamming model at MAC layer . . . 90
5.2.2 Physical parameters . . . 92
Radio Propagation Loss Model . . . 94
Vehicle Distribution . . . 95
5.2.3 Threshold determination . . . 96
5.2.4 Is threshold-based detection method feasible for real-time applications? . . . 97
5.3 Real-time Jamming Detection Method for beacons in Vehicular Networks 100
5.3.1 Contention Collision-Jamming Differentiation detection method (CJD) . . . 100
Jamming detection algorithms . . . 100
Proposed detection method analysis . . . 104
Distributed Detection Method (D-CJD) . . . 107
Performance Evaluation of the proposed detection method (CJD) 110
5.3.2 Contention-Jamming-Interference Differentiation detection method (CJID) . . . 112
5.4 Simulation Results . . . 113
5.4.1 Platoon scenario . . . 114
5.4.2 General scenarios . . . 116
5.5 Conclusions . . . 118

6 Thesis Conclusions **121**
6.1 Summary of Contributions . . . 121
6.2 Future works . . . 123

A Dissemination Improvement as a function of MAC and topology parameters **125**

B The over estimation of number of neighbors impacts precision of CJD **127**

Bibliography **129**

List of Figures

2.1 Intelligent Transportation Systems and Vehicular Communication Networks . . . 8
2.2 The National ITS Architecture Layers - United State Department of Transportation . . . 10
2.3 Types of Communications in ITS architecture . . . 10
2.4 DSRC allocated spectrum . . . 12
2.5 WAVE protocol architecture . . . 14
2.6 Relationship of ETSI ITS station reference architecture to OSI reference model and WAVE protocol architecture . . . 15
2.7 Backoff procedure in CSMA/CA . . . 18
2.8 Scheme of EDCA derived from WAVE standard IEEE 1609.4-Multichannel operation . . . 19
2.9 Channel cordination: alternating access . . . 20
2.10 Classification of multi-hop communication protocols in vehicular networks . . . 25
2.11 Vehicular wireless communication Attack classification . . . 29
2.12 Objective-based classification . . . 30

3.1 Classification of reliable MAC protocols . . . 37
3.2 BC and Poll frame format . . . 42
3.3 Proposed polling scheme implemented in CSMA . . . 44
3.4 Operation of devices implementing polling scheme . . . 45
3.5 Four Access Catergories and Access zones . . . 53
3.6 The effects of reliable MAC protocol to dissemination protocol . . . 58
3.7 Analytical Model Validation . . . 60
3.8 One hop communication no hidden nodes . . . 61
3.9 One hop communication under impact of hidden nodes . . . 62
3.10 Performance of dissemination protocol implementing polling scheme in highway scenario . . . 64
3.11 Performance of dissemination protocol implementing polling scheme in urban scenario . . . 66

4.1 Formats of SocVe frames . . . 75
4.2 Extracted map of Hanoi . . . 78
4.3 Centrality of Points of Interest (PoIs) . . . 79
4.4 Topology Analysis . . . 80

4.5 SocVe Success Ratio versus PoI Centrality 82
4.6 Success Ratio SocVe, DAER, Epidemic protocol 83
4.7 Average Delay SocVe and DAER 83

5.1 Mean PDR in normal scenario $\rho_a = 0$ and jammed scenario $\rho_a > 0$ 96
5.2 The influence of jamming probability, distance of jammer on PDR at the receiver 97
5.3 Analytical jamming model validation 98
5.4 Analytical Threshold and Simulation Results 99
5.5 Detector Operation 101
5.6 Observation Process 102
5.7 Impact of wrong estimation on detection probability 106
5.8 Probability of false alarms due to wrong estimation 108
5.9 The influence of detection probability on attack probability 110
5.10 The influence of detection probability on number of vehicles 111
5.11 The influence of detection probability on contention window size 111
5.12 Detection Probability and False Alarm Probability 115
5.13 Detection probability and false probability in scenario 1 group of 10 vehicles 116
5.14 Detection Probability and False Alarm Probability of CJD and CJID in scenarios of 2 groups and 3 groups of vehicles 118

List of Tables

2.1 Four Access Categories 20

3.1 Proposals for reliable broadcast 38
3.2 Probabilities descriptions 49
3.3 Simulation Parameters 59

5.1 Probabilities denotes 91
5.2 Parameters in analytical model 98
5.3 Parameters in Simulations 114

List of Abbreviations

AIFS	Arbitration Interframe Space
BSS	Basic Service Set
CCA	Clear Channel Assessment
CCH	Control Channel
CCHI	Control Channel Interval
CSMA	Carrier Sense Multiple Access
DCF	Distributed Coordination Function
DIFS	DCF Interframe space
DSRC	Dedicated Short Range Communications
DTN	Delay Tolerant Networking
EDCA	Enhance Distributed Channel Access
ITS	Intelligent Transportation System
NAV	Network Allocation Vector
OBU	On-board Unit
RSU	Roadside Unit
SCH	Service Channel
VANETs	Vehicular Ad hoc NETworks
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisements

Publications

1. Nguyen-Minh, Huong, Abderrahim Benslimane, and Der-Jiunn Deng. "Reliable broadcasting using polling scheme based receiver for safety applications in vehicular networks." Vehicular Communications Journal Vol. 4 (2016), Elsevier Publisher, pp. 1-14.

2. H. Nguyen-Minh, A. Benslimane, "'Polling Scheme for Reliable Broadcasting in Vehicular Networks"', accepted be presented and published at IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium ('ICC'14 AHSN'), 9-13 June.

3. Nguyen-Minh, Huong, Abderrahim Benslimane, and Milena Radenkovic. "Social delay tolerant approach for safety services in vehicular networks."Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, 2015.

4. Nguyen-Minh, Huong, Abderrahim Benslimane, and Abderrezak Rachedi. "Jamming detection on 802.11p under multi-channel operation in vehicular networks." Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, 2015.

Chapter 1

Introduction

The growth of economy and mobility requirements of citizens, associated with the increase in the volume of road transport in the cities all over the world, is the main cause of increasing traffic congestion, energy consumption, source of environmental and social problems, as well as damages and loss from road accidents. It is innovative for human life to create advanced applications which aim to provide services relating to different modes of transport and traffic management, making transport networks more safer, more coordinated and smarter. Hence, Intelligent Transportation System (ITS) and its enabling technologies are proposed and globally discussed. Frameworks for ITS deployments are officially adopted in different countries in recent years. According to EU Directive 2010/40/EU (7 July 2010), ITS is expected to make a significant contribution to the improvement of environmental performance, efficiency such as energy efficiency, safety, and security of road transport such as the transport of dangerous goods, public security and passenger, and freight mobility.

Intelligent Transportation Systems (ITS) are systems in which information and communication technologies are applied in order to efficiently and safely use the transport infrastructure and means of transportation (cars, trains, planes, ships). Although ITS may refer to all modes of transport, many standardized documents are dedicated to the road transport context. Elements of ITS are standardized by various international organizations in the European Standard ETSI EN 302 665 (2010-09) [31], the suit of standards IEEE 1604, ISO TC204, etc.. Among these elements, wireless communication including various enabling technologies plays the key role in deploying ITS.

1.1 Motivations

Vehicular ad hoc network plays a role of wireless communication technology supporting ITS in the domain of vehicles. It provides inter-networking technologies for direct vehicles to infrastructure (V2I) and vehicles to vehicles (V2V) communications. Before bringing ITS to real life, enabling technologies should be well studied. Various vehicular network projects and consortia have been launched in Europe such as Car to Car Communication Consortium (C2C-CC), COOPERS, CyberMove, etc., in the US such as VSC, CAMP/VSC-2, etc., in Japan e.g. SmartWay. They discuss and evaluate standardized protocols and parameters, testing ITS applications in different scenarios.

However, characteristics of vehicular environment always create challenges. A wide range of applications and usage scenarios requires for enhancements in standardized protocols and security in vehicular networks before implementing in daily life.

The broadcast communication mode of safety applications causes difficulties in designing medium access control and networking protocol, as well as threats of wireless attacks. The existing standardized protocols have not solved all the problems in broadcasting while broadcasting is the main communication mode in vehicular networks. Moreover, in order to support applications in ITS, typical exchanged messages among vehicles, namely beacons, are used to maintain the cooperation among vehicles. They are prone to become new targets for wireless attacks, especially attacks at low layers such as jamming attacks.

From the point of view of the communication network, we evaluate the performance of a safety application by three criteria which are reliability, connectivity, and security. The reliability regards to the ability to deliver data to predefined recipient(s). The connectivity criterion refers to how the safety information is delivered to the recipient(s) when the connectivity in the network is not always available. Finally, the security criterion of a safety application reflects the protection of the application against threats of attacks in the network.

In this thesis, we investigate medium access control protocols, networking protocols, and jamming attacks with the aim to enhance the performance of safety applications in vehicular networks in terms of reliability, connectivity, and security. Regarding to the reliability, the standardized MAC protocol has not specified any technical solution to assure the delivery of broadcast messages. However, this is important for safety applications because vehicles should receive vital information in broadcasting manner with high reliability. Therefore, firstly, we propose a polling scheme to make the broadcasting more reliable so that more vehicles can receive critical information in time to react. Besides urgent information exchanged among vehicles locally, there is also other safety-related information that needs multi-hop communication to deliver this information to distant vehicles. Due to the fragmentation in vehicular networks, the multi-hop communication has to deal with the temporary disconnection problem. Based on the inherited social features of mobile networks, social characteristics can be used to overcome this problem in vehicular networks. Thus, secondly, we introduce a social delay tolerant approach for vehicular networks, especially, for some kinds of safety applications. In these kinds of safety applications, important but less urgent information is forwarded from vehicles to one or some special entities (for example, police cars or emergency vehicles) whose positions are unknown. Last but not least, because of the importance of basic safety messages (beacons), they are vulnerable to wireless attacks at lower layers. It remains security issues such as modeling, detecting and reacting to this threat. Hence, we study and introduce a detection method for jamming attacks on beacons in vehicular networks. Since every vehicle has its own beacon to transmit, there will be contention to access the medium before transmitting,

the medium access contention is the main concern when we study the broadcasting in vehicular networks. Moreover, the performance of the communication among vehicles is impacted by physical parameters, e.g. propagation loss and vehicle distribution. Hence, we study the jamming attacks on broadcasting with consideration of both medium access contention and physical parameters. To the best of our knowledge, it is the first time that these characteristics are taken into account together in the studies of jamming attacks in vehicular network.

1.2 Research Methodology

We report and classify related works in vehicular networks. The existing works can be categorized based on their aims (what aspects they want to improve), their objectives (what kind of applications, unicast or broadcast, one-hop or multi-hop communication) and the parameters or metrics that they use in their protocols to deal with the problem. This draws a big picture of technical solutions for safety applications in vehicular networks.

We study our proposed protocols in analytical models, and then implement them into network simulator to validate the numerical results obtained from analytical models. Based on the analytical analysis, we can also evaluate the standard protocols so that we can compare our proposals to the standards. Parameters used in the analytical models are chosen from the reference values in standards. All computations in analytical models are conducted in Matlab software that allows analyses on large data sets.

Concurrently, simulations are carried on in a discrete-event network simulator, NS-3. Behaviors of vehicles and respective events are simulated. The mobility of vehicles in our simulations is generated in Simulation of Urban Mobility (SUMO) (a road traffic simulation package) and/or collected from real data traces. Simulations allow us to validate the analytical results and also investigate our proposals in different scenarios on which different mobility data sets and radio channel models can be integrated. In our simulations, we consider the characteristics of wireless access medium on vehicular environments such as the propagation loss models, modulation mode, operating frequency and other parameters specified in the standard IEEE 802.11p.

We implemented our proposals at corresponding network layers in NS-3. In our first contribution on reliable broadcasting, our polling scheme is implemented at MAC layer. Our second proposal on social-inspired forwarding is implemented at networking layer in NS-3. Finally, jamming attack and our proposed detection method are implemented by new objects added to NS-3. In the simulation, we studied jamming attacks and our detection method in platoon scenario and general scenario.

1.3 Thesis Contributions

The thesis contributes to the field of safety applications in vehicular ad hoc networks. It provides a big picture of technical solutions to enhance the performance of safety applications in terms of reliability, connectivity, and security. In each of these criteria, we propose models, protocols, and methods to analyze existing problem. Correspondingly, our three contributions in this thesis are resumed as follows:

Firstly, we improve the reliability of broadcasting in vehicular networks by implementing an additional scheme, a polling scheme, to the standard IEEE 802.11p. Safety-related information is retransmitted to assure that all concerning vehicles in vicinity area receive the information. Our scheme is investigated with analytical analysis and simulations in urban and highway scenarios. Moreover, due to the fact that safety applications require the cooperation of local communication and dissemination, we also study our polling scheme as an under layer protocol of a dissemination protocol. The impact of the enhanced MAC protocol on dissemination is analyzed.

Secondly, in order to mitigate the network fragmentation and motivated by the social feature of vehicular networks, we propose a Social delay tolerant forwarding approach in Vehicular networks (SocVe) for a kind of safety applications that requires high delivery rate but tolerant delay. We design our protocol with consideration of vehicular environment characteristics and constraints of safety applications so that suitable social metrics are chosen.

Finally, we investigate the threat of jamming attacks in the context of vehicular environment. Periodically exchanged safety messages among vehicles, called beacons, are vulnerable to this kind of attacks while there are only a few studies on this topic. We introduce a novel analytical model in order to investigate the impact of jamming attack on broadcasting. We show that the degradation at a certain level in network performance is an indication of a jamming attack in the network; therefore results from this analysis will allow us to determine network performance thresholds to distinguish between normal operation and attacked scenario (threshold-based detection methods). Our study is dedicated for broadcasting. We especially consider the medium access contention that is a strike characteristic of beacon broadcasting. We also study the feasibility of the existing threshold-based methods to detect jamming in real-time applications. From our analysis, these methods are not suitable for safety applications. Hence, we propose a real-time and MAC-based detection method to meet the requirement of time in safety applications in vehicular networks. Our detection method can more accurately distinguish the causes of failed transmissions such as contention collisions, interferences, and jamming attacks. The jamming attacks are detected with a low probability of false alarms. Our detection method is evaluated with both analytical analysis and network simulations. It performs high detection probability in different studied scenarios while false alarms are almost avoided.

1.4 Thesis Structure

The remainders of the thesis is organized as follows:

Chapter 2 describes the background of our research areas. It firstly discusses the overview of vehicular networks which play a role of wireless communication technology supporting ITS. Disciplines of Wireless Access in Vehicular Environments (WAVE) are described in this chapter. The chapter presents expected applications and architecture of WAVE followed by enabling technologies proposed for vehicular networks. Characteristics of vehicular environments produce challenges on designing protocols for WAVE, especially for safety applications in WAVE. These difficulties, fundamental protocols, and open issues on improving quality of service and security of safety applications are discussed also in this chapter.

Chapter 3 discusses the reliability for broadcasting in vehicular networks. Our polling scheme is presented and analyzed in this chapter. After that, we describe how our polling scheme is integrated into a position-based dissemination protocol in order to support both reliability in local communication area and in a large communication area. The chapter also raises a discussion of the impact of a general reliable MAC protocol on dissemination.

Chapter 4 is dedicated to a discussion on protocols that deal with temporary disconnection to forward messages in vehicular network. The chapter also describes social properties of vehicular networks which are the basis to analyze our proposed social-aware forwarding protocol. Then, our analysis of connectivity in the studied scenario and the corresponding performance of our proposed protocol are elaborated.

Chapter 5 presents our core contribution in the field of security for safety applications in vehicular networks. Firstly, a classification of jamming attacks and detection methods are briefly discussed. Secondly, the impact of jamming attacks on beacons is studied in our proposed analytical model which adopts characteristics of vehicular environment. The study provides reference values for threshold-based detection method. Thirdly, our real-time detection method aiming to overcome shortcomings of threshold-based detection method is elaborated. The analytical analysis and simulation results to evaluate our method in platoon scenario and general scenario are presented.

Chapter 6 concludes the thesis. All thesis contributions, methodology, and main results are briefly resumed. To extend and improve our works, future works are discussed at the end of the chapter.

Chapter 2

Overview of ITS and Vehicular Ad hoc Networks

The communications among vehicles and vehicles-to-infrastructure enable the ability to provide the safety, efficiency and convenience in transportation systems. Accordingly, safety applications and non-safety applications (including applications supporting convenience and efficiency) have been being innovated. In this chapter, we outline an appropriate architecture of ITS for road transport and localize the domain of vehicular networks in the ITS architecture. The overview of ITS applications is also resumed. We generally discuss fundamental protocols that are standardized or proposed by existing works. Some problems, which impact on the operation of safety applications, have not been resolved by the existing works, thus, the need of improving the quality and security of safety applications still remains.

ITS has been developed throughout the world. Standardization organizations all over the world have included some aspects of ITS and its communication technologies in their charters. There is a list of international ITS standards including the family of IEEE 1609 standards, standards of European Telecommunication Standard Institute (ETSI), International Organization for Standardization (ISO), European Committee for Standardization (CEN) and so on. Various ITS applications and enabling communication technologies are specified in these standards. We would like to emphasize that vehicular network is one domain of communications for ITS. Where the domain of vehicular networks is positioned in ITS architecture will be clarified in this chapter. Mainly, we focus on vehicular domain (vehicular communication networks) on which vehicle-to-vehicle communication and vehicle-to-infrastructure communication are direct, in other words, we are working on Vehicular Ad-hoc Networks (VANETs).

The rest of this chapter is structured as follows: in section 2.1, applications and ITS projects are briefly described. Section 2.2 shows the overview of ITS architecture and position of VANETs in this ITS architecture. Section 2.3 describes the current state of standards for VANETs. Section 2.4 lists out challenges of vehicular environments. Section 2.5 provides taxonomies of fundamental protocols proposed by existing works. The last section discusses open issues on supporting safety applications with high reliability in fragmented networks and against wireless attacks.

2.1 ITS Applications

An ITS scenario is illustrated in Fig.2.1. ITS applications are very various, ranging from safety-related applications that aim to avoid vehicular crashes, alert danger road situation, to traffic efficiency applications that help to reduce congestion in road transport system, and other applications that provide convenience for transportation system users, environment-friendly driving applications, electronic payments-tolling, etc.. According to their purposes, they can be classified into two types: safety applications and non-safety applications. In this thesis, we focus on safety applications.

Applications in ITS are supported by several communication technologies including existing infrastructure communications and Dedicated Short Range Communication (DSRC) that provides inter-vehicle communication (Vehicle-to-Vehicle, V2V) and Vehicle-to-Roadside communication (Vehicle-to-Infrastructure, V2I).

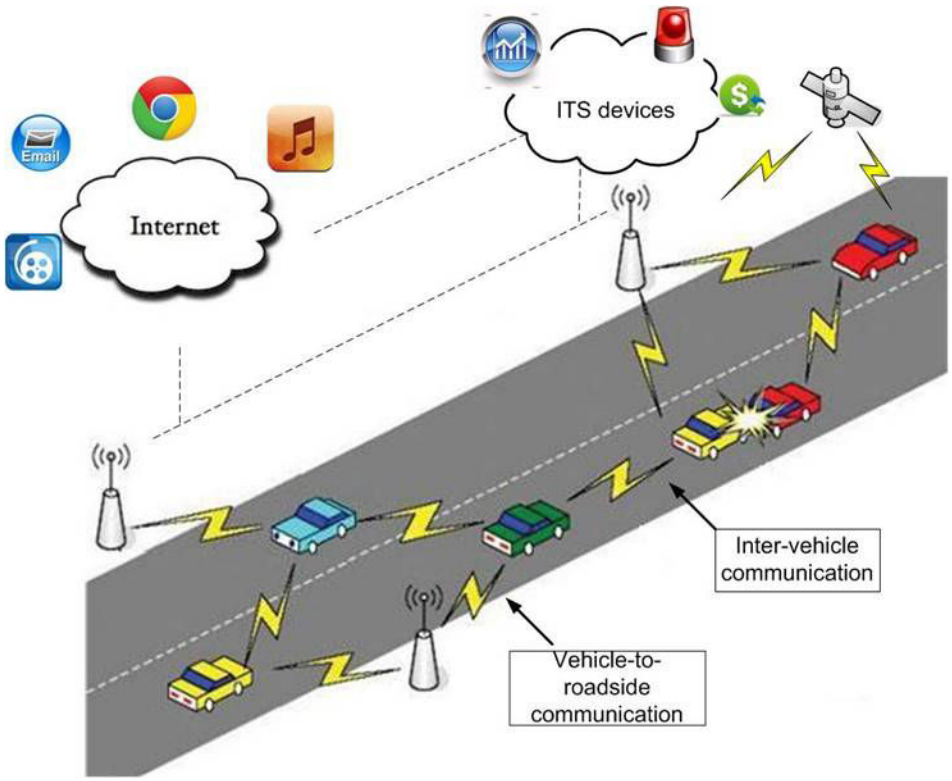


FIGURE 2.1: Intelligent Transportation Systems and Vehicular Communication Networks

Consortia and projects [83] around the globe have been developing lists of safety applications in vehicular networks. Vehicle Safety Communication-Application Project selected six safety applications to address top seven crash scenarios: Emergency electronic brake lights, forward collision warning, blind spot warning and lane change warning, do not pass warning, intersection movement assist, and control loss warning. The Vehicle Safety Communications Consortium (VSCC) of CAMP have identified eight such applications (CAMP VSCC 2006) which are divided into two groups:

the near-term applications are traffic signal violation warning, curve speed warning, and emergency electronic brake lights; the mid-term applications are pre-crash warning, cooperative forward collision warning, left turn assistant, lane change warning, and stop sign movement assistance. Car to Car Communication Consortium (C2C-CC) develops a European Industry standard for vehicular communication (VC) systems, active safety applications prototyping and demonstrations, harmonization of VC standards worldwide, realistic deployment strategies and business models. CyberCars2 and CyberMove investigate cooperation between vehicles running at close range in different transportation systems.

According to mentioned above consortia and projects, safety applications can be classified by their usage scenarios or priority. Besides, they can be classified into two types according to their operation range: one-hop and multi-hop applications. The exchanged information may be concerned by only neighboring vehicles such as information of location, velocity of vehicles and local road condition included in periodically exchanged messages (beacons). This type of safety applications requires only one-hop communication. Otherwise, the information may be useful for distant vehicles to warn them about hazardous events. Therefore, multi-hop communication is important for this type of safety applications.

In ITS, vehicles should be equipped novel facilities to collect information of surround environment. Therefore, besides communication technologies, vehicular positioning, vehicular sensors and on-board computation platforms are also enabling technologies for cooperative driving systems [41]. However, they are out of the scope of the thesis, communication aspect of ITS is our interest.

2.2 ITS Architecture and Vehicular Networks domain

The National ITS Architecture is introduced in the United States ITS program which was created by Congress in the Intermodal Surface Transportation Efficiency Act of 1991, and is administered by the U. S. Department of Transportation (DOT). The program uses advanced electronics to improve traveler safety, decrease traffic congestion, facilitate the reduction of air pollution, and conserve vital fossil fuels.

The National ITS Architecture provides a common framework for planning, defining, and integrating intelligent transportation systems. The architecture defines functions that are required for ITS, physical entities or subsystems where these functions reside, and information flows and data flows that connect these functions and physical subsystems. The architecture framework is described in Fig.2.2. It is comprised of three layers including the Institutional Layer and two technical layers which are Transportation Layer and Communication Layer.

The Institutional Layer includes the institutions, policies, funding mechanisms, and processes that are required for effective implementation, operation, and maintenance

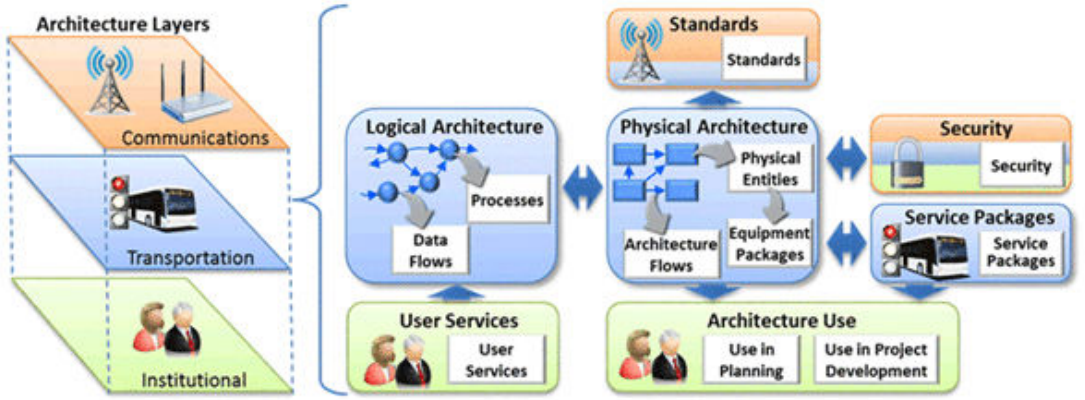


FIGURE 2.2: The National ITS Architecture Layers - United State Department of Transportation

of an intelligent transportation system. The Institutional Layer is shown as the base because solid institutional support and effective decisions are prerequisite to an effective ITS program. This is where the objectives and requirements for ITS are established.

The Transportation Layer is where the transportation solutions are defined in terms of the subsystems and interfaces, the underlying functionality, and data definitions that are required for each transportation service.

The Communications Layer provides the accurate and timely exchange of information between systems to support the transportation solutions. Hence, vehicular networks belong to this layer. At Communications Layer, four communication types are identified to support different communications among ITS subsystems and entities. These are field-vehicle (vehicle-infrastructure) and vehicle-vehicle communications that make up vehicular networks domain, fixed point-fixed point and wide area wireless communications, shown in Fig. 2.3.

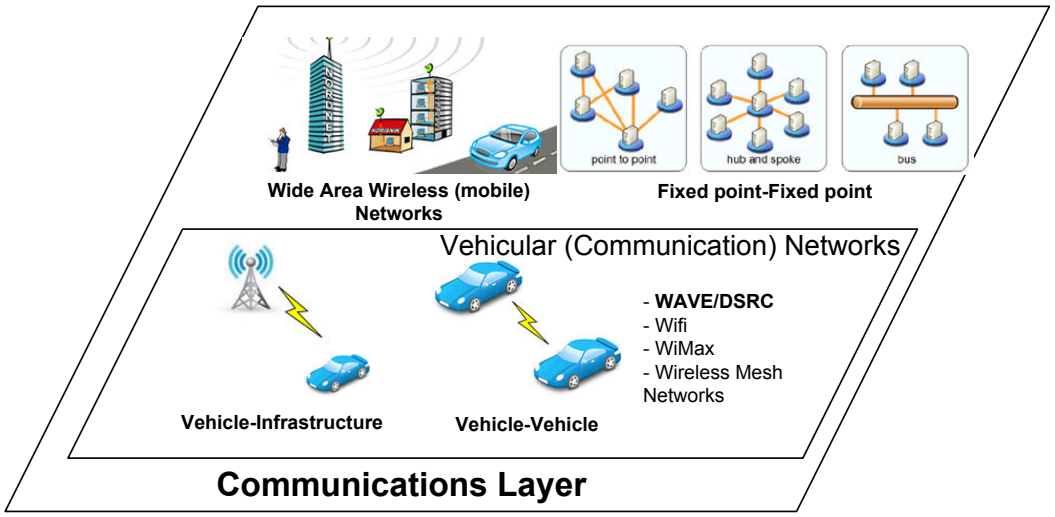


FIGURE 2.3: Types of Communications in ITS architecture

According to National ITS architecture, these four types of communication are briefly described as follows:

Field-Vehicle Communications are wireless communications used for broadcast and interactive communication between vehicle and infrastructure units. They support location-specific and situation relevant communications for ITS capabilities such as toll collection, transit vehicle management, driver information, and automated commercial vehicle operations as well as connected vehicle applications. This communication channel is supported by technologies such as 5.9 GHz Band Wireless Access in Vehicular Environments (WAVE) / Dedicated Short Range Communications (DSRC), Wi-Fi, WiMAX, and wireless mesh networks.

Vehicle-Vehicle Communications are short range wireless communications among vehicles. They support a wide range of applications such as advanced collision avoidance, road condition notifications, and cooperation between advanced vehicle control systems. WAVE/DSRC is the enabling technology for this inter-vehicle communication.

Fixed point- Fixed point Communications provide communications among stationary entities. A variety of public or private communication networks and technologies are used when this type of communications is implemented. They support a variety of maintenance, monitoring and management services. The communication can include, but is not limited to, twisted pair, coaxial cable, fiber optic, microwave relay networks, spread spectrum, etc. Any physical network topology (including all three provided examples in Fig.2.3) that can support the identified information transfers is consistent with the communications layer and the National ITS Architecture.

Wide Area Wireless (Mobile) Communications offer broad coverage, enabling communications with vehicles and traveler mobile devices at any location on or off the road network. Both broadcast (one-way) and interactive (two-way) communications services are grouped into wide-area wireless communications in the National ITS Architecture. These links support a range of services in the National ITS Architecture including real-time traveler information and various forms of fleet communications. Technologies supporting this type of links include cellular networks, WiMAX, wireless mesh networks, and any other wireless network technology that offers broad regional coverage.

Communication in vehicular networks is one domain of ITS communication. It includes the first two types of communications: vehicle-to-vehicle communication and vehicle-to-infrastructure communication. Besides infrastructure-based wireless network technologies, direct communications in vehicular ad hoc networks are vital networking technologies for the ITS implementation. In this thesis, we work on vehicular (communication) networks which is one domain of ITS communication. We especially focus on vehicular ad hoc networks which support direct communications between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The other two communications types in ITS communication architecture (fixed point-fixed point and Wide Area

Wireless Communications) are out of the scope of this thesis.

ITS standards have been developed for corresponding entities in the ITS architecture. The IEEE WAVE standards including the family standard IEEE 1609 and DSRC are specified to provide communications between vehicle and infrastructure, and communications among vehicles. The WAVE standards provide a guideline of protocols which are necessary for the operation of WAVE devices, while DSRC is often referred to the radio spectrum at 5.9 GHz band or technologies associated with WAVE. Concurrently, ETSI TC ITS presents European Standards for ITS communications in ETSI EN 302 665 (2010-09) [31]. In the next section, communication standard protocols and related works on WAVE will be elaborated. The section also discusses challenges in designing protocols for vehicular environment and open issues that should be solved before deploying safety applications in ITS.

2.3 Enabling communication technologies

2.3.1 DSRC spectrum allocation

DSRC, a two-way short-to-medium-range wireless communications, permits very high data transmission critical in communication-based active safety applications. The Federal Communication Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band for ITS vehicle safety and mobile applications. DSRC enables V2V, V2I communications in ITS.

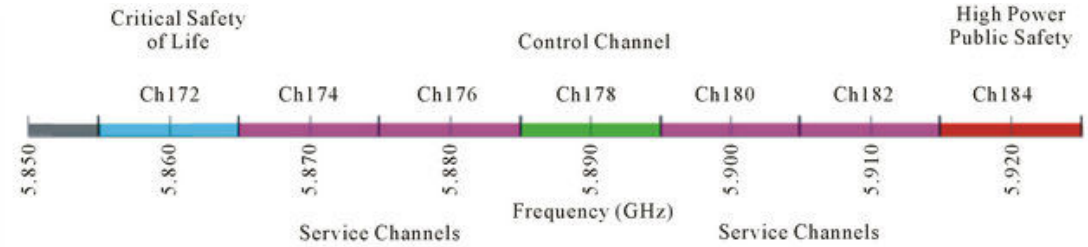


FIGURE 2.4: DSRC allocated spectrum

The spectrum of the 5.9 GHz band is from 5.85 GHz to 5.925 GHz as illustrated in Fig.2.4 . The lower 5 MHz is reserved as a guard band. The remaining 70 MHz is divided into seven 10 MHz channels, from channel 172 to 184. In the U.S., channel 178 is assigned for exchanging management information including WAVE Short Message (WSM) and WAVE Service Advertisements (WSA). It is called control channel (CCH). Other channels are service channels.

The FCC further designated service channels 172 and 184 for specific purposes. Channel 172 and Channel 184 are designated for public safety applications involving the safety of life and property. Specifically, according to FCC 06-110 [B8], channel 172 is for "vehicle-to-vehicle safety communications for accident avoidance and mitigation, and safety of life and property applications;" Channel 184 is for "high-power, longer

distance communications to be used for public safety applications involving safety of life and property, including road intersection collision mitigation.". While according to the standard SAE J2735 DSRC, the basic safety messages which vehicles attach their instant states in are managed to be transmitted in CCH. WAVE standards specify the use of the CCH for WSA broadcast, and preclude IP traffic on the CCH, but otherwise do not specify how the various channels are used. It means that no safety channel is specified and any SCH can be configured to be safety channel. Whatever channel is chosen as a safety channel, ITS devices need the concurrent alternating operation on more than one channel to support both safety applications and non-safety applications. Hence, channel switching or multichannel operation is always adequate.

2.3.2 WAVE protocol stacks

As DSRC is an interest in different countries, standards are also specified by professional organizations all around the world such as ETSI with European Standards for ITS, International Organization for Standardization with the standard Communication Access for Land Mobiles (CALM). The WAVE standards are specified with association with DSRC in the U.S. Though the specific meaning of terms and implementation model vary from standard to standard, they have centered on an architecture that has the common concept. The concept is that applications are supported by all lower communication layers. In this section, we describe the architecture as the WAVE protocol stack of IEEE WAVE standards with reference to the layered OSI model (Open Systems Interconnection model) of ISO. The ITS station reference architecture in ETSI follows the principles of the layered OSI model with an extension that included ITS applications. It will be described in comparison with the WAVE protocol architecture.

The IEEE WAVE standards are flexible to support multiple device types including Roadside Units (RSUs) and On-board Units (OBUs). RSUs are stationary while OBUs are installed in vehicles. Other envisioned devices are portable units and pedestrian units.

The WAVE protocol stack which is comprised of IEEE 1609 standards is illustrated in Fig.2.5 with reference to OSI model.

Physical layer: the physical protocol for DSRC is standardized in the standard IEEE 802.11p that is now incorporated in IEEE Std 802.11-2012. The standard IEEE 802.11p adds a number of extensions to IEEE Std 802.11 including functions and services that support a device to communicate directly to another device outside of an independent or infrastructure network. This is an operation outside the context of basic service set (OCB) that is a communication scenario encountered in vehicular communication. The standard IEEE 802.11p-2010 also standardized the 5.9 GHz OFDM PHY (5.850–5.925 GHz in the U.S., 5.855–5.925 GHz in Europe), channel bandwidths, operating classes, transmit power classification, transmission masks, and the alternate channel and alternate adjacent channel rejection requirements.

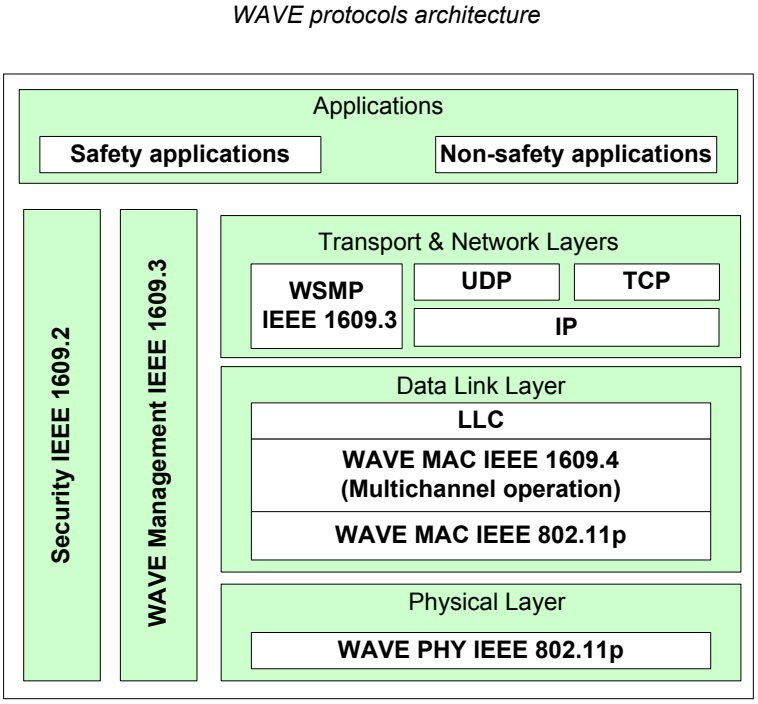


FIGURE 2.5: WAVE protocol architecture

Data Link layer: Data link layer includes two sublayers Medium Access Control (MAC) and Logical Link Control (LLC). The LLC works as an interface between MAC sublayer to the upper layer. It identifies the networking protocol at its above layer. The MAC sublayer is also identified by the standard IEEE 802.11p WAVE amendment. The multichannel operation is extensionally designed for vehicular communication by the standard IEEE 1609.4. The standard IEEE 1609.4 describes how a device switches alternatively among DSRC channels to support both safety applications and non-safety applications.

Network and Transport layers: Above the LLC sublayer, the protocol stacks separate into two sets of protocols. The standard IEEE 1609.3 defines WAVE Short Message (WSM) and WSMP that allows applications to directly control physical characteristics, for examples, channel number, and transmitter power, used in transmitting the messages. The WSMP is designed for optimized operation in vehicular networks. The WSMs can be sent in any channel while IP messages are not allowed in control channel.

Application layer: Application protocols are various. They are objects of different standards. The Society of Automotive Engineers (SAE) DSRC technical committee has developed the SAE J2735 Message Set Dictionary cooperatively with the IEEE WAVE standards for safety applications. Besides, ETSI develops a basic set of applications to support roadside safety and traffic efficiency.

Management services are associated with different data plane entities to provide

layer-specific functions that are necessary for system operation. These functions include time synchronization for channel coordination and processing service requests and advertisements. In particular, the standard IEEE 1609.4-2010 specifies extensions to the standard IEEE 802.11 MAC sublayer management entity (MLME) and the standard IEEE 1609.3-2010 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. The standard defines secure message formats and the processing of those secure messages within the DSRC/WAVE system.

ETSI ITS station reference architecture: In European standards, ITS station reference architecture is quite different from the WAVE protocol architecture as illustrated in Fig.2.6. The architecture is described in ETSI EN 302 665.

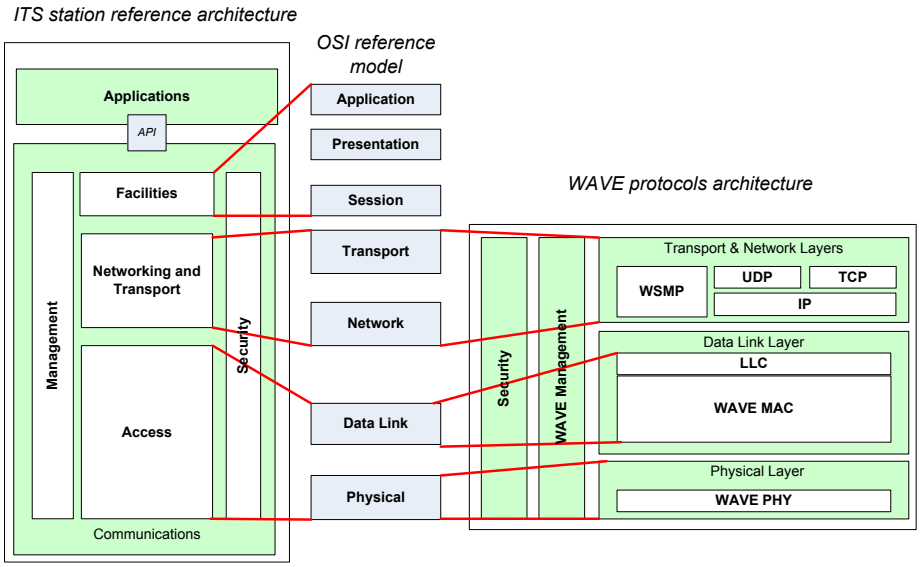


FIGURE 2.6: Relationship of ETSI ITS station reference architecture to OSI reference model and WAVE protocol architecture

In ITS station reference architecture, Access layer represents ITS OSI Physical and Data Link Layer. Networking and Transport layers represent ITS OSI network and transport layers. Facilities layer represents the three highest layers of OSI, presentation, session and application layers. Different from WAVE architecture, ITS station reference architecture defines the facilities layer as a common layer supporting all kind of applications. Common data and functions aggregated from lower layers at the facilities layer are selected to facilitate the requirements of the application that the facilities layer support. It means that the facilities layer maps information provided by lower layers to respective applications. Hence, the stack of common lower layer protocols can support all type of applications thanks to the facilities layer.

2.4 Challenges for communication in vehicular environment

VANETs allow vehicles to directly communicate to each others and to infrastructure. This brings opportunities to improve road and vehicle safety and efficiency with ITS applications that VANETs support. However, new challenges are also created due to characteristics of vehicular environment. The key technical challenges include the following issues: inherent characteristics of radio channel, highly dynamic operating environment, lack of centralized management, requirements of high reliability but low latency communication, the requirement of scalability, the balance of security and privacy.

Inherent characteristics of radio channel: The radio channel in vehicular environment is an unfavorable medium for wireless communication. For example, degradation in the signal strength of the received signals, fading effects are prone to occur due to the impact of weather; multipath propagation is caused by the mobility of transmitters and receivers and obstacles such as building, tunnels. Besides, the relative speeds among vehicles create Doppler Effect that leads to a spread in frequency, so cause inter-carrier interference.

Highly dynamic operating environment: The high-speed movement of vehicles makes network topology change dynamically. Due to the high mobility, the connection duration among vehicles are limited, consequently, the exchanged information is limited and is required to be concise. Therefore, vehicular mobility creates difficulties in designing networking protocol such as routing protocol.

Lack of centralized management: This is the nature of ad-hoc networks. It creates challenges when implementing medium access control, routing protocols and also security solutions. Vehicles are self-organizing devices. Local information can be obtained at a given vehicle from its neighbors but global information is not easy to be aggregated.

Requirements of high reliability but low latency communication: ITS applications are proposed to improve safety and efficiency of transportation systems. Any incident happening in transportation is real-time, it is vital that information about the incident is predicted or notified as soon as possible so that drivers or responsible entities can have enough time to react. Therefore, almost applications in ITS, especially safety applications are real-time. Information should be received in time and with high delivery rate at relevant entities. These requirements should be taken into account in protocols for vehicular environment.

Requirement of scalability: The scale of vehicular networks can reach thousands of devices correspondingly to the scale of road systems. It creates difficulties in management and also the problem of radio congestion due to limited bandwidth while there are a large number of devices communicating with high data rate.

The balance of security and privacy: In VANETs, vehicles have to share their information to cooperate. In distributed communication environment like vehicular networks, it is likely easier to support various ITS applications with more information of individuals. However, the much more shared information, user privacy is more vulnerable to be utilized for bad purposes by malicious parties.

Challenges are primarily addressed in standardized works. However, not all problems from these challenges are solved since VANETs scenarios or ITS scenarios are very various. There are various research activities making efforts to deal with these challenges, evaluate standards and enhance the performance of standardized protocol in certain scenarios. Relating standards and fundamental protocols proposed for medium access control supporting one-hop communication, multi-hop communications and security are briefly elaborated in following sections.

2.5 Fundamental protocols for vehicular networks

2.5.1 Medium access control protocols

The standard 802.11p and Multichannel operation IEEE 1609.4

The standard IEEE 802.11p [47] specifies Distributed Coordination Function (DCF) known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) - a fundamental access method for stations which are OBUs in the context of VANETs. In this thesis, the term "vehicles" is referred to OBUs, or stations, or nodes in a network in general.

The CSMA protocol is illustrated in Fig.2.7. Before transmitting, a vehicle senses the medium to determine if another station is transmitting. Physical and virtual carrier sensing (CS) functions are used to determine whether the medium is busy or not. If the medium is not determined to be busy, the vehicle proceeds its transmission. Otherwise, the vehicle should defer until the end of the current transmission. After a duration of DCF Interframe space (DIFS) if the previous transmission is successful or a duration of Extended Interframe Space (EIFS) if the transmission is failed, it selects a random backoff interval within a contention window and shall decrement its backoff interval counter while the medium is idle. When the backoff interval counter reaches zero, it starts transmitting. The vehicle waits for a duration of Arbitration Interframe Space (AIFS) instead of DIFS if the packet is prioritized for Quality of Services (QoS) supporting. Short Interframe Space (SIFS) is the shortest interframe space between two consecutive transmissions from different stations.

For a packet that has an individual predefined destination address (unicast packet) and is longer than a predefined length, an acknowledgment (ACK) frame is sent by the receiver to confirm a successful transmission. If there is no ACK is received, the sender shall proceed again a backoff interval for a retransmission with a double contention window. It will stop retransmission process till the contention window reaches the

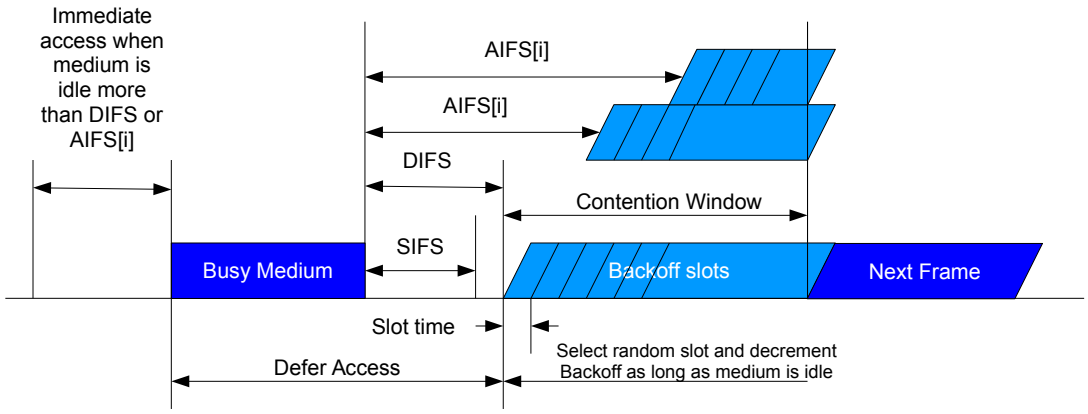


FIGURE 2.7: Backoff procedure in CSMA/CA

maximum or the number of retransmission times reaches a certain number specified in the standard. Besides, for unicast packets, Ready-to-Send/Clear-to-Send scheme (RTS/CTS) is used to avoid collisions and hidden terminals. The transmitter and the receiver exchange short control frames RTS and CTS after determining that the medium is idle or after any deferral or backoffs.

CSMA/CA CS mechanism: CSMA/CA uses two CS mechanisms which are physical CS and virtual CS. The medium is indicated busy if any of them or both indicates a busy medium. The physical CS function should be provided by PHY layer. Whenever the vehicle receives any signal with receive power higher than Clear Channel Assessment (CCA) threshold, it determines the medium as busy. The CCA threshold is specified in individual PHY specifications.

The virtual CS mechanism is provided by MAC layer. This function is carried on regarding Network Allocation Vector (NAV). The NAV maintains a prediction of future traffic on the medium based on the duration information that is included in RTS/CTS frames. The RTS and CTS frames contain a Duration field that defines the period of time that the medium is reserved for transmitting the actual data frame and returning ACK frame. A station receiving either the RTS (sent by the originating station) or the CTS (sent by the destination station) shall process the medium reservation. Thus, a station might be unable to receive from the originating station (hidden terminal to the originating station) and yet still know about the impending use of the medium for transmitting a data frame via CTS. However, RTS/CTS can not be used for broadcast packets that have group addressed destinations because there are more than one recipients for RTS, thus, there are multiple concurrent CTS responses leading to CTS collision. Besides, RTS/CTS frames add overhead inefficiency, so the mechanism is not suitable for short data frames. While broadcast and short packets are primary traffic

types exchanged in VANETs.

Enhance Distributed Channel Access (EDCA): According to applications, information exchanged by vehicles will be prioritized depending on its importance and urgency. The standard IEEE 802.11p specifically adapts Enhanced Distributed Channel Access (EDCA) that was originally specified in the standard IEEE 802.11e, introducing Quality of Service (QoS) support. Four access categories (ACs) are defined by their AC index, corresponding AIFS number (AIFSN) and minimum/maximum contention windows. An AIFS is comprised of time duration for AIFSN slots plus one SIFS. EDCA Function (EDCAF) replaces DCF as the medium access function. Each frame or packet is assigned to one of four ACs by the application creating it. Vehicles operate alternatively in two operation channels: CCH and one of the SCHs in order to support concurrently safety applications and non-safety applications. The multichannel operation is specified in the standard IEEE 1609.4 [49]. Scheme of EDCA derived from the standard is shown in Fig.2.8 and is briefly described in following paragraphs.

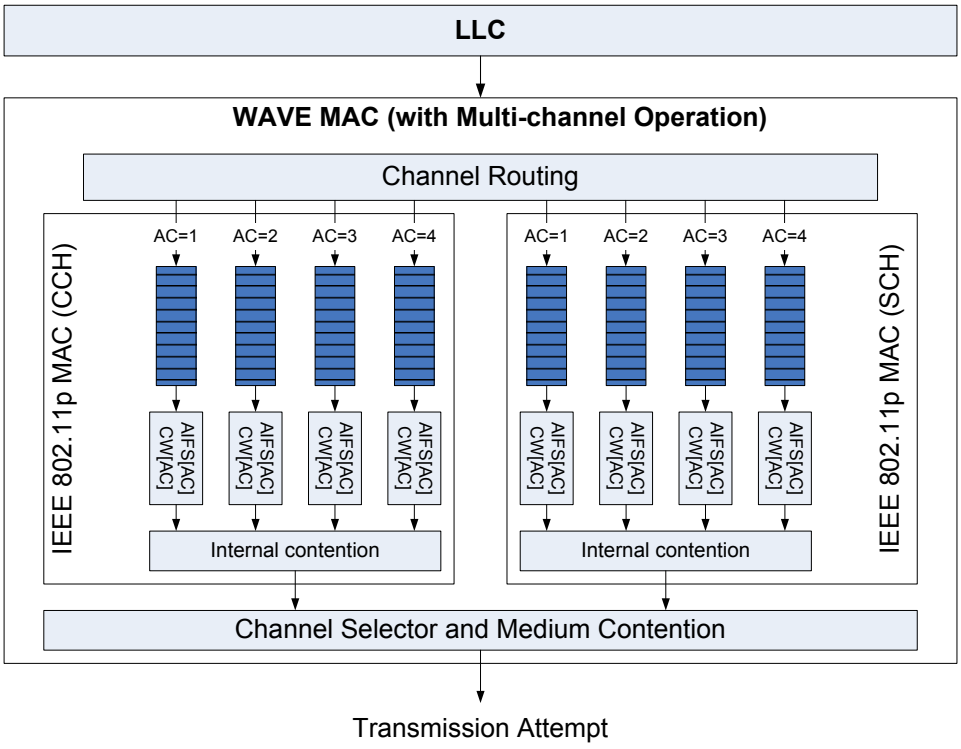


FIGURE 2.8: Scheme of EDCA derived from WAVE standard IEEE 1609.4-Multichannel operation

Respectively to four ACs, four queues are provided in each channel. Each of them has specific parameters shown in Table.2.1 (EDCA for outside the context of BSS referred to ad hoc mode). Names of ACs, AC_VO, AC_VI, AC_BE, AC_BK, are reserved

as defined in the standards but the name with index AC1, AC2, AC3, AC4, are customized for convenient use in the remainders of the thesis.

TABLE 2.1: Four Access Categories

Access category	AIFSN[i](slots)	CWmin[i] (slots)
AC_VO (AC1)	2	3
AC_VI (AC2)	3	7
AC_BE (AC3)	6	15
AC_BK (AC4)	9	15

The AIFS replaces the fixed DIFS time defined in the DCF. The vehicle can access for transmitting when the medium is sensed idle for an AIFS. The AIFS, minimum and maximum contention windows are individual for each AC. Contention among ACs is resolved internally, the smallest waiting time frame will be the one contending to other station in the medium. If a internal collision happens, i.e. there are more than one frames having waiting time expired at the same time, the frame from higher prioritized AC will be preferred. The other one will repeat the backoff procedure.

Channel coordination: Channel coordination is designed to define how the devices switch between one channel to another. Multichannel operation allows single-PHY devices to access to high-priority data and management traffic in CCH interval, as well as general traffic in SCH interval. Vehicles alternatively switch between CCH and a SCH every channel interval as illustrated in Fig.2.9.

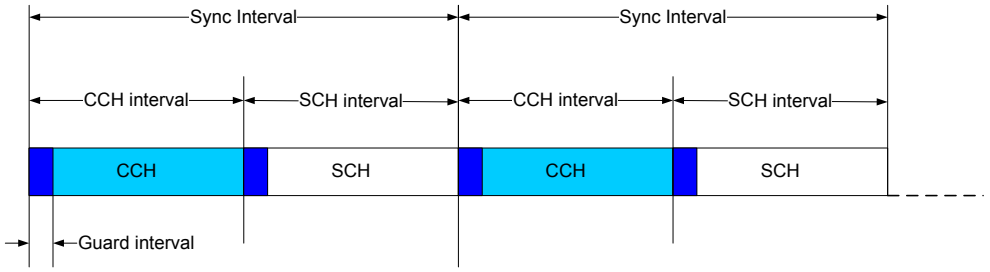


FIGURE 2.9: Channel cordination: alternating access

During the interval that vehicles operate on CCH, namely CCH interval (CCHI), only WSMP messages are allowed. After CCHI, vehicles switch to SCH for an SCH interval (SCHI), both WSMP and IP messages are allowed to be transmitted. The values of CCHI and SCHI are stored in the MIB attributes that are specified in the standard IEEE 1609.4. They are 50 ms each interval. A sync interval is comprised of one CCHI and SCHI, i.e. 100 ms. Vehicles use Coordinated Universal Time (UTC) for synchronization. At the beginning of each channel interval, there is a guard interval used for radio switching and timing inaccuracies. At the beginning of the guard interval, all

medium access activities on the previous channel should be suspended and may be resumed in the next interval of this channel. During the guard interval, the medium is declared to be busy to avoid simultaneous transmission attempts at the end of the guard interval.

Concerns when designing MAC protocol in VANETs

The broadcast is the nature of vehicular networks. When a vehicle transmits a message, the message can be typically received by many neighbors of the sender. This nature indeed is good for vehicular communication as many vehicles may benefit the safety information included in the message. However, hidden terminals in the broadcast environment and the scale of vehicular networks cause medium access collisions and congestion that lead to a degradation, particularly, in packet delivery rate, and generally in network performance.

When two wireless transmitters cannot sense each other (hidden terminals for each other) and broadcast at the same time, they cause collisions encountered at all receivers within the reach of both senders. This is known as the problem of hidden terminals in wireless communication. The RTS/CTS mechanism and/or Acknowledgment scheme solve this problem for unicast packet while there is no such mechanism for broadcast packets. Since there is no acknowledgment scheme for broadcasting, any failed transmissions of broadcast packets due to collisions or errors in radio propagation are not retransmitted.

In the broadcast environment, if there is any ongoing transmission in the channel, other terminals have to suspend their transmission and refer until the medium is idle again to access the medium. They are the exposed terminals. While the bandwidth of operation channels assigned for VANETs applications is currently 10 MHz, with the high density of vehicles, the channel easily suffers from channel congestion. For examples, 100 vehicles broadcast 10 packets/s as required broadcast frequency of some safety applications suggested in [50], each packet has a suggested length of 400 Bytes, this generates a traffic load of 3.2 Mbps. With lowest data rate 3 Mbps which is lower than the traffic load, congestion can occur. When there are more vehicles in the networks, the congestion is even worse. The supported data rate is limited by a bandwidth of 10 MHz and radio characteristics of channels for vehicular environment, it ranges from 3 to 27 Mbps. The lower data rate is more robust against noise and interference.

The coexistence of two types of communications (one-hop and multi-hop) must be taken into account. For safety applications, vehicles periodically transmit status information to nearby neighbors. Thus, one-hop broadcast is the primary communication type of vehicular networks. The information of incidents on the road should also be disseminated along multi-hops to inform coming vehicles to the vicinity of the danger. In some safety applications, local information may be an interest of central management entities for special purposes such as studying, statistics, collision predicting, etc..

Besides all above issues in designing MAC protocol for vehicular networks, the central challenge in VANET is the lack of central communication coordinators. All of these constraints should be considered while we design a MAC protocol for vehicular environment.

Proposed MAC protocols in VANETs

While current development and standardization works focus on an appropriate CSMA-based MAC protocol defined in the standard IEEE 802.11p, there are several proposals for MAC protocol in WAVE that base on other medium access approaches: Time-division multiple access (TDMA) [71][74][64], Space-division multiple access (SDMA) [7] [55] and Code-division multiple access (CDMA) [78] [67].

With TDMA, the medium accessing time is slotted, each time slot is assigned to a vehicle for its transmission. However, the lack of centralized management makes slot assignment be a difficult task. Reservation-ALOHA (R-ALOHA) [25] was proposed to improve the throughput of typical slotted ALOHA which is one of the earliest proposed medium access control protocol for wireless communication. The protocol is extended to be used for inter-vehicle communication by authors in [71][74][64].

In R-ALOHA system, the channel time is divided into frames that comprise N slots in each. Each time slot should be long enough for transmission of a packet. Initially, if a vehicle has a packet to transmit, it chooses randomly a slot to transmit. After each complete frame, vehicles have a usage pattern of a frame. They can determine which slot is used or unused. The unused slot is the one that no packet is transmitted or a collision is encountered. Otherwise, the slot is used. Consequently, the vehicle that has a packet to transmit selects unused slots and contends for it. If the initial transmission in the unused slot is successful, the vehicle becomes the owner of the slot and uses this slot in the next and subsequent frames for its own transmissions as long as it needs. If a collision occurs, i.e. more than one vehicle choose this given unused slot to transmit, a different unused slot is chosen for next contention. However, it remains one question, how the vehicle determines its own transmission in the unused slot is successful or collision to decide to own the slot for next following frames. In [71], the communication is unicast, an acknowledgment included in a frame is sent by the receiver. Otherwise, in broadcast in wireless communication, there is no way for a vehicle to determine its own transmission is successful or not.

R-ALOHA is extended to address the mobility in vehicular environment by Man and Rckert [74]. To deal with the hidden terminal problem and the mentioned above issues (vehicles cannot detect collisions that they are involved in), they propose the Concurrent Slot Assignment Protocol (CSAP). Each frame is divided into N pairs of data slots and collision slots. The vehicle owning a given slot broadcasts its perspective on the reservation status of all other slots in its corresponding collision slot. The perspective is contained in a vector. Since every vehicle broadcasts its own vector, each vehicle is able to merge the vectors and obtain a slot assignment of all vehicles within

two-hop surrounding. The exchange of vectors is vital in this solution. This may create significant latency for vehicles to totally complete slot assignment. Moreover, network topology changes dynamically in vehicular networks while the slot assignment must be repeated whenever the topology changes.

With SDMA, the medium access is assigned according to the location of vehicles. Depending on the geographical position of a given vehicle, a time slot, or frequency or spreading code is derived and assigned to the vehicle. These approaches rely on the availability of GPS to provide vehicles knowledge of their positions. The first SDMA-based system model is introduced by Bana and Varaiya [7]. The geographical space is divided into N partitions and bandwidth is divided into N FDMA-channels, respectively N partitions in time space for TDMA or N spread coding for CDMA. They propose a mapping function to map the space divisions to other resource divisions.

CDMA is a medium access method that allows concurrent accesses of stations by using different spreading codes. Principally, a signal is multiplied by a spreading code before being transmitted to wireless channel in order to increase the transmitted signal bandwidth. That can avoid intentional interference. CDMA is considered for inter-vehicle communication in [78]. In their work, vehicles sense current using spreading code to find the unused codes. Lott et al. [67] combine TDMA and CDMA in their works. Although the solution may make the signal robust against interference and noise, how to assign spreading codes to stations properly and the near-far problem are still typical challenges for implementing CDMA in VANETs.

2.5.2 Multi-hop communication protocols in vehicular networks

As mentioned above, ITS applications are supported by not only one-hop communication but also multi-hop communication. One-hop communication can be provided by MAC protocols which are commonly used by all applications, while multi-hop communication is provided by different networking protocols depending on the application that it supports. Therefore, there is a wide range of proposals for multi-hop communication protocols in VANETs.

The information is disseminated in the network to one or a group of vehicles or every vehicle hop by hop. The vehicles that receive the information and forward it to next hop are relays. Multi-hop communication protocols supporting dissemination of information in the network describe how relays are selected. They can be considered as routing protocols or forwarding approaches. Routing protocols determine the way to choose a path from source to destination while the path sometimes cannot be defined for a moment due to the lack of connectivity or in multi-hop broadcasting, all vehicles in networks are interested in the information. In these cases, the protocols are considered as forwarding protocols. Depending on requirements of specific communication environments and supported applications, multi-hop communication protocols are proposed.

In WAVE standards, WSMP and Internet protocol IPv6 are selected as networking protocols. However, how they support multi-hop communication is not mentioned. IP and higher layer protocols used over IP are used for WSA and IP messages that are allowed to be transmitted only in SCHs, not CCH. They may support multi-hop communications in vehicular networks, however, only non-safety applications, not safety applications. WSMP messages including safety messages are allowed in both SCHs and CCH. Although WSMP is standardized in WAVE standards, no routing or forwarding protocol is mentioned for safety applications in the WAVE standards. While in European standards, ETSI describes GeoNetworking protocol as a networking protocol providing routing in VANETs in the standard ETSI M453 (07-2014).

Challenges in multi-hop communication in VANETs

The central challenges on disseminating information across long distance and to predefined destinations are dynamic network topology, short and intermittent connectivity and capacity constraints. Since vehicles move with high speed, their positions change every second. It is a challenge to carry a packet to a destination when the sender has no idea about the position of the destination. The mobility of vehicles results in limited connection duration when two vehicles encounter each other. Besides, the multi-channel operation even shortens the connection duration for safety messages exchanging as vehicles spend half of the time for other various non-safety applications in SCHI.

The nature of vehicular environment may cause intermittent connectivity since connectivity is dropped due to bad link condition which is a result of strong fading and distortion. Moreover, the connectivity is not always available because of sparse network or network fragmentation. A vehicle or group of vehicles is isolated hence the messages are not forwarded and kept in buffer for a long time.

As mentioned above, the capacity of VANETs is limited by broadcast nature of wireless networks especially in big scale networks like vehicular networks. Therefore, the disseminated information and control frames supporting the networking protocol should be selected and concise. The redundancy caused by duplicated packets in dissemination should be paid attention as well.

Proposed multi-hop communication approaches for safety applications

Since VANETs is a type of Mobile Ad hoc Networks (MANETs) where mobile stations are vehicles, it inherits features of MANETs. Forwarding approaches supporting multi-hop communication are well studied in MANETs. They can be considered to adapt to VANETs.

The classification of multi-hop communication protocols is depicted in Fig.2.10. Based on the manner that relays are chosen, proposed multi-hop communication protocols in VANETs can be classified into three categories: flat protocols, position-based protocols, and hierarchy protocols. Otherwise, they can be categorized according to

their communication types (unicast or broadcast), then there are routing protocols for unicast (communication between two vehicles) and dissemination protocols for multi-hop broadcast (the information is broadcast multi-hop to all vehicles within large area).

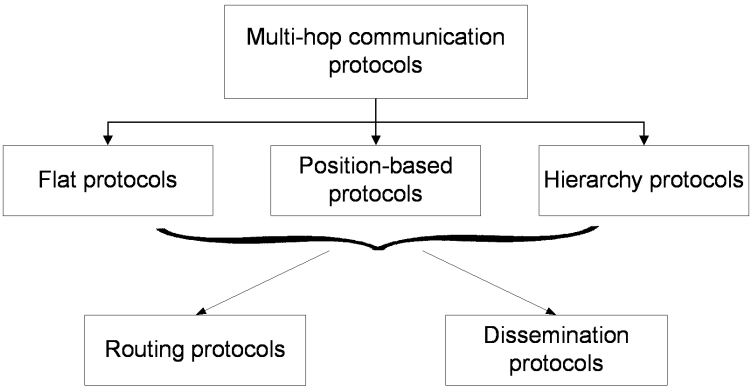


FIGURE 2.10: Classification of multi-hop communication protocols in vehicular networks

Flat protocols select relays only based on the availability of paths or routes to the destination. Pairwise links between two vehicles are not weighted. Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are designed for MANETs to choose the relays belonging to the most-up-to-date and quickest route from the source to the destination. They reduce overhead since they do not maintain routes unless they are needed. However, due to highly dynamic topology, such protocols like AODV and DSR tend to have poor route convergence and low communication throughput [59]. There are several developments based on original AODV to adapt highly dynamic nature of VANETs. Combining information of speed and location of vehicles, the two predict link lifetime protocols are proposed in [79], PRAODV and PRAODV-M. PRAODV constructs an alternate route before predicted lifetime of a link ends. While PRAODVM selects the maximum lifetime path among multiple route options instead of the shortest path. In [82], the route requests are only forwarded within Zone of Relevance (ZOR) using AODV manner. The location must be utilized on this solution. Hence, flat routing protocols originally are not suitable for VANETs due to the dynamic topology so that they should combine other elements in order to deal with the fast change of network topology in vehicular networks.

Relating to dissemination, flooding or epidemic approach is popular. It is a basic approach to spread information very quickly in MANETs. Original flooding protocols can be considered as flat protocols. Every station that receives the information naively rebroadcasts predefined times. The approach is simple, quick but it creates a large amount of duplicated messages that can lead to collisions. Especially, the "broadcast storm" phenomenon is easy to happen since a given message is multiplied and

rebroadcast by all stations. It leads to collisions and no successful transmission. In order to deal with "broadcast storm" in vehicular networks, control schemes are proposed to optimize the number of duplicated messages. Tonguz et al. [101] propose a flooding approach in which vehicles determine to rebroadcast depending on the density of traffic. Wegener et al. [105] propose to control the flooding not only according to the vehicle density in the vicinity but also to the novelty of the flooded information to reduce broadcasting obsolete information. In some other approaches inspired by flooding manner, vehicles decide to forward messages based on their interests in the content contained in the messages [24], or their distances to the previous sender [19], or position of the destination provided in geocast address presented in [29][110].

Position-based protocols choose relays based on their positions. They are promising candidates for routing protocols in VANETs since geographical location information is available via GPS and street maps and many applications benefited from this information. Moreover, trajectories of vehicles follow the structure of road and streets systems and so positions of vehicles within short duration can be predicted [10]. However, there exists a problem for these protocols. For example, greedy routing always forwards the packet to the node that is geographically closer to the destination than the current relay. It will fail when the packet is forwarded to the closest relay to the destination but there is no direct link to the destination. Such situation is known as the local maximum. GPSR (Greedy Perimeter Stateless Routing) [54] combines greedy routing and perimeter mode to alternate greedy mode when the routing reaches local maximum. It is studied in VANETs scenarios [63][35]. Although the forwarding is limited in only a given relay that closer to the destination, the route is corrupted due to sparse network or bad link condition, there is no relay after the current one. Besides, even the given relay is close to the destination but the direct link may not exist due to obstacles, so the local maximum occurs. The perimeter mode recovers from the local maximum but the packet is routed following "right hand rule" and suffers long delay. Routing loop may happen due to the mobility of vehicles.

The digital map is used in some works for navigation system to calculate a preferred route from source to destination. Geographic Source Routing (GSR) is proposed by Lochert et al [66]. They assume the availability of a street map in city environments. GSR essentially uses a Reactive Location Service (RLS) which is a request/reply scheme to get the destination position. The sender floods the network with the position request and then the destination responds with its position reply. The global knowledge of the city topology is needed for the sender to determine the junctions that it has to forward the packet. The Dijkstraś shortest path algorithm is used to find the junctions that make a path from the source to the destination. Forwarding between junctions is then done in the greedy manner. It proposes a promising routing strategy for VANETs in city environments. In simulations, GSR demonstrates a better average delivery rate, a smaller total bandwidth consumption, a similar latency of first delivered packet compared to

DSR and AODV. However, the availability of vehicles around junctions, which are relay candidates, is not taken into account. Since there are some streets or roads having more traffic than others in city transportation environment, authors in [95] propose Anchor-based Street and Traffic Aware Routing (A-STAR). Along the routes that have high traffic, the connectivity is likely always available. Junctions (anchors) in the map are weighted according to their traffic conditions. Packets are forwarded to the high weighted junctions. The A-STAR proposes a more efficient recovery strategy to a local maximum than GPSR and GSR. The street where a forwarded packet reaches local maximum is marked as "out of services" temporarily and is not used for anchor computation for "out of service" duration. Therefore, packets are temporarily not forwarded to this direction and hence local maximum is avoided. However, in big scale networks, above solutions may create long delay due to requirement for global computation.

Geocast routing is basically position-based multicast protocol on which multicast group is defined to be in a certain geographic region [9]. They are implemented for delivering the packet from the source to all other vehicles within a specified geographical region (Zone of Relevance, ZOR). Vehicles out of ZOR have no interest of the disseminated information. The dissemination comprises communication between the source and the destination region and communication inside the destination region. Flooding is normally used for communication inside ZOR while the communication between the source and the destination zone may base on unicast routing or flooding. An idea of a conventional geocast scheme is proposed in [18] and it is enhanced and studied in different scenarios in other works [6]. According to the idea, vehicles receiving a packet set up a waiting time counter respecting distance to the sender before rebroadcast. The furthest vehicles to the sender are the relays that rebroadcast the packets. An abiding geocast protocol is proposed in [73]. The geocast packet is firstly forwarded as a unicast packet to the geocast server which can be an elected vehicle, a roadside server. Otherwise, each vehicle stores this geocast packet destined to its location and keeps neighbor information. The packet is then stored and periodically forwarded to all vehicles in the ZOR during the geocast lifetime by the server.

Position information is also exploited in dissemination protocols in VANETs. Urban Multi-Hop Broadcast protocol (UMB) [56] is designed to overcome interference, packet collisions, and hidden nodes problems during message dissemination in multi-hop broadcast. In UMB, the furthest vehicles to the sender in broadcast direction are selected as relays. Relays are responsible for forwarding and acknowledging the packet. Vector-based TRAcking DEtection (V-TRADE) and History-enhanced V-TRADE (HV-TRADE) [99] are GPS-based message broadcasting protocols. Based on position and movement information, neighbors of the sender are classified into different forwarding groups. The sender selects one border vehicle for each group and broadcasts a packet with IDs of the border vehicles. Messages are broadcast multi-hop to all vehicles in the networks while the rebroadcast is carried on by only selected border vehicles. The solution is limited due to the control overhead to collect information of position and

movement of neighboring vehicles.

Cluster-based/hierarchy routing protocols are able to provide multi-hop communication the scalability since a virtual network infrastructure must be created through the clustering of vehicles. Each cluster is comprised of a cluster head that is responsible for intra-cluster communication and inter-cluster coordination, and cluster members that communicate to each other and to cluster head via direct links. The inter-cluster communication is performed via cluster heads. The stability of the virtual infrastructure is the key of cluster-based routing protocols [13]. Many cluster-based routing protocols are proposed in MANETs but they are unstable in VANETs due to the mobility of vehicles in various vehicular scenarios. Forming and maintaining clusters are challenges in vehicular environment. A Clustering for Open IVC Networks (COIN) algorithm is proposed in [15]. Cluster head election is based on vehicular dynamics and driver intentions, instead of ID or relative mobility as in classical clustering methods. Santos et al. [93] present Location Routing Algorithm with Cluster-based Flooding (LORA-CBF). The protocol forwards packets in greedy routing manner but only the cluster-heads can become relays. Each cluster-head checks if the destination is among its cluster members.

2.5.3 Security in vehicular networks

Besides enabling technologies providing medium access control and networking for vehicular communication, security aspect is also taken into account in ITS standardized works and projects. The IEEE presents the standard IEEE 1609.2 in the family standard 1609 for DSRC for security specifications, while ETSI Technical Committee ITS presents ETSI TS 102 940 (2012-06) as a technical specification of ITS security. Both standards of IEEE and ETSI mainly define message authentication and Public Key Infrastructure (PKI) implementation. However, the message authentication, encryption, and PKI can only solve the high layer attacks which try to manipulate the content of the message, eavesdrop and utilize information for bad purposes while they can not deal with attacks at physical layer and medium access control layer.

Wireless attacks in VANETs

Wireless communication attacks can be categorized depending on different criteria. Engoulou et al. [30] mention three bipolar criteria: outsider vs. insider; malicious vs. rational; active vs. passive. According to a cryptographic-related classification proposed by Mejri et al. [75], they are classified into four categories: attacks on availability, attacks on authenticity and identification, attacks on confidentiality, attacks on integrity and data trust.

Depending on where the attacks belong to, they can be at different layers of the networks or cross-layer. The attacks can target to control the communication or to prevent vehicles from contacting, or to gain the resource for attackers. Hence, in this

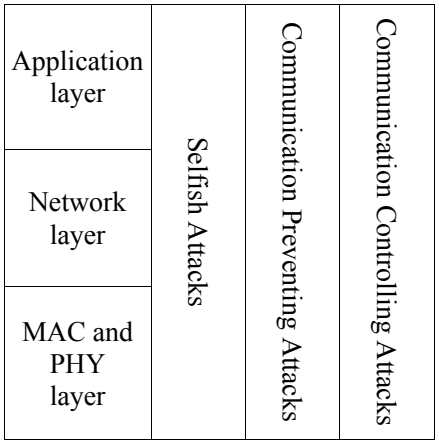


FIGURE 2.11: Vehicular wireless communication Attack classification

thesis, we classify attack models in wireless communication, particularly in vehicular networks, with reference to network layers and objectives which is shown in Fig.2.11.

From the view of a network model, attacks can collect information from different network layers. For example, at application layer, an attacker extracts personal information of users from their exchanged messages with the service providers. He may manipulate the information of a traffic jam warning to inject wrong traffic information in the network. Furthermore, he can masquerade as a priority vehicle by modify the content of his broadcast messages. At network layer, the information of positions, locations of vehicles is available. An attacker can modify his information of position and location included in his packets to hide himself. In multi-hop communication, he can pretend to be a good relay candidate by broadcast his fake information of position, then the traffic is diverted to his desired destination. At MAC layer and physical layer, the attacker can simply broadcast useless traffic to overwhelm the operating channel, the communication is hence prevented [41].

According to objectives, attacks can be classified into three categories as shown in Fig.2.12: communication controlling attacks, communication preventing attacks and selfish attacks. The communication controlling attackers aim to collect and modify exchanged information in the network in order to take control of the communication. For examples, the attacker might want to convince other vehicles to take an alternative route, giving themselves a clear path. He might suppress packets of warning traffic jams or inject fake warnings to keep others away from his path [41]. The information that he uses for this aim can come from application layer, e.g. content of the message about the status of the road. The information may come from network layer, e.g. the position of the attacker indicates the location of the incident notified in the message but the coordination is fake. Communication preventing attacks target the availability of networks services such as Denial of Service (DoS) attacks. DoS attackers try to block

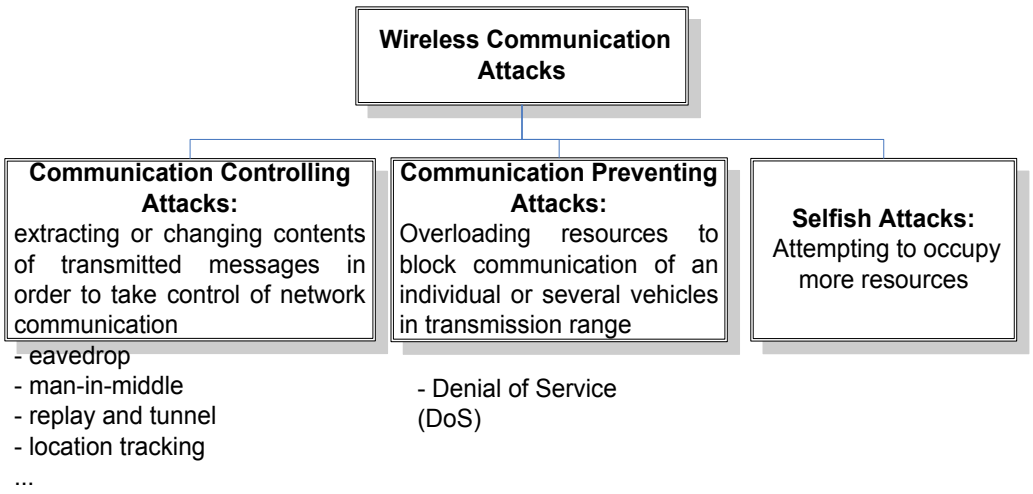


FIGURE 2.12: Objective-based classification

the principal communication medium. The DoS attacks can be at application layer, for example, the attacker sends a large amount of data to a target, a given vehicle, to overload it. Jamming is one kind of DoS attack. The attacker, called jammer, blindly or selectively transmits a signal to disrupt the communication channel [75]. Due to the simplicity of jamming attacks, this kind of attacks belongs to lower layers. Selfish attackers attempt to gain their resources. They can be passive attacks or active attacks. Passive attackers do not disturb other vehicles while active attackers manipulate communication protocol for their own benefits despite their impacts to other vehicles. Among wireless communication attacks, jamming is a big threat for vehicular networks due to its simple requirement of devices, real-time attack and hard to detect especially at lower layers (PHY and MAC) [86].

Security requirements

In order to support different applications in ITS, corresponding protocols including security protocols should meet the requirements of such applications. Especially, safety constraints of safety applications are very strict as they relate to real life safety of the user. When a security solution is proposed, the following requirements should be considered: latency, authentication, low overhead, privacy, attack detection and certificate revocation.

Latency: Since vehicles move at high velocity, any event occurs within very short time which also requires very short time for reaction. For example, events such as emergency brake, blind spot leading to collisions, control lost, etc., happen in second.

Authentication: authentication is the ability to distinguish between malicious and genuine sources of information. As vehicular environment is broadcast, anyone can send messages which can be received at any vehicle within transmission range of the

sender. Thus, we need to ensure that the message is originated from the genuine party. Authentication is guaranteed by Public Key Infrastructure (PKI). However, this requirement may be lighter to safety applications since the safety information is public and the latency required for safety application is too short to implement authentication scheme.

Low overhead: the scale of vehicular networks and broadcast nature of wireless communication require exchanged information to be concise. Moreover, messages are time critical in vehicular networks, security overhead may reduce the resource for useful information.

Privacy: from the view of users, privacy is the core requirement. Vehicles facilitated ITS function always share their information of location, speed and sometime trajectory. This information is vulnerable to be abused for bad purposes by the third party. For instance, a malicious vehicle can keep tracking a given vehicle by eavesdropping its messages. Otherwise, vehicles can be tracked by legal parties such as for crime investigation, road toll system or surveillance system, users sacrifice a part of their privacy whenever they use the vehicles. Therefore, any proposed solutions in VANETs including security solutions should balance the benefit from sharing information and the privacy of users.

Attack detection and certificate revocation: this requirement is crucial for safety applications as every safety applications is real-time. Malicious vehicles or misbehavior should be detected as quickly as possible so that other vehicles have enough time to be aware of the situation and react to it for the safety of their users.

Security proposals for vehicular networks

Public Key Infrastructure provides a basis for enabling authenticated and privacy-preserving protocols in vehicular networks. In PKI, described in the standard IEEE 1609.2 [48], each valid vehicle is assigned a key pair including a private key and a public key issued by Certificate Authority (CA). The private key is privately stored in the device while the corresponding public key is attached to a digital certificate published by CA. When a vehicle sends a message, it signs the message with its own digital signature encrypted by its private key. Then it encrypts the signed message with the public key of the recipient. Only the recipient that owns the corresponding private key can decode the message and then decrypts the signature with the public key of the sender. The digital signature provides the authentication of the message while the message is secured by the key pair.

In order to reserve privacy, avoid revealed private keys and to revoke certificates of misbehaving vehicles, a Certificate Revocation List (CRL), a list of obsolete certificates, is published by CA. However, in big scale networks like vehicular networks, the CRL could be very large. Moreover, it is not easy to update CRL at individual vehicles in distributed communication. An RSU-aided certificate revocation (RCR) mechanism is proposed in [62]. Whenever a vehicle with revoked certificate passes an RSU, the RSU

generates a warning and the warning will be disseminated to all the networks by inter-vehicle communication.

Privacy information could be extracted from certificates and private signature. Anonymous key pairs on which vehicles choose randomly among thousands of short-lived anonymous keys to sign the message may protect the private information of the sender from being revealed. However, the CA has to handle a huge database of key pairs. An idea of group signature is proposed in [61]. Short group signatures are used by vehicles to preserve the anonymity of individuals while the identity of each vehicle can be recovered from the group signature by CA. Identity-based cryptography is adopted at RSU to digitally sign each message launched by RSUs.

Location privacy is the interest of the work of Albert et al. [104]. If a vehicle changes its certificate between two observation points of an attacker who moves along the same lane and with the same speed, the attacker can correlate the certificates used by that vehicle and so tracks its movement. They propose Random Encryption Periods (REP). The REP is triggered when an OBU needs to change its certificate. The OBU sends request to its neighbors moving the same direction to announce the start of REP. During REP, all vehicles use the secret group key. All OBUs receiving the encrypted request change their certificates and their speed or their lanes. REP provides location privacy for an OBU changing its certificate.

Dealing with selfish behavior of vehicles, researchers solve the problem by different methods. Considering vehicular communication as a game of vehicles, Sou [97] proposes a selfishness detection mechanism for file sharing. The mechanism formulates a game to model the frame sharing behavior with intermittent vehicle-to-infrastructure communication. Based on self-history, vehicles differentiate selfish user and non-selfish users and then adjust their sharing probability to punish the selfish user. Authors in [36] propose a trust model at network layer. A monitoring vehicle observes the number of forwarded messages from other monitored vehicles to compute a local trust metric. The honesty of vehicles is evaluated by this local trust metric which reflects their cooperation.

Authenticated messages can be protected from communication controlling attacks such as eavesdropping, spoofing, alteration, and replay. Selfishness can be detected after some time for monitoring globally transmissions in the networks. However, the basic requirement is that vehicles can communicate with each others, especially for safety applications. For instance, in safety-related scenarios, if the medium is jammed, partly communication in the networks is blocked; vehicles in the vicinity of the incident may miss important information and cannot react in time. In this situation, the highest priority is detecting the attack and recovering the communication. In MANETs, communication preventing attacks such as denial of service attacks are well studied but not in VANETs.

2.6 Open issues on improving performance of safety applications

The fundamental protocols provide basic concepts for communication in VANETs; however for supporting safety applications, it still remains open issues of assuring the quality of services and security. Safety applications have strict constraints since they relate to the safety of the user. Safety-related information must reach adequate recipients in acceptable delay for them to react. We discuss here three main issues relating to the performance of safety applications: reliability, connectivity, and security.

For safety applications, it is critical that vehicles receive urgent and/or important information in time and as many vehicles within impacted area as possible are noticed. This is referred to the reliability of the communication. However, there is no acknowledgment scheme or RTS/CTS scheme for broadcast messages. These schemes help the sender to be informed about any failed transmissions so that the important messages can be transmitted again. While messages are likely dropped or failed to be transmitted due to the characteristics of the radio channel in vehicular environments in which fading, distortion usually occur. Moreover, channel switching causes synchronous contention at the beginning of an operation interval (CCHI or SCHI). This leads to collisions for all contending packets (messages). Without supplementary schemes to make the communication more reliable, certain packets containing safety information are lost. Therefore, there is a need for a scheme for reliable broadcasting in VANETs, in particular, reliable broadcasting for safety applications because almost safety applications are supported by broadcast communication.

Due to the scale of vehicular networks and variety of ITS applications, not only local vehicles within a one transmission range but also vehicles or management entities at the far distance are interested in the information of the event. Thus, both one-hop communication and multi-hop dissemination are necessary and their coexistence should not be neglected. From the view of network layered model, one-hop communication is supported by MAC protocol at MAC layer while multi-hop dissemination is a task of a networking protocol at the next higher layer. Any proposal at MAC layer may impact to the higher layer protocol that it supports, so the coordination between protocols from two layers should be considered.

Various multi-hop forwarding approaches have been proposed for vehicular environments in order to support different communication modes: unicast (pairwise communication), broadcast, multicast and geocast (a special case of multicast). According to applications, suitable forwarding protocols are selected. Moreover, applied scenarios in vehicular networks vary from mobility, scale to connectivity. Therefore, it is reasonable to analyze properties of the scenarios when evaluating a protocol.

In vehicular networks, the path from the origin to the destination does not always available due to the intermittent connectivity and fragmentation of the network. In order to deal with this problem, the message is stored and then forwarded when the

connection is available. The objective of the forwarding protocols is to choose best carriers that are vehicles carrying the message toward the destination. The selections of carriers are based on the prediction of the chance that the carriers may reach the destination via single or multiple hops. These forwarding protocols are defined as opportunistic forwarding protocols. They will be discussed more details in chapter 4 where we will elaborate solutions to improve the quality of safety services in term of connectivity.

The periodically exchanged messages in VANETs may become a new attack target of jamming attacks that are easy to conduct in vehicular environment. Recently, standardized works and almost security related works for VANETs have been making efforts to find the solutions at higher layers that based on encryption, handling and managing PKI [37], etc. while attacks at lower layers, in general, and jamming attacks, in particular, still remain an open issue in vehicular environment.

Furthermore, securing messages with encryption and deployment of PKI cannot deal with jamming attacks since communication is temporarily blocked. Therefore, there is a need of specified solutions which take into account requirements and challenges of vehicular ad hoc communication. The solutions are especially necessary for safety applications due to the lack of specific studies of this such particular object.

Background of ITS and fundamental protocols for communication in vehicular ad hoc networks have been presented in this chapter. We also discuss open issues in supporting safety applications in vehicular networks. The next three chapters will address these issues and describe our solutions to improve the quality of service and security of safety applications. The reliability for safety applications is further discussed in chapter 3. Connectivity issue is investigated in chapter 4. Our core contribution in the field of security for VANETs is elaborated in chapter 5.

Chapter 3

Reliability in broadcasting for safety applications in Vehicular Networks

Broadcasting plays an important role in vehicular communications because almost safety applications operate in broadcast mode. In our definition, the reliability in broadcasting for safety applications in vehicular networks regards to the delivery of data to all the vehicles within a concerned area. For example, all vehicles in a certain distance to an incident must be noticed about the event to react to it. The reliability for safety applications is mainly evaluated in term of the ratio of delivered packets (Packet Delivery Rate) and delay to deliver the packets. Each safety application has its own constraints. Depending on the supported safety application, a reliable protocol should guarantee an acceptable packet delivery rate within an acceptable latency at the receivers. According to the performance evaluation of the standard IEEE 802.11p for broadcasting [20], the performance of the standardized MAC protocol in some vehicular scenarios is poor when the simultaneous contention occurs as a consequence of multichannel operation. In the standard, broadcast packets are not retransmitted when they encounter contention collisions or poor channel quality. Therefore, the reliability has not been provided for broadcasting. In order to improve the reliability in broadcasting, we propose a polling scheme which can be integrated into the standardized MAC protocol. Our scheme allows broadcast packets to be retransmitted when some vehicles within the transmission range of the sender do not get the information.

Among existing solutions for the reliability in broadcasting, we are interested in only the solutions at MAC layer because these solutions can be suitable for all kinds of safety applications. These applications may require only one-hop communication or also multi-hop communication. In consideration of the cooperation among layers, we carry on a further investigation of the impact of a reliable MAC protocol on dissemination.

The remainder of the chapter is organized as follows: the state of the art of proposals to improve reliability in broadcasting in vehicular networks is resumed in section 3.1; our proposed scheme is described and analytically studied in section 3.2 and section 3.3; the impact of a reliable MAC protocol on dissemination is discussed in section 3.4; the performance evaluation of our scheme in one-hop communication scenario and

dissemination in highway and urban scenarios is analyzed in section 3.5; the chapter is concluded in section 3.6.

3.1 State of the art

3.1.1 Problem Statement

According to the standard IEEE 1609.4 [49], vehicles operate alternatively between one control channel (CCH) and one of six service channels (SCHs) within every 100 milliseconds (ms), namely sync interval. During CCH interval (CCHI), all vehicles exchange safety-related messages comprising event messages and periodic messages. Carrier sense multiple access (CSMA) is used as a MAC protocol in vehicular networks. It is described in the standard IEEE 802.11p. To make an efficient reservation of the channel and reduce collisions, a handshake scheme, Ready-to-send/Clear-to-send (RTS/CTS), is used for unicast messages. In order to gain the reliability, acknowledgment (ACK) and retransmission mechanisms are used. However, no such mechanism is applied for broadcast messages. Unfortunately, safety applications in VANET mainly work in broadcast fashion since the safety-related information is useful for all neighbors of the sender. Therefore, a reliable broadcast scheme is needed to guarantee the reception of safety-related messages at all vehicles. It is challenging to design the scheme in distributed environment, unstable links caused by high mobility and limited operation time which is a consequence of multichannel operation. They are strike characteristics of WAVE [3].

Reducing congestion helps to improve the reception rate of packets, thus, it improves the reliability of the communication in the case of congestion. However, avoiding congestion does not guarantee the reception of a packet; the reliability is not always provided. We would like to emphasize the difference between the objectives of proposals for congestion control and for reliable broadcast. In this study, we discuss reliable broadcast in all communication conditions, not only in congestion.

3.1.2 Reliable protocols for broadcasting in vehicular networks

Solutions for reliable broadcasting can belong to different layers such as MAC layer or networking layer or higher layer. They also target different objectives (single-hop and/or multi-hop communications, event messages or periodic messages) regarding the applications that they aim to support.

From the view of MAC layer, reliable protocols can be classified as shown in Fig.3.1. Some approaches defer totally from the standard. They propose other MAC protocols for broadcast in VANETs than CSMA in the standard IEEE 802.11p to make the communication more reliable [81]. While the another solution is adding a reliable scheme to the existing MAC protocol in the standard to improve the reliability of broadcasting

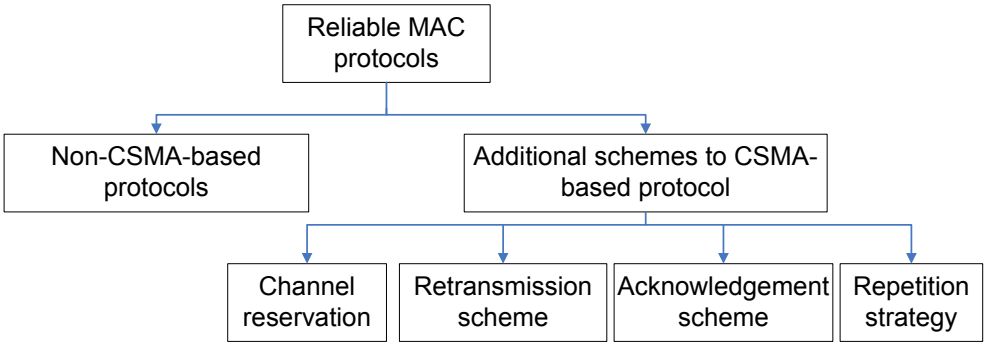


FIGURE 3.1: Classification of reliable MAC protocols

in VANETs [43][91][44]. This scheme can be one of following schemes: channel reservation scheme, retransmission scheme, acknowledgment scheme or repetition strategy. Among these CSMA-based solutions, some works solve the problem by combining MAC protocol and networking layer protocols such as dissemination protocols [72][14][102][108]. The retransmissions by the sender, channel reservation schemes, acknowledgment schemes or repetition strategies are decided based on cross-layer information instead of only MAC layer information.

Some related works that make efforts to provide reliable broadcast are summarized in Table.3.1. Authors in [81] propose VeMAC, a TDMA-based MAC protocol for reliable broadcast in VANETs. The protocol works in a system model in which each vehicle has two transceivers operating concurrently in CCH and one SCH. Each vehicle selects a fixed time slot in each frame for their transmissions. The slot selection of a given vehicle is determined based on the pattern of slot usage of its two-hop neighbors. A list of one-hop neighbors and slots that their neighbors used are included in the header of beacons. Based on successfully received beacons, a given vehicle can construct a set of slots that its neighbors within two hops use for their transmissions; it hence selects randomly a slot among the rest slots - available slots in the frame. If there is another vehicle choosing the same slot, a collision occurs, then the given vehicle will not find itself in the list of neighbors of its neighbors. Therefore, based on headers of received beacons, the given vehicle can determine whether there is a collision for its transmission or not. It will select another available slot if the collision is detected. The protocol requires time for slot selection. Moreover, the list of neighbors added in the header of the beacons makes packets longer while in VANETs, exchanged information is better to be very concise.

Retransmission schemes and acknowledgment schemes that let the sender know whether its message is delivered successfully or not are added to existing CSMA MAC protocol to improve the reliability at MAC layer. These proposals operate at MAC layer

Protocols	**Applications**	**At layers**	**Concepts**
VeMAC[81]	single-hop	MAC	TDMA-based
SCPR[44]	single-hop	additional Reliability sublayer (between Transport and Application layers)	combining network coding and repetition
Retransmission schemes[43]	single-hop	MAC	blind retransmission
Cross-layer schemes[72]	single-hop, multi-hop	MAC, Networks	retransmission and location-based repetition
CLBP[14]	single-hop, multi-hop	MAC, Networks	channel reservation
SRB[102]	multi-hop	MAC, Networks	channel reservation, cluster-based dissemination
Piggyback approach[108]	single-hop	MAC, Networks	piggyback cooperative repetition
ABSM[91]	single-hop	MAC	acknowledgment scheme

TABLE 3.1: Proposals for reliable broadcast

and support single-hop communication. Two retransmission schemes are proposed in [43]. The source simply rebroadcasts its message for several times. The message is rebroadcast consecutively in a row or subsequently for predefined times. Although the retransmission improves the probability of message delivery, it creates duplicated messages. Also, if a collision occurs to the message, all subsequent copies will encounter collisions. An Acknowledgment-based broadcast protocol from Static to Highly Mobile (ABSM) is proposed in [91]. In ABSM, a vehicle receiving a message sets up a waiting time to rebroadcast the message. It includes IDs (Identities) of the sources of messages that it received to its beacons, this information is considered as an acknowledgment of receiving the message to other vehicles. During waiting time, a given vehicle will stop rebroadcasting if all of its neighbors receive the message. The scheme relies on the periodically exchanged beacons.

Repetition strategy of neighbor vehicles may enhance the delivery of broadcast packets but it generates more traffic in communication that may lead to congestion. A piggyback repetition scheme is proposed by Yang et al in [108]. Vehicles broadcast not only their original messages but also messages that they received. However, not all received messages are piggybacked. Criteria are identified in the work to choose which messages should be piggybacked based on deadline and distance of the source of the message. The repetition is limited by times of repetitions and lifetime of the messages.

Hassanabadi et al. [44] propose an idea of combining retransmission scheme and network coding. Each vehicle retransmits its message for several times during the lifetime of the message. Similar to piggyback idea, instead of retransmitting their own messages, vehicles broadcast a combination of its message and all received messages from other neighbors. Network coding technique supports generating the combination.

A wide range of reliable protocols utilize information coming from network layer such as location and velocity of vehicles. A cross-layer broadcast protocol (CLBP) is proposed in [14] in which the authors present a relay-selection scheme. Before transmitting a safety message, vehicles exchange BRTS/BCTS (Broadcast Ready to Send/Broadcast Ready to Send). Based on distance to the source, one relay is selected to forward the message and response BCTS within DIFS to the sender. The authors in [72] suggest schemes classified for one-hop beacons and multi-hop emergency messages, on which copies of messages are rebroadcast by a relay vehicle that is chosen according to its directional distance to the origin. The origin retransmits its messages if it does not receive enough specified number of copies from selected relays within specified time duration. Copies play roles of both forwarded messages and acknowledgments. Aiming to provide reliable broadcast specially for multi-hop communication, a Selective Reliable Broadcast (SBB) protocol is proposed by Vegni et al.[102]. In SBB, the source vehicle sends a Ready to Broadcast (RTB) whenever it has a message ready to be broadcast. Respecting to the distance to the source, neighbor vehicles calculate waiting time and respond the source by their Clear to Broadcast (CTB). Based on CTBs from neighbors, the source can calculate and determine clusters of neighbors. It elects the furthest vehicle in each cluster to be cluster head of this cluster and forwards the message to only this vehicle.

3.1.3 How to provide the reliability for safety applications?

Safety applications in VANETs are discussed in [50, 42]. From the communication perspective, they are supported by two basic types of messages: periodic messages and event messages. These two types of safety-related messages (or safety messages) are described in standardized works [2][1] of European Telecommunication Standards Institute, ETSI. According to ETSI, periodic messages, namely beacons, are cooperative awareness messages (CAMs) [2] and event messages are Decentralized Environmental Notifications (DENs)[1] that warn unexpected hazards. CAMs or beacons are transmitted periodically with the purpose of sharing information (position, velocity...) among neighboring vehicles. These beacons give drivers knowledge of surrounding environment and their nearby neighbors. While DENs contain information of the occurring event that may influence to not only nearby neighbors but also all vehicles situated in close neighborhoods.

CAMs and DENs issued from a given vehicle are important for its neighboring vehicles. Besides, DENs are required to be disseminated to more distant vehicles (in addition to neighboring vehicles) since they provide critical context information that

surrounding vehicles may need to be aware of or react timely to. Unfortunately, almost existing related works consider either CAMs or DENs separately. Communication within one hop referring to CAMs is the objective of the related works in [84] and [5]. In [38], authors propose a multi-channel dissemination protocol for event safety messages (DENs). If the DENs come during service channel interval (SCHI), they will be intermediately broadcast at all available channels. Otherwise, if they come during CCHI, they will be broadcast normally. If after CCHI, the event safety messages do not gain access to the medium, they will be disseminated with the same algorithm in the next SCHI. Delay of the event safety messages within single hop dissemination is reduced. However, there is no gain for the reliability for periodic safety messages. [14] also focuses on multi-hop dissemination of event messages DENs but no coexisting one-hop communication for beacons is considered. The authors in [43] take into account both CAMs and DENs but their protocol is evaluated only for a single-hop scenario.

DCF/CSMA has been standardized for MAC protocol in VANETs. Therefore, it is more feasible to enhance the reliability of broadcast by adding an optional reliable scheme such as retransmission or acknowledgment scheme. Especially, the scheme purely relies at MAC layer; no information from upper layers is needed. Hence, the scheme will be more flexible to be integrated with higher layer protocols. Moreover, the MAC protocol implemented with the reliable scheme can either stand alone supporting single-hop applications (CAMs) or be combined with dissemination protocol to support multi-hop applications (DENs).

The dependence of network performance on the number of retransmissions and network density is studied in [33]. Simple retransmissions by the sender help to increase the chance for all nodes to get messages correctly but it obviously creates a redundancy that degrades the utilization of the network due to resource wasting. Moreover, in multichannel operation, the resource is extremely limited, thus, the redundancy is an important factor to be considered. In order to reduce the redundancy and enhance the efficiency of the retransmission, the number of retransmissions is optimized according to network density in this work. However, the information of instant density is difficult to collect in highly mobile network.

Due to all above reasons, we propose a pure MAC reliable scheme, polling scheme, which can be integrated into the existing MAC protocol in the standard IEEE 802.11p and support the dissemination protocol as a lower layer protocol. We take into account multichannel operation, reducing redundancy and coexisting safety applications. We aim to provide flexible and reliable broadcasting that can support both CAMs and DENs.

Apart from MAC protocols, dissemination protocols are also important in vehicular communication. Message dissemination making use of local information, e.g. position [8][60], direction and road segment [57] and time stamp [92], has been well studied. These works propose a solution of how to spread out a safety message efficiently with

an assumption of using the standard IEEE 802.11p for MAC layer. The effect of MAC delay to time-based dissemination protocol is considered in [92]. However, none of these studies raises a discussion of the impact of a reliable MAC protocol on higher layer protocol such as a dissemination protocol.

As the objective of our proposal is to support the coexisting safety applications, the reliable broadcasting protocol should also be integrated and analyzed in relevant scenarios. In this chapter, our contributions to provide reliable broadcasting for safety applications are two folds: the polling scheme at MAC layer and the integration of the scheme or any reliable MAC protocol in general, into a position-based dissemination protocol.

Firstly, we introduce a new polling scheme which makes the MAC protocol more reliable. Our polling scheme is integrated into the standardized MAC protocol. By using a notification (a very short message) after data transmissions, some supposed receivers that have not received the data packet will send a poll to ask the origin for a retransmission. Moreover, with this notification, senders can detect the collisions that occur for their recent transmissions and then automatically enter to back off procedure as it is specified in the standard IEEE 802.11p. Rebroadcasting is limited by polling manner, so the number of duplicated copies is reduced. Since the scheme operates without the need for additional higher layer information, it is operated at MAC layer so it is suitable for one-hop communication and also supports multi-hop dissemination as a MAC protocol. Knowledge of the surrounding network and complicated computations are not required in our scheme. We evaluate our proposed scheme under a strict condition that messages come to all nodes at the same time at the beginning of CCHI due to multichannel operation. We present an analytical model for our polling scheme that addresses closely to unique specifications of WAVE: channel switching and prioritized access categories.

Secondly, to consolidate and validate our analytical results, we conduct simulations in which our polling scheme is implemented in MAC protocol and studied together with a dissemination protocol in NS-3. We previously evaluate the protocol separately at MAC layer and compare it to the standard protocol and another retransmission scheme, called batch scheme [43]. Then, we study our proposed scheme, at MAC layer, integrating with a dissemination protocol in urban and highway scenarios. Furthermore, impacts of a reliable MAC protocol on dissemination are analyzed. From the best of our knowledge, it is the first time in literature that this issue is brought to a discussion. We analyze how the performance of the multi-hop dissemination protocol changes when broadcasting within each hop is enhanced. An improvement compared to the standard IEEE 802.11p protocol in term of packet delivery rate is observed in almost scenarios when we apply polling scheme at MAC layer. Details of our proposals will be elaborated in the next section.

3.2 Polling scheme for reliable broadcasting

Broadcasting of safety messages without a reliable scheme results in a low percentage of vehicles receiving the crucial information properly (in the vicinity of an incident). To address this problem, we propose a polling scheme on which any vehicle missing the safety message can detect the missing and request for a retransmission. As the message is retransmitted only when necessary, we can reduce the redundancy and enhance the utilization of the channel.

Our polling scheme is a receiver-oriented scheme. After the first transmission, the safety message may not be received by all vehicles within the transmission range of the source due to collisions or low quality link. A short message called Broadcast confirmation (BC) is sent after each transmission as a notification by the source. It is for all vehicles (receivers) to verify whether they receive the recent message or not. Then receivers can ask the source for a retransmission by a short message called a Poll if missing occurs. BC is also a notification for sending nodes to retransmit if a collision has happened for their recent transmissions. The frame format of BC and Poll and polling scheme will be elaborated as below.

The format of BC and Poll frames is defined in Fig.3.2.

Frame Control (2 Bytes)	Duration (2 Bytes)	TA (6 Bytes)	Sequence Control (2 Bytes)	FCS (4 Bytes)

(a) Broadcast Confirmation frame

Frame Control (2 Bytes)	Duration (2 Bytes)	SA (6 Bytes)	Sequence Control (2 Bytes)	FCS (4 Bytes)

(b) Poll frame

FIGURE 3.2: BC and Poll frame format

Frame control field is 2 bytes. It has a format of the frame control field for control frame in the standard IEEE 802.11. Subtype fields included in frame control fields of BC and Poll frames respectively have values of 0110 and 0101 which are reserved in the standard. Hence, there is no conflict between new frames and existing frames in the standard.

When a BC follows a data frame, the duration value is the time, in microseconds, required to retransmit previous data frame, plus one Poll frame and plus one DIFS interval. The TA (Transmitter Address) field of BC frame is the address of the vehicle

who sends the previous data frame. The sequence control field of BC frame is identical to sequence control of the data frame that it follows.

The Poll frame responding to a BC frame has duration value of the time, in microseconds, required to retransmit data frame (this information is obtained from BC frame that the Poll follows), plus one DIFS. The SA (Source Address) field is the address of the origin of the data frame that the Poll frame is sent to request for a retransmission.

The Frame Check Sequence (FCS) field is defined the same as it is done in the standard IEEE 802.11.

In our proposed polling scheme, a node firstly broadcasts message whenever medium is continuously idle for DCF Interframe Space (DIFS) duration, or after a backoff procedure as it is specified in Distributed Coordination Function (DCF) IEEE 802.11. It then additionally sends a BC to inform other nodes that it has broadcast a message. BC is broadcast within DIFS duration after the transmission. Applying the concept of minislot in [72] and [14], we divide DIFS into minislots. To avoid the collision, BC will be sent at a random minislot within a DIFS after the main transmission. Duration of a minislot t_{mini} (ms) and number of minislots n_{mini} (minislots) within DIFS is defined as:

$$t_{mini} = 2.\delta + t_{switch} \tag{3.1}$$

$$n_{mini} = \frac{DIFS}{t_{mini}} \tag{3.2}$$

where δ is the maximum channel propagation delay within the transmission range, t_{switch} is a time duration that a transceiver switches between receiving mode and transmitting mode. Based on the reception of BC from other nodes, a given source node knows that there is at least one node has transmitted at the same time with it. Therefore, if it overhears at least one successful BC from others during DIFS duration after the transmission, or the medium keeps busy while no BC is received after the transmission, it will suspend its BC (if any), choose random backoff slot in minimum contention window and then will start backoff procedure.

The short message BC can be received with high probability because a short message is less affected by error than a long message. With the same packet error rate, a 16-Byte BC has a higher successful probability than the previous 500-Byte data packet. Besides, during DIFS after a transmission, no transmission are allowed except BCs. The BC is transmitted only if after the main transmission, the source node finds that medium is idle. Hence, there are only collisions among BCs. Fortunately, collision among BCs is reduced by the random access of BCs during the DIFS. The BC can be failed to be received partly at some nodes due to hidden terminal problem. Our proposed scheme helps to reduce the hidden terminals problem for the retransmission of the data frame but not for BCs. Provided that one node who has not received the prior data packet within transmission range of the source, gets the BC, a retransmission will be requested.

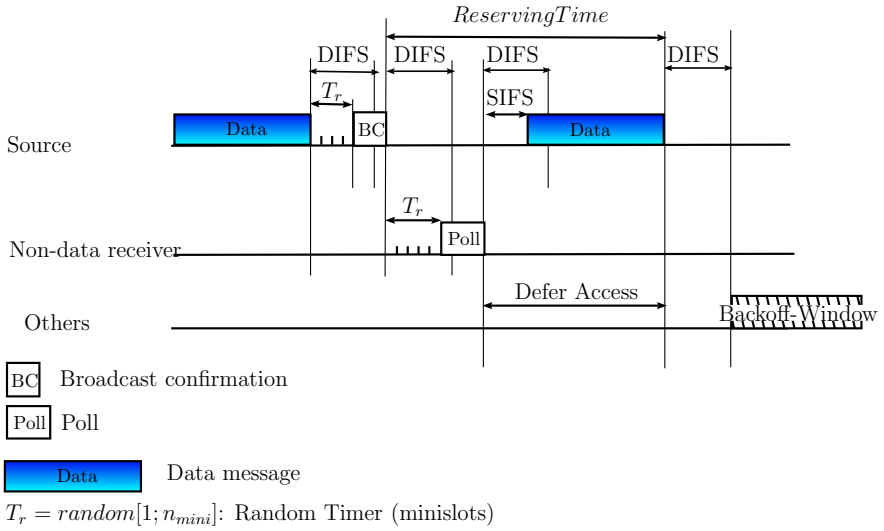
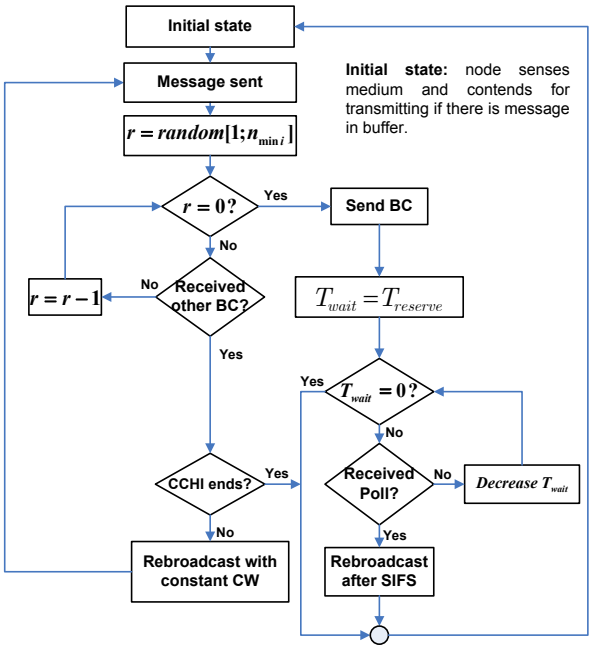


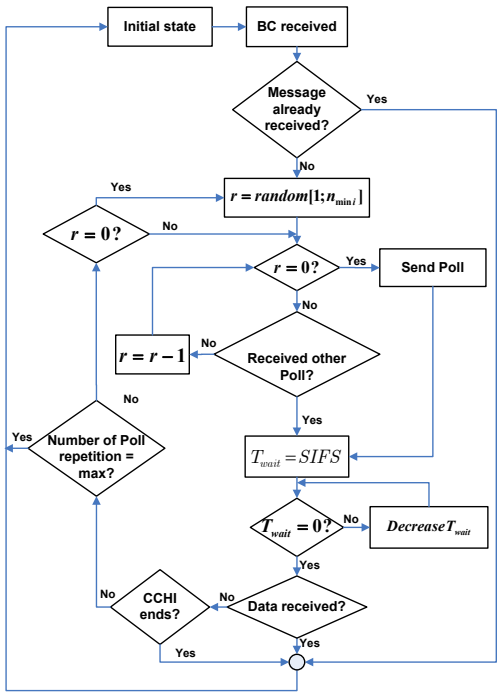
FIGURE 3.3: Proposed polling scheme implemented in CSMA

The main idea of polling scheme is described in Fig.3.3. A BC is sent at random minislot within DIFS after a data packet. A node that has not received the prior data properly is called a non-data receiver. After hearing a BC, it creates a Poll to request the source node for the data packet. It sends the Poll after a random number of minislots $T_r(minislots)$ within a DIFS following the last busy medium due to the transmission of the BC. Other non-data receivers, who overhear correctly a Poll, freeze their Polls and wait for the coming data. If after a duration of SIFS, no data packet is received, these nodes will send their Polls to request for the data packet for several attempts or until they get it. The collision of Polls with other transmissions at the source node is nearly eliminated. Any nodes receiving the BC will defer for duration of one DIFS, plus one Poll, which is included in the duration field of the BC. Therefore, only Polls are transmitted at this duration after a BC.

Fig.3.4 illustrates flowcharts of our proposed polling scheme under multichannel operation. For safety applications, a safety message has a short length, so it is considered as a single packet in this work. In Fig.3.4(a), the first paradigm is executed by a sender that has already broadcast a message (or packet). After sending a message, the vehicle sets a timer for a BC, a BC timer, by choosing a random number r from 1 to n_{mini} slots. The BC timer has a duration of r minislots. In the next step, the node counts down BC timer. While counting down, if it overhears BC from the other, it will stop the timer and move to next procedure. In this next procedure, it broadcasts message again with the same contention window. When BC timer reaches 0, the vehicle will send its BC. After sending BC, the vehicle keeps its recent transmitted message for a duration of time called $T_{reserve}$(seconds). It starts a timer $T_{wait} = T_{reserve}$ (seconds) and counts down. The node comes back to its initial state when T_{wait} reaches 0. During T_{wait} seconds, if this source vehicle receives a Poll from any other node, it will stop the timer and then it will intermediately retransmit the recent message after a SIFS.



(a) Source nodes



(b) Neighbor nodes

FIGURE 3.4: Operation of devices implementing polling scheme

Fig.3.4(b) is the operation of a receiver implementing polling scheme. Based on the received BC, the node checks whether it has already got related data message or not. If not, i.e the given node is a non-data receiver, it will start a timer for transmitting a Poll within a DIFS. Similarly to BC, a Poll timer is set up by choosing a random number r from 1 to n_{mini} slots. The non-data receiver sends its Poll when Poll timer reaches 0. During counting down Poll timer, if it overhears a Poll from other, it will freeze its Poll timer and wait for data from the source node within SIFS. Timer T_{wait} is set to SIFS and counts down. Until T_{wait} reaches 0, if data message responding to the Poll is not retransmitted, the non-data receiver will continue its Poll timer and send Poll. After sending the Poll, if it does not get the requested data message, the procedure of sending Poll will be repeated. The non-data receiver stops the polling scheme after the maximum number of Poll repetitions without receiving data, or when it gets the data correctly, or when CCHI ends. The reserving time $T_{reserve}$ is the maximum time for Poll transmission and data retransmission.

$$T_{reserve} = DIFS + n_{mini}.Poll/R + SIFS + L/R, \tag{3.3}$$

where L, Poll and R denote the packet length including payload and headers, the length of a Poll, and the applied data rate.

3.3 Proposed polling scheme analysis

3.3.1 Assumptions

Reflecting unique features of WAVE and IEEE 802.11p such as multichannel operation and differentiated access categories, an appropriate performance evaluation model is designed in [20]. We generalize and extend the model to measure our scheme particularly for broadcasting in WAVE. The model extensively considers periodic safety messages within one CCHI of 50 ms. Our proposed polling scheme is analyzed in the worst-case scenario that each of n vehicles is supposed to have one periodic packet ready to be transmitted at the beginning of each CCHI. Due to the limited lifetime of 100 ms recommended for periodic safety messages in [50], it is reasonable to assume that non-transmitted messages after CCHI will be dropped. It is assumed that all nodes have carrier sense ranges within the communication range of each other. Since positions of nodes do not change significantly within a short time duration of 50 ms (i.e., less than 2 m for a vehicle moving at the speed of 100 km/h), mobility is not considered in this section. All computations are counted for one CCHI.

The model describes access contention for broadcasting of vehicles at the beginning of CCHI. Eight probabilities of transmissions (Table.3.2) that can happen in a slot are calculated based on the current number of contending vehicles and their remain slots in contention window. After a given slot, depending on what happens in this slot, the number of contending vehicles and their remain slots in contention window change.

These two parameters in next slot is influenced by the state of the previous one. If a given slot is a slot of a successful transmission, number of successful messages till this given slot increases by one. Therefore, number of successful messages after a CCHI can be obtained recursively slot by slot from the beginning to the end of CCHI. From number of successful messages, packet delivery rate can be derived.

3.3.2 Basic model

In our basic model, all periodic packets have the same priority (the same Arbitration Interframe Space AIFS and contention window). After a failed message, non-receivers request only one time for a rebroadcast. If the source fails to rebroadcast during the period for polling, the message will be dropped.

We define CSMA contending interval as a time interval which starts when every node senses the medium, backs off if needed, till the node transmits a message. With our polling scheme, each transmission can be considered to happen in a contending interval including two phases: first phase of CSMA contending interval (including carrier sensing, contending and transmitting), and the second phase of polling and retransmission if it is requested. In the first phase, let T_{s1} and T_{c1} (seconds) denote the duration of a transmission without collision and the duration of a collision respectively. Similarly, in the second phase, let T_{s2} and T_{c2} denote the duration of a successful retransmission and the duration of a failed request for retransmission respectively. T_{c1} reaches maximum when all BCs collide in all minislots. T_{s2} reaches maximum when all of Polls fail except the last one sent at the last minislot, and so do T_{c2} when all Polls fail till the last minislot. Since maximum values of T_{c1}, T_{s2} and T_{c2} reflect the longest time spent for BCs and Polls, we use them for evaluating the polling scheme in worst-case.

$$T_{s1} = L/R + DIFS + BC \tag{3.4}$$

$$T_{c_{1max}} = L/R + DIFS + n_{mini}.BC/R \tag{3.5}$$

$$T_{s_{2max}} = DIFS + n_{mini}.Poll/R + SIFS + L/R \tag{3.6}$$

$$T_{c_{2max}} = DIFS + n_{mini}.Poll/R + SIFS \tag{3.7}$$

These above values are measured in slots respectively as $s_1 = T_{s1}/\sigma$, $c_1 = T_{c1max}/\sigma$, $s_2 = T_{s2max}/\sigma$, $c_2 = T_{c2max}/\sigma$ where σ is slot time in seconds. Mentioned in above section, L, Poll and R denote packet length including payload and headers, length of a Poll, and applied data rate respectively. BC denotes the length of a broadcast confirmation.

The probability $P(l,n,w,k)(1 \leq l \leq w \ and \ 1 \leq k \leq n)$ that n vehicles select backoffs from a contention window of w slots, $l-1$ empty slots passed before the first transmission attempt, and k vehicles transmit in slot l^{th}, is computed in below equation:

$$P(l,n,w,k) = \left(1-\frac{l-1}{w}\right)^{n}.\begin{pmatrix} n \\ k \end{pmatrix}\left(\frac{1}{w-l+1}\right)^{k}.\left(1-\frac{1}{w-l+1}\right)^{n-k} \tag{3.8}$$

The above probability is modeled through a Bernoulli process. $\frac{1}{w-l+1}$ is the probability that a node chooses uniformly any slot out of $(w-l+1)$ available slots.

A group of nodes includes all nodes which have the same message type and the same number of slots remaining in their contention window. If there are more than one group of nodes in network, the model can be derived in (3.9) to compute the probability of having k_i nodes of group i transmit at slot l^{th}. There are n_i nodes of group i having w_i slots remaining in their contention window, m groups of nodes in the network, and i is from 1 to m.

$$\begin{aligned} P(l,N^{(m)},W^{(m)},K^{(m)}) &= P(l,n_1,n_2,...,n_m,w_1,w_2,...,w_m,k_1,k_2,...,k_m) \\ &= P(l,n_1,w_1,k_1).P(l,n_2,w_2,k_2)...P(l,n_m,w_m,k_m) \end{aligned} \tag{3.9}$$

where $i = 1..m$; $n_i \neq 0$. If $n_i = 0$ the element $P(l,n_i,w_i,k_i)$ will be absent in the above equation.

We define matrix $N^{(m)}$ as a matrix of n_i. Hence, $N^{(m)}$ describes the distributions of nodes in groups. $W^{(m)}$ is a matrix of respective contentions windows w_i. $K^{(m)}$ is a matrix of transmitting nodes k_i. For convenience, the uppercase letters are used for describing matrices and the lowercase letters are for numbers. All the probability of successful transmissions and probability of failed transmissions are summarized in Table.3.2. Because of the assumption that all nodes are in communication range of each other, a successful transmission means that all nodes receive the broadcast message. Similarly, a failed transmission means that no node gets the message. The computation of probabilities are elaborated as follows.

Probability of successful transmission

In the first phase, the message is transmitted successfully at slot l^{th} without error with probability P_{s1}. n nodes in network, which distribute in groups, are described by matrix $N^{(m)}$; $n = \sum_{i=1}^{m} n_i$.

$$P_{s1}(l,N^{(m)},W^{(m)}) = P(l,N^{(m)},W^{(m)},{K_s}^{(m)}).(1-p_e)^{L} \tag{3.10}$$

where p_e is bit error rate; ${K_s}^{(m)}$ is a matrix that has the sum of all elements equaling to 1, i.e. $\sum_{i=1}^{m} k_i = 1$. Otherwise, if error occurs, other nodes will request for missing data

TABLE 3.2: Probabilities descriptions

Denotes	**Description**	
	First phase	**Second phase**
P_{s1}	Successful	No Poll
P_{s2}	No collision, error data	Successful
P_{s3}	Collision, successful BC	Successful
P_{c1}	Collision, failed BC	No Poll
P_{c2}	No collision, error data	Successful Poll, error data
P_{c3}	No collision, error data	Failed Poll
P_{c4}	Collision, successful BC	Successful Poll, error data
P_{c5}	Collision, successful BC	Failed Poll, no retransmission

by a Poll. The source will successfully retransmit if at least one Poll is transmitted and no error for the retransmitted data message. It happens with probability P_{s2}.

$$\begin{aligned} P_{s2}(l, N^{(m)}, W^{(m)}) = P(l, N^{(m)}, W^{(m)}, {K_s}^{(m)}) \\ .(1-(1-p_e)^L).P_{spoll}(n-1).(1-p_e)^L. \end{aligned} \tag{3.11}$$

The successful polling probability $P_{spoll}(n-1)$ happens when there are $(n-1)$ nodes sending Polls and one Poll is transmitted successfully. It happens when at least one minislot (among n_{mini} minislots) is randomly chosen by only one node among $n-1$ nodes. It can be statistically obtained.

If n_c nodes collide in the first phase and one of their BCs is successfully sent with probability $P_{BC}(n_c)$, (n_c-1) nodes will arrange to retransmit in the next contending interval. The rest $(n-n_c)$ nodes will prepare their Polls to send. ${K_c}^{(m)}$ is a matrix that has sum of all elements equaling to n_c, i.e. $\sum_{i=1}^{m} k_i = n_c$. Probability of successful retransmission in the second phase after a collision is:

$$\begin{aligned} P_{s3}(l, N^{(m)}, W^{(m)}, n_c) =& P(l, N^{(m)}, W^{(m)}, {K_c}^{(m)}) \\ & .P_{BC}(n_c).P_{spoll}(n-n_c).(1-p_e)^L. \end{aligned} \tag{3.12}$$

where $P_{BC}(n_c)$ is obtained in similar method to P_{spoll} mentioned above.

Probability of failed transmissions

The message is lost when a collision occurs for both data message and BC and then no Poll is sent during the second phase. This case is denoted by probability P_{c1}. In the other cases of probability in Table. 3.2, after the first failed transmission, nodes enter the second phase for sending Polls. In this second phase, the message can be lost due to four reasons: getting error in both the first phase and the retransmission, denoted by

probability P_{c2}; getting error in the first phase and all Polls colliding in second phase, P_{c3}; collision in the first phase, successfully polling but error in retransmission, P_{c4}; collision in the first phase, one BC is sent successfully then nodes fail for polling leading to no retransmission, P_{c5}.

$$P_{c1}(l, N^{(m)}, W^{(m)}, n_c) = P(l, N^{(m)}, W^{(m)}, {K_c}^{(m)}).(1 - P_{BC}(n_c)). \tag{3.13}$$

$$\begin{aligned} P_{c2}(l, N^{(m)}, W^{(m)}) =& P(l, N^{(m)}, W^{(m)}, {K_s}^{(m)}) \\ & .(1-(1-p_e)^L).P_{spoll}(n-1).(1-(1-p_e)^L). \end{aligned} \tag{3.14}$$

$$P_{c3}(l, N^{(m)}, W^{(m)}) = P(l, N^{(m)}, W^{(m)}, {K_s}^{(m)}).(1-(1-p_e)^L).(1-P_{spoll}(n-1)). \tag{3.15}$$

$$\begin{aligned} P_{c4}(l, N^{(m)}, W^{(m)}, n_c) =& P(l, N^{(m)}, W^{(m)}, {K_c}^{(m)}).P_{BC}(n_c) \\ & .P_{spoll}(n-n_c).(1-(1-p_e)^L). \end{aligned} \tag{3.16}$$

$$P_{c5}(l, N^{(m)}, W^{(m)}, n_c) = P(l, N^{(m)}, W^{(m)}, {K_c}^{(m)}).P_{BC}(n_c).(1 - P_{spoll}(n-n_c)). \tag{3.17}$$

Number of successful messages

We define $X(t, N^{(m)}, W^{(m)})$, which is computed in (3.18), as the mean number of successful messages when there are t slots left in the CCH interval, w_i contention slots left in backoff counter of the vehicle group i, there are m groups and n_i vehicles in each group i, i is from 1 to m.

The denotation $X(t, N^{(m+1)}, W^{(m+1)}) = X(t, N^{(m)}+\{n_{m+1}\}, W^{(m)}+\{w_{m+1}\})$ means that a new group has been added to the network after a 2-phase contending interval,

where $N^{(m+1)} = N^{(m)} + \{n_{m+1}\} = [n_1\ n_2\ ...\ n_m\ n_{m+1}]$, similarly, $W^{(m+1)}$ is defined.

$$
\begin{aligned}
X(t, N^{(m)}, W^{(m)}) = & \sum_{l=1}^{min(w,t)} \{ \\
& \sum_{k=1} P_{s1}(l, N^{(m)}, W^{(m)}).(1 + X(t - l + 1 - s_1, N^{(m)} - {K_s}^{(m)}, W^{(m)} - L^{(m)})) \\
& + \sum_{k=1} P_{s2}(l, N^{(m)}, W^{(m)}).(1 + X(t - l + 1 - s_1 - s_2, N^{(m)} - {K_s}^{(m)}, W^{(m)} - L^{(m)})) \\
& + \sum_{k=2}^{n} P_{s3}(l, N^{(m)}, W^{(m)}, k).(1 + X(t - l + 1 - c_1 - c_2, N^*, W^*)) \\
& + \sum_{k=2}^{n} P_{c1}(l, N^{(m)}, W^{(m)}, k).X(t - l + 1 - c_1, N^{(m)} - {K_c}^{(m)}, W^{(m)} - L^{(m)}) \\
& + \sum_{k=1} P_{c2}(l, N^{(m)}, W^{(m)}).X(t - l + 1 - s_1 - s_2, N^{(m)} - {K_c}^{(m)}, W^{(m)} - L^{(m)}) \\
& + \sum_{k=1} P_{c3}(l, N^{(m)}, W^{(m)}).X(t - l + 1 - s_1 - c_2, N^{(m)} - {K_c}^{(m)}, W^{(m)} - L^{(m)}) \\
& + \sum_{k=2}^{n} (P_{c4}(l, N^{(m)}, W^{(m)}, k).X(t - l + 1 - c_1 - s_2, N^*, W^*) \\
& + \sum_{k=2}^{n} (P_{c5}(l, N^{(m)}, W^{(m)}, k).X(t - l + 1 - c_1 - c_2, N^*, W^*)\},
\end{aligned}
\tag{3.18}
$$

where $N^* = (N^{(m)} - {K_c}^{(m)}) + \{k-1\}$; $W^* = (W^{(m)} - L^{(m)}) + \{W_0\}$; $k = k_1 + k_2 + ... + k_m$; $n = n_1 + n_2 + ... + n_m$; $w = min(w_1, w_2, ..., w_m)$; ${K_s}^{(m)}$, ${K_c}^{(m)}$ are matrices that have the sum of all elements equal to k in each terms of the equation. $L^{(m)}$ is a matrix where every element is equal to l and has size of matrix $W^{(m)}$. W_0 is a matrix where every element is equal to the minimum contention window w_0 and has the same size of matrix $L^{(m)}$.

Each term of (3.18) corresponds to one probability defined in Table. 3.2. After a contending interval, one node succeeds when no collision occurs in the first phase while other nodes continue contending. Therefore, the number of groups of nodes in the network is still m; this is shown in calculation terms of P_{s1}, P_{s2}, P_{c2}, P_{c3}. However, if a collision occurs in the first phase, except the node wining BC and joining in the polling phase, all the collided nodes retransmit their data with the same minimum contention window (w_0). They make up a new group $(m + 1)$ with contention window w_0 in the next contending interval; this is shown in calculation terms of P_{s3}, P_{c4}, P_{c5}. The fourth term in (3.18) refers to P_{c1} in Table. 3.2. It is calculated for the case that collision occurs among data messages and also among BCs. Thus, there is no retransmission for all collided nodes. Consequently, in the next contending interval, only the nodes that have not attempted to transmit yet are left in the network and it still remains m groups of nodes.

$X(T, N^{(1)}, W^{(1)})$ is the total number of successful messages when there are T slots left in CCH interval (T is the maximum number of slots in CCH interval); $N^{(1)} = [n]$; $W^{(1)} = [w_0]$; where n is initial number of nodes that have contention window size w_0. The packet delivered rate PDR can be calculated as:

$$PDR = \frac{X(T, N^{(1)}, W^{(1)})}{n}. \tag{3.19}$$

3.3.3 Extended model for prioritized broadcasting

Concerning QoS for various services, IEEE 802.11e defines four access categories which is also addressed in IEEE 802.11p. As mentioned before in section 2.5.1, the four access categories (ACs) are listed in Table.2.1. ACs are prioritized by the Arbitration inter-frame spacing number (AIFSN) and minimum contention window ($CWmin$). A shorter AIFSN and shorter $CWmin$ mean that a message has a higher probability of being transmitted with low access latency. Respectively, ITS applications are mapped to access categories according to their importance and urgency. In the DSRC implementation guide of SAE J2735 standard from SAE International organization, several safety applications are described and mapped to respective access categories. For instance, crash-pending notification, pre-crash notification, collision warning are applications using highest priority access category (AC1). While emergency vehicles approaching, periodic public safety status information applications are mapped to second priority access category (AC2). Other non-safety applications, such as WAVE Service Announcement (WSA) and electronic payment, are mapped to the two lower priority access categories (AC3 and AC4).

With regard to multiple access categories, we modify and generalize the model to work with matrices of two dimensions. The matrices $N^{(m)}$, $W^{(m)}$, $K^{(m)}$ mentioned above change to two dimension matrices that describe one AC in each row and one group of nodes in each column. When there are n_{ij} nodes, which have w_{ij} slots left in their current contention window and belong to group j of AC_i in the network, matrix number of nodes $N^{(m)}$ can be defined as (3.20). Similarly, the matrix of the number of slots left in contention windows, $W^{(m)}$, can be defined.

$$N^{(m)} = \begin{bmatrix} N_1 \\ N_2 \\ N_3 \\ N_4 \end{bmatrix} = \begin{bmatrix} n_{11} & n_{12} & \dots & n_{1j} & \dots & n_{1m} \\ n_{21} & n_{22} & \dots & n_{2j} & \dots & n_{2m} \\ n_{31} & n_{32} & \dots & n_{3j} & \dots & n_{3m} \\ n_{41} & n_{42} & \dots & n_{4j} & \dots & n_{4m} \end{bmatrix} \tag{3.20}$$

where $i = 1..4$ refers to four ACs; $j = 1..m$ refers to m groups if m is the maximum number of groups that one AC may have.

Due to the differentiation of ACs, the contention among packets is divided into different access zones: $\Delta_i = AIFSN_i - AIFSN_1$ (slots), when $AC1$ has the smallest $AIFSN$, as they are depicted in Fig.3.5. During Δ_2, there are only contentions among

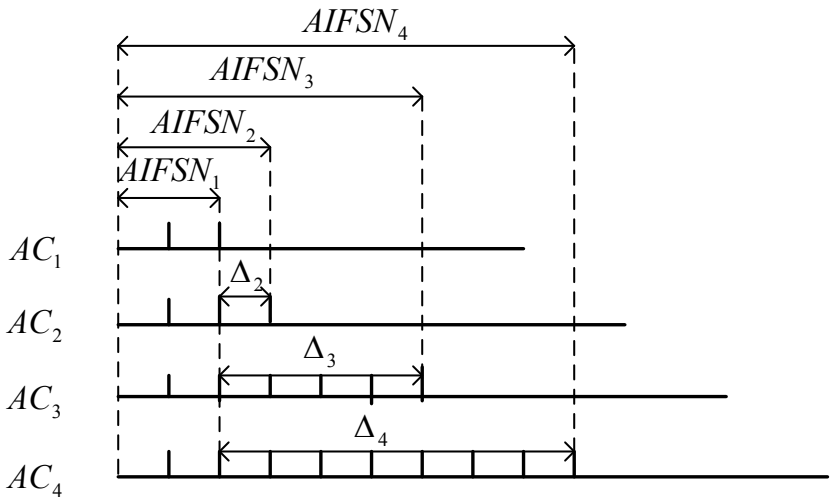


FIGURE 3.5: Four Access Catergories and Access zones

$AC1$ packets. From the end of Δ_2 to the end of Δ_3, only $AC1$ and $AC2$ packets contend for transmission. After Δ_3 to the end of Δ_4, $AC1$, $AC2$, $AC3$ packets contend. After Δ_4, packets of all ACs join the contention. The probability of transmission when there are k_{ij} nodes in group j of AC_i transmit at slot l^{th} is derived from (3.8) as below:

$$P(l, N^{(m)}, W^{(m)}, K^{(m)}) = \begin{cases} 0 & * \\ \prod_{a=1}^{i} P(l - \Delta_a, N_a, W_a, K_a) & ** \end{cases} \tag{3.21}$$

(*): if $\Delta_i < l \leq \Delta_{i+1}$ and $\sum_{i'=i+1}^{4} \sum_{j=1}^{m} k_{i'j} \neq 0$

(**): if $\Delta_i < l \leq \Delta_{i+1}$ and $\sum_{i'=i+1}^{4} \sum_{j=1}^{m} k_{i'j} = 0$; where the distribution of transmitting nodes k_{ij} in groups is described by matrix $K^{(m)}$; $1 \leq l \leq min(w_{ij} + \Delta_i)$. The above term of (3.21) means that when $l \leq \Delta_{i+1}$, probability that a node having higher access category index (lower priority) than ACi packet transmits is 0, because a node cannot transmit during its AIFS. The below term of (3.21) is the computation for the rest cases. With the assumption that messages have the same length, computation of transmission probability in (3.21) is placed to (3.10)-(3.18). Consequently, probabilities and number of successful messages can be derived as functions of t and two-dimension matrices $N^{(m)}$,$W^{(m)}$, provided that sum of all elements in transmitting matrix K_s or K_c is equal

to k. The k and w in (3.18) follow below rules:

$$k = \begin{cases} \sum_{j=1}^{m} k_{1j} \text{ if} 1 \leq \mathrm{l} \leq \Delta_2, \\ \sum_{j=1}^{m} (k_{1j} + k_{2j}) \text{ if} \Delta_2 \leq \mathrm{l} \leq \Delta_3, \\ \sum_{j=1}^{m} (k_{1j} + k_{2j} + k_{3j}) \text{ if} \Delta_3 \leq \mathrm{l} \leq \Delta_4, \\ \sum_{j=1}^{m} (k_{1j} + k_{2j} + k_{3j}) \text{ if} \mathrm{l} \geq \Delta_4, \end{cases} \tag{3.22}$$
$$w = min(w_{ij} + \Delta_i), where\ i = 1..4\ ,\ j = 1..m$$

$X^{(1)}(T, N^{(1)}, W^{(1)})$, the total number of successful messages when there are T slots left in CCH interval, and packet delivered rate can be calculated respectively.

3.4 Reliable MAC protocol in dissemination of safety messages

As mentioned above, safety services require the reliability measured by the percentage of vehicles receiving the safety messages, not only within transmission range but also a large area covering all the vulnerable vehicles. It is necessary to consider concurrently MAC protocol in dissemination scenario on which safety messages are spread out to notify as many vehicles as possible with the shortest latency.

In order to support dissemination in vehicular networks, several dissemination protocols for broadcast messages are proposed [51][28]. RSU system is exploited to efficiently and reliably route the packet to far location in the network in [76]. An efficient routing protocol for connecting vehicular networks to the internet is proposed in [11]. The routing protocol supports seamless handover, when a vehicle moves to the communication range of a new gateway, by spreading the advertisement message of the new gateway to the approaching vehicles. The authors introduce stability metric to select relays which have the most stable links to the sender. To deal with the broadcast storm which highly affects the design of dissemination protocol, forwarder smart selection protocol is proposed in [102]. The source vehicle is able to calculate inter-vehicle distances among its nearby neighbors. Nearby vehicles form a cluster. After defining clusters, the source node elects and forwards the packet to only cluster-heads. Cluster-heads become the relays forwarding the message to the next hop. Therefore, the number of copies of safety messages transmitted in the networks is controlled. Within one hop communication, in our polling scheme, only the source rebroadcasts the safety message. Thus, the broadcast storm is avoided. We aim to investigate our polling scheme also in multi-hop broadcasting but not to design an optimized dissemination protocol. Hence, we choose a basic distance-based dissemination protocol, instead of an enhanced dissemination protocol to study.

Distance-based dissemination protocols, which are classified into the category of position-based forwarding protocols mentioned before in chapter 2, are well studied

in the literature. However, they are not studied together with proposals for MAC protocols. In these protocols, the packet is forwarded multi-hop by relays. Generally, the idea is that relay candidates set up a timer according to their distances to the source. The furthest node will have the shortest timer and be the first one forwarding the packet to next hop, other candidates suspend their timers. Obviously, the duration of timers set up by relays plays a vital role in this solution. However, delay for packets queued in MAC layers changes the time that the packet is broadcast. This makes the packet be transmitted later even the timer is shorter, and reversely. This may make the upper layer dissemination protocol work improperly.

A dissemination protocol for alarm messages on which relays are chosen based on their distance to the source node is proposed in [8], called ODAM protocol. The author builds the protocol on top of the Internet Protocol (IP) with an assumption of using IEEE 802.11 for MAC protocol. However, according to the standard IEEE 1609.3, IP messages are not suggested for safety applications. Due to above reasons, it urges for a design that suitably implements both MAC protocol and dissemination protocol in a device.

In this work, we implement a distance-based dissemination protocol directly on top of MAC protocol skipping IP protocol. Values of parameters used in the dissemination protocol are proposed in consideration of realistic implementation of the two protocols while they are only mentioned in general in other related works [8][60]. The coverage of safety messages within one hop is supported by our polling scheme at MAC layer. Then these safety messages are transmitted multi-hop to all vehicles by selected relays which have the furthest distance to the previous hop relay. Moreover, the impact of reliable MAC protocol to dissemination is also investigated in this section.

The suit of protocols is managed as a process of two phases: local operation phase aiming to assure the reception within transmission range and forwarding phase in order to broadcast the packets to next hop. This process is repeated again in each hop till the packet is expired or dissemination distance reaches a threshold (chosen by application providers).

3.4.1 Local operation

A safety message is initially broadcast by an origin node which detects the danger and wants to warn others in the network. Our polling scheme is performed by all nodes in one transmission range of the source. We assume that a neighbor node requests for rebroadcasts maximum x times. Thus, the maximum duration of the local operation phase is estimated as a sum of duration for broadcasting a BC T_{BC}, waiting time for one DIFS for Poll T_{DIFS}, the duration for sending a Poll T_{Poll}, if any, and duration for rebroadcasting data packet T_{DATA}. It can be calculated as follows:

$$T_{local} = x.(T_{BC} + T_{DIFS} + T_{Poll} + T_{Data}) \tag{3.23}$$

The next phase will start when the local operation finished (after a period of T_{local} from the first received packet).

3.4.2 Forwarding mechanism

After receiving a safety message, nodes acting as relay candidates set up their timers according to the distance from them to the source and start counting down. They start broadcasting the message to next hop whenever their timers reach 0. Because the further node is, the shorter timer it has, the furthest node will be the first one transmitting the packet, others will cancel their forwarding processes. In order to limit the probability of more than one relay rebroadcast at the same time that leads to collisions or duplicated packets, the transmission range is divided into small segments of one vehicle length $l_{veh}(m)$, i.e., only vehicles within a distance of l_{veh} have the same timers. Total number of segments in a transmission range is defined as $N_{Seg} = \frac{R}{l_{veh}}$, where R is the transmission range.

Regarding to OSI layered network model, a packet is moved from higher layer to MAC layer before transmitted to the medium. The packet is downward to MAC layer queue, but it is not transmitted intermediately due to DCF/EDCA procedure specified in the standard IEEE 802.11. During the waiting time in MAC queue, another node having a longer timer than the given node probably transmits prior because the packet may be downward to MAC layer later but the node wins the medium and has a chance to transmit earlier. Taking into account this fact, we propose a time step definition. A time step is a time duration, after each time step, relay candidates reduce their timers by one if no transmission of forwarding packet has been detected. The value of a time step is approximately equal to the propagation time of a packet from the source to the node at the distance of a transmission range.

The forwarding timer of node i, T_{F_i} (seconds), is inversely proportional to the distance from the source or the previous relay to node i.

$$T_{F_i} = T_{local} + \left[\frac{R - d_i}{R}\right] .N_{seg}.T_{seg} \tag{3.24}$$

where T_{local} is the waiting time for local operation phase before forwarding, d_i is the distance from node i to the source, N_{seg} is the total number of segments and T_{seg} is a duration of a time step.

Nodes in next hop receive the forwarded packet and perform the same process of local operation and forwarding. By that way, successful transmissions within one hop are provided with high probability. Consequently, the total performance of the dissemination protocol may be improved in term of receive ratio.

3.4.3 Effect of MAC protocol to dissemination performance

In this subsection, we raise a discussion about how MAC protocol impacts to a dissemination which has not been addressed in existing works. The question is how a reliable MAC protocol improves the dissemination performance, i.e., if the successful probability of one-hop transmission is improved, how the success rate of dissemination within multi-hop varies.

In order to consider the impact of MAC protocol to dissemination protocol, we assume that the dissemination works under the best situation, i.e., the emergency message is forwarded by the only and furthest relay. Vehicles distribute along the roads according to Poisson process with average density λ. Let d denote the average distance between current hop relay and previous hop relay. P_{mac} denotes successful probability within one hop. Since in two dimensions space, a dissemination can be described as a symmetric process, at this point, we consider one direction dissemination. Number of nodes that receive at first hop is $P_{mac}.\lambda.d$ while the number of non-data receivers/nodes is $(1 - P_{mac}).\lambda.d$. From the second hop, due to the overlap transmission range of nodes at two consecutive hops, the number of covered vehicles (nodes received the message) comprises the number of vehicles that received message in previous hop, number of non-data receivers in previous hop but covered by the overlap transmission in current hop, and number of vehicles in current hop that receive the message recently. Therefore, at hop h^{th} ($h \geq 1$), number of covered vehicles is computed as below equation:

$$\begin{aligned} \chi^{(h)} &= P_{mac}.\lambda.d + (h-1).P_{mac}((1-P_{mac}).\lambda.d + \lambda.d) \\ &= (2h - 1 - (h-1).P_{mac})P_{mac}.\lambda.d \end{aligned} \tag{3.25}$$

Let P_0 denote the successful transmission probability within one hop (at MAC layer) with the standard IEEE 802.11p. Δ denotes an improvement in successful transmission probability at MAC layer when any reliable MAC protocol is applied. Successful transmission probability when a reliable MAC protocol is applied is $(P_0 + \Delta) \leq 1$. According to (3.25), the number of covered vehicles at hop h^{th}, when we apply a reliable MAC protocol, can be calculated as:

$${\chi_{reliable}}^{(h)} = (2h - 1 - (h-1).(P_0 + \Delta)).(P_0 + \Delta).\lambda.d \tag{3.26}$$

It is easy to obtain below (3.27) when we process above (3.26) (Appendix A).

$$\begin{aligned} {\chi_{reliable}}^{(h)} &= {\chi_0}^{(h)} + \left[-(h-1).\Delta^2 + (2h - 1 - 2(h-1).P_0).\Delta\right].\lambda.d \\ &= {\chi_0}^{(h)} + I(h, P_0, \Delta, \lambda, d) \end{aligned} \tag{3.27}$$

while ${\chi_0}^{(h)}$ is the number of covered vehicles when using the standard protocol. The

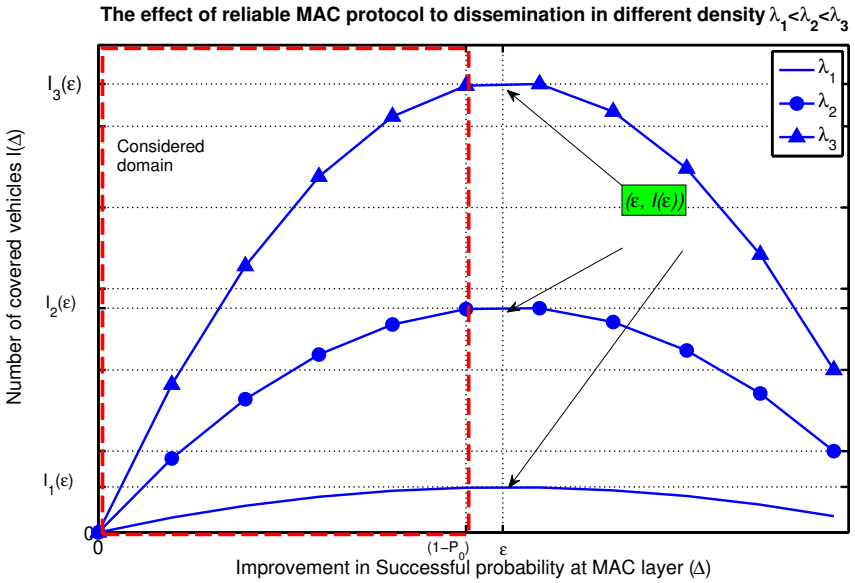


FIGURE 3.6: The effects of reliable MAC protocol to dissemination protocol

right portion of (3.27) is an improvement, $I(h, P_0, \Delta, \lambda, d)$, in term of number of received vehicles when a reliable MAC protocol is applied. The improvement is a function of four parameters: the number of hops that the messages is forwarded, the successful probability of the standard MAC protocol, density, the distance between relays, and the improvement at MAC layer transmission when applying a reliable MAC protocol.

Aiming to consider the impact of MAC protocol to dissemination protocol, we consider function $I(h, P_0, \Delta, \lambda, d)$ corresponding to the argument Δ (Appendix A), called $I(\Delta)$. As the function is in quadratic function format with negative first coefficient $(-(h-1).\lambda.d)$, its graph has downward parabola shape, as it is shown in Fig.3.6, with turning point $(\varepsilon, I(\varepsilon))$; where $\varepsilon = (1-P_0) + \frac{1}{2(h-1)}$; $I(\varepsilon) = \frac{(2h-1-2(h-1).P_0)^2.\lambda.d}{4(h-1)}$; $\lambda_1 < \lambda_2 < \lambda_3$; It can be proved that $\varepsilon > (1-P_0)$ (Appendix A).

As $0 \leq \Delta \leq (1-P_0)$, we pay attention only on this feasible domain. As the first coefficient of the function depends linearly on h, λ and d, an adjustment in the number of hops that message is transmitted, and/or density and/or the position of relays can decide how much a reliable MAC protocol can help the dissemination. An increase of any of these arguments can lead to a bigger improvement in dissemination. With the same value of h and d, the higher density λ is, the faster function increases (Appendix A), i.e. a reliable MAC protocol can improve the overall success ratio of dissemination protocol better in high density. While in a sparse network, the improvement is insignificant.

3.5 Performance Evaluation of proposed polling scheme

The information contained in safety messages is important and real time. Thus, packet delivery rate and delay are appropriate metrics to evaluate the performance of protocol proposed for vehicular networks. Moreover, channel utilizing efficiency should be also taken into account when multichannel operation is adopted. Our polling scheme is evaluated by three metrics: the packet delivery rate, the delay and the percentage of duplicated packets. The packet delivery rate is the ratio of the number of successfully received packets and the total number of generated packets. The delay is counted for a successfully received packet from when the packet is transmitted till it is received at a receiver. Percentage of duplicated packets is the percentage of duplicated packets over the total number of received packets at receivers.

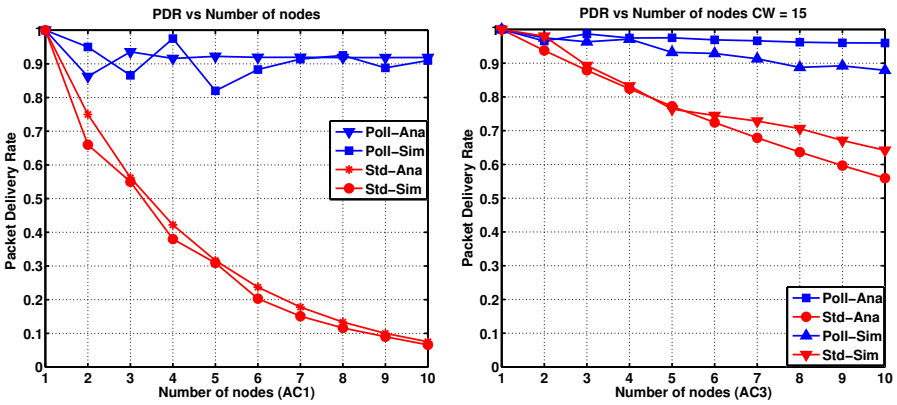
TABLE 3.3: Simulation Parameters

MAC Parameter	***Value***
Slot time (σ)	13 μs
SIFS	32 μs
Propagation delay (δ)	1 μs
Switching time (t_switch)	1 μs
Data Rate (R)	3 Mbps
Packet Length (Payload + Header)	500 Bytes
BER (p_e)	10^{-4}
BC, Poll length	16 Bytes
One hop experiment parameter Packet arrival rate (one hop communication experiments) - Beacons (AC2) - Event messages (AC1)	 10 packets/s 1 packets/s
Transmission range	250 m
Dissemination experiment parameter	
Vehicle arrival rate in a vehicle flow: - Highway (2-4 flows) - Urban (5-10 flows)	 0.2 - 1 (vehicles/s/flow) 0.04 - 0.22(vehicles/s/flow)
Simulation area - Highway - Urban	 2-4 lanes, 10 km 1 km^2
Number of vehicles (total)	100 vehicles
Transmission range	250 m
Beacon size	100 Bytes
Beacons arrival rate	10 packets/s

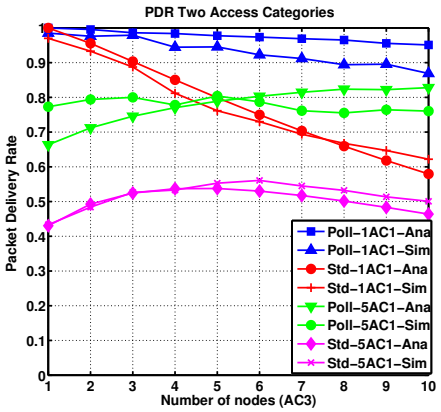
In our analytical model and simulation, we choose a set of parameters which is familiar in vehicular networks: 3 Mbps is the lowest acceptable data rate in vehicular networks; packet length of 500 bytes is normal packet length for safety message which can include additional security header. The length of BC and Poll is 16 bytes. Other parameters used in computation and simulation are listed in Table. 3.3.

3.5.1 One-hop communication

We resolve the analytical model in Matlab and validate it by simulations in NS-3. In order to study our polling scheme in one-hop communication, nodes in simulations are located in a circle so that everyone is in other's communication range. Fig.3.7 shows the packet delivery rate as a function of the number of nodes when each node has one message ready to be sent at the beginning of a CCHI. Each simulation is repeated for 100 CCHIs and the results are the average values that we obtained.



(a) CW = 3 (b) CW = 15



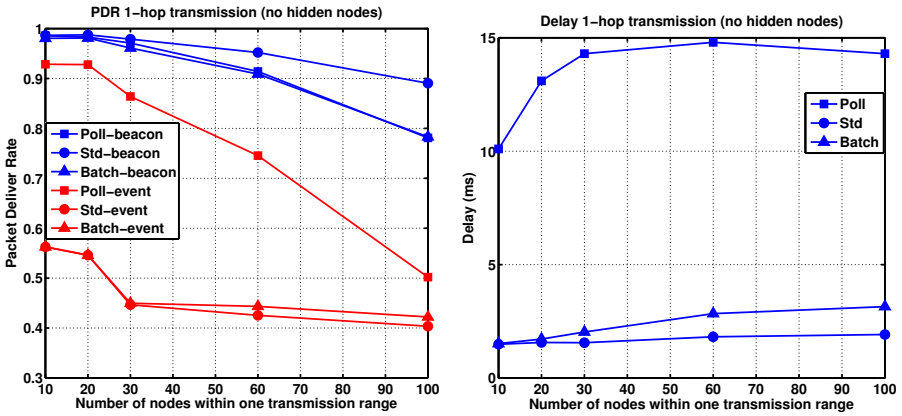
(c) Two Access Categories

FIGURE 3.7: Analytical Model Validation

Our polling scheme performs a significant improvement in term of packet delivery rate (PDR) compared to standard MAC protocol as it is shown in Fig.3.7. In our polling scheme, failed packets are rebroadcast hence the PDR is improved. In basic case where all packets have the same priority, our polling scheme performs 80% higher PDR than the standard for $AC1$, shown in Fig.3.7(a) and 40% for $AC3$ in Fig.3.7(b). The result of using polling scheme is shown in Fig.3.7(c) for packets of two access categories. Compared to the standard, our polling scheme shows an improvement of up to 60% in packet delivery rate when there are 1 packet $AC1$ and from 1 to 10 packets $AC3$

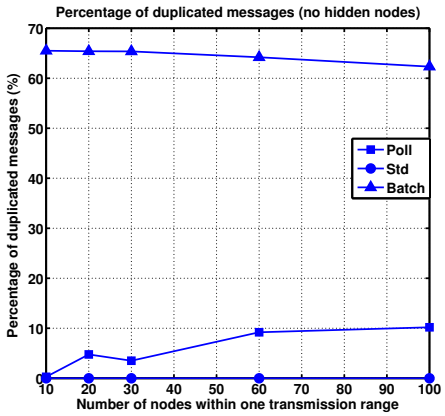
contending at the beginning of each CCHI, and up to 50% when number of packets $AC1$ is 5.

We compare our protocol to a related work, which has the same objectives to ours, proposed in [43]. Aiming to make broadcasting in vehicular environment more reliable, [43] proposes a batch scheme at MAC layer on which a safety message is rebroadcast the defined number of times consecutively per SIFS. A ring topology where nodes are located in a circle is used in order to consider one-hop communication. Fig.3.8 and Fig.3.9 show the PDR and delay as functions of the number of nodes within one transmission range with and without the impact of hidden nodes. The density can be computed based on the average distance between each pair of nodes. The number of nodes in the circle can be referred as the number of nodes within one hop communication in the simulation. Nodes switch alternatively between one control channel and one service channel every 50ms. Waiting packets in queues are flushed when each CCHI ends. Each node sends periodically 100-Byte beacons $AC2$ with $CW = 7$ at the arrival rate of 10 packets/s and the higher priority event messages $AC1$ of 500Bytes with $CW = 3$ at arrival rate of 1 packet/s. Proposed protocols are applied for event messages.



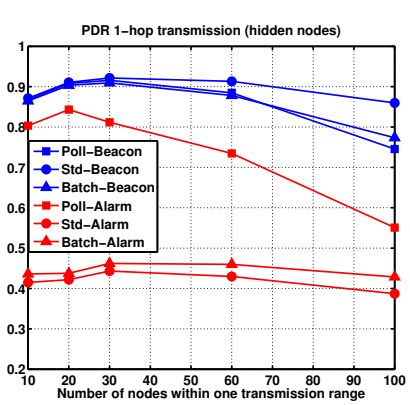
(a) PDR

(b) Delay for event messages

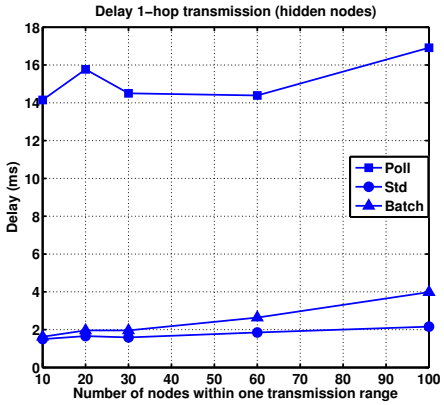


(c) Duplicated percentage of event messages

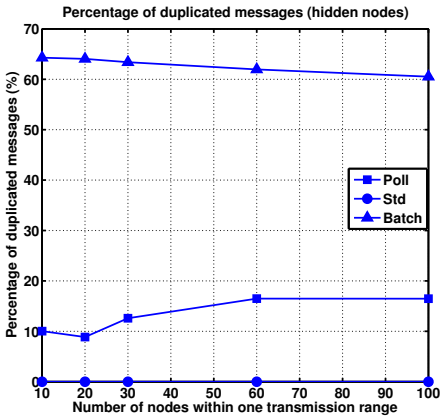
FIGURE 3.8: One hop communication no hidden nodes



(a) PDR



(b) Delay for event messages



(c) Duplicated percentage of event messages

FIGURE 3.9: One hop communication under impact of hidden nodes

Fig.3.8 shows the performance when all nodes are in coverage range of each other, i.e., the topology circle has a diameter of one transmission range of approximate 250 meters. In the standard and the batch scheme, event packets have 50% lower success ratio than beacons while it is balanced when we use polling scheme. The rebroadcast of batch scheme helps to improve the success ratio of event packets while packet delivery rate of beacons drops slightly. On the other hand, our polling scheme balances the performance of beacons and event packets. PDR obtained with our scheme is 20% higher than the batch scheme when the network becomes dense with 100 nodes within one transmission range. With our polling scheme, we obtain the PDR of 0.8, similar to the batch scheme, for beacons and 0.5 for event messages in this density. Fixed redundancy (percentage of duplicated packets) of 60% for event messages generated in the batch scheme may create collisions and occupy the medium. This leads to drop packets due to switching channel, especially when there are a lot of vehicles contending. While our polling scheme creates duplicated messages only if a part of the network does not receive messages, the rebroadcast messages will be duplicated for the rest vehicles. When the number of nodes within one hop communication reaches more than

60 nodes, the percentage of duplicated packets stops increasing and stays at 10%. Because collisions likely occur to short messages, they lead to no notification or request for rebroadcast is received and no retransmission is conducted.

The impact of hidden nodes is taken into account in our second simulation. The result is shown in Fig.3.9. A bigger circle has a diameter of two transmission ranges is added around the one transmission range diameter circle in the previous experiment. 10 nodes located in the big circle play a role of hidden nodes to the one-hop communication of nodes within the small circle. In Fig.3.9, performance metrics are calculated for the nodes in the small circle. The BCs and Polls work as a NAV notification. BCs inform a duration of the next Poll waiting time while Polls inform the duration of their following expected data packets. From this information, other nodes defer their access in order to avoid collisions. This helps to reduce collision created by hidden nodes. In Fig.3.9(a), our polling scheme shows up to double success ratio compared to the standard and the batch scheme for event messages in our simulation with hidden nodes. Our polling scheme presents a longer delay of 10 ms to 15 ms in both two experiments of no hidden nodes and hidden nodes, compared to approximately 2 ms in the standard and the batch scheme. This can be considered as a tradeoff for PDR improvement. However, this delay is acceptable for safety services that require the delay to be smaller than 100 ms.

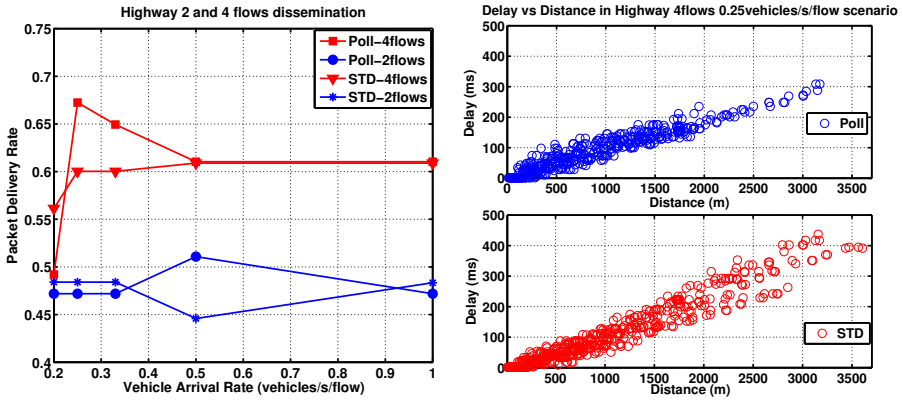
3.5.2 Dissemination in urban and highway scenarios

We evaluate the suit of protocols described before (polling scheme integrated into a distance-based dissemination protocol) in 10 km highway with 2 to 4 flows of cars coming from two opposite directions. We also set up an experiment in an urban scenario which is exported from a 1-kilometer-square real map of Hanoi city, Vietnam. Vehicle mobility is generated in Simulation of Urban Mobility (SUMO) simulator. In the urban scenario, 5 and 10 flows of vehicles with random origin-destination are generated. In both two scenarios, 100 vehicles are injected into the network as traffic flows, at arrival rate from 0.2 to 1 vehicles per second per highway vehicle flow, and from 0.04 to 0.22 vehicles per second per urban vehicle flow, within a simulation time of 15 minutes. The higher vehicle arrival rate and/or number of vehicle flows are, the higher density is. Their speed is limited by street descriptions in the real map. We choose one source among 100 vehicles in the network to initialize safety message dissemination after first 200s of simulation. Performance is evaluated for instantly presenting vehicles in the simulation.

Besides safety applications requiring dissemination of event messages to notify hazards, there are other safety applications which pay attention also on nearby neighbor nodes such as emergency brake application or blind spot warning, etc. These applications require both periodic safety messages (beacons) and event messages. Taking into account this fact, in our simulation, vehicles broadcast periodically beacons of 100

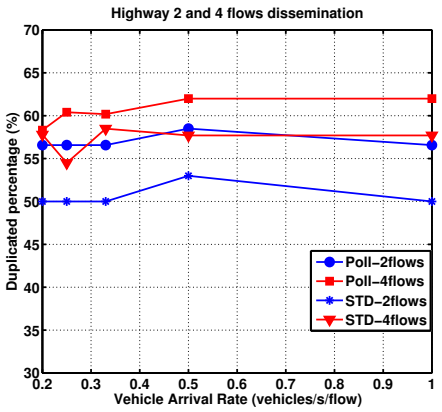
Bytes in Poisson process at arrival rate of 1 packets/s in scenarios of urban and 10 packets/s in scenarios of highway. On another hand, some selected source nodes broadcast randomly event messages of 500 Bytes that is suggested for the length of safety short messages in WAVE. According to different event messages generated time, we obtain several results.

Fig.3.10 and Fig.3.11 show the average success ratio and delay in highway and urban area when the dissemination is carried on with and without our polling scheme. The fragmentation in the network may occur. Results count for these interruptions during the dissemination. The event message may be important for all vehicles in the network not only in the one-hop neighborhood and the content of the message changes gradually. Thus, information contained in event messages remains true for few seconds. Therefore, we assume that event packets are kept in the queue for a maximum delay of 10 s while other packets are flushed every 50 ms as an effect of switching channel.



(a) Packet Delivery Rate

(b) Delay



(c) Duplicated

FIGURE 3.10: Performance of dissemination protocol implementing polling scheme in highway scenario

Fig.3.10 shows the result in highway scenario with 2 flows and 4 flows. In the scenario of 2 flows and low vehicle arrival rate, i.e, low density, the dissemination protocol

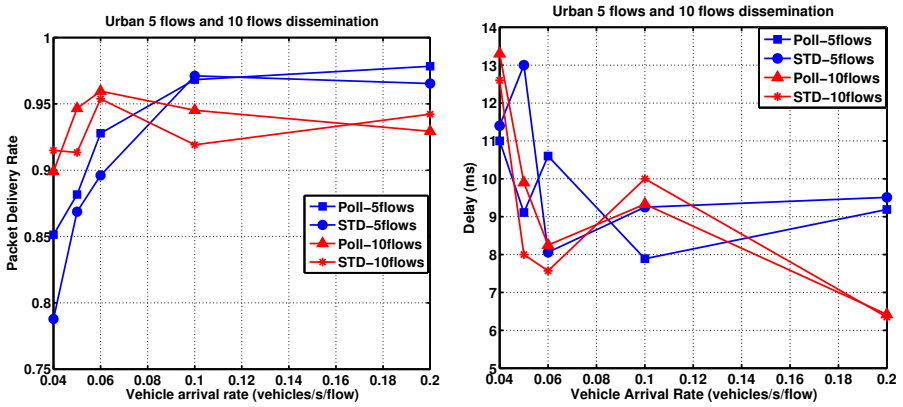
with our polling scheme has a better PDR only when vehicle arrival rate is bigger than 0.5 vehicles/s/flow. This is the consequence of sparse network, i.e., there are not many nodes within an area of a transmission range. The forwarding can play a role of a retransmission of the event message. Thus, even some nodes in the previous hop miss the event safety message, they can be covered by a transmission of a relay to next hop. Our polling scheme well performs when we increase the number of flows to 4. Dissemination with our polling scheme implemented at MAC layer has PDR of nearly 0.7 when the network becomes denser due to the increase of vehicles arrival rate. However, the PDR drops again when vehicle arrival rate keeps rising to 1 vehicles/s/flow and there is no improvement even we apply polling scheme at MAC layer.

Fig.3.10(b) describes delay of the event message that vehicles at different distances receive in highway scenario of 4 flows and vehicle arrival rate of 0.25vehicles/s/flow. Although the dissemination with our polling scheme has higher PDR than dissemination with the standard IEEE 802.11p, it has lower coverage distance of 3300m compared to 3700m. In the upper figure in Fig.3.10(b), using our polling scheme, vehicles which are close to each other have similar delays. Otherwise, in the lower figure in Fig.3.10(b), delays of neighbor vehicles are more diverse. The reason is that the forwarding of relays plays also the role of retransmission of lower layer protocol. Some vehicles receive the safety messages when the source vehicles broadcast while some others have to wait until the relays rebroadcast to forward the messages to next hop.

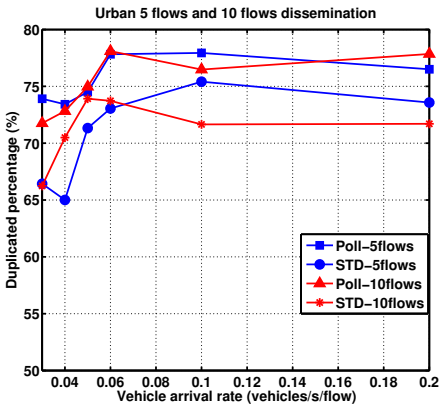
On the other hand, our proposed polling scheme performs quite higher PDR and lower delay in urban scenario Fig.3.11. With our polling scheme, the transmission within one hop is more reliable. Thus, neighbor nodes receive the event message right when the one-hop transmission is done. Therefore, the delay is quite lower. 5 flows of vehicles are not dense enough to show the congestion cases on which a drop in PDR to radio collision should be observed. For instance, in the urban scenario of 10 flows, there is a drop of PDR for both our polling scheme and standard MAC protocol when the vehicle arrival rate reaches 0.06 vehicles/s/flow.

In both two scenarios, our polling scheme shows slightly higher duplicated percentage compared to the standard, nearly 10%. The packet forwarding of relays may play a role of retransmission the safety messages, together with retransmission of polling scheme, this leads to the increase of duplicated percentage.

In comparison with one hop communication, the MAC protocol implementing our polling scheme performs insignificant improvement in PDR in dissemination scenarios. The packet forwarding also plays a role of retransmission for the previous hop communication. However, our proposed scheme reduces delay that a vehicle gets the safety message. Vehicles within each hop transmission are almost guaranteed to receive event messages before the forwarding to the next hop is carried on. It can be said that our polling scheme is more suitable for one-hop broadcast communication. Our polling scheme does not give priority to any specific type of safety message. Hence,



(a) Packet Delivery Rate (b) Delay



(c) Duplicated

FIGURE 3.11: Performance of dissemination protocol implementing polling scheme in urban scenario

it is compatible with background traffic such as periodic messages. In practical, periodic messages are used for supporting such ITS safety applications that require high frequency such as emergency vehicle warning, slow vehicle indication, intersection collision warning [2].

3.6 Conclusions

In this chapter, we have introduced a polling scheme, a new approach for increasing the reliability of broadcasting non-prioritized and prioritized traffic in vehicular network. Considering the individual characteristics of the standard IEEE 802.11p and IEEE 1609.4, the scheme is modeled and evaluated in multichannel operation, error-prone conditions, and effects of different access categories. Our polling scheme can support high reliable one-hop communication in term of percentage of vehicles receiving the safety-related information. It is suitable for nearby safety services such as emergency braking light, collision risk warning due to hidden obstacles, etc.

Disseminating event messages in emergency situations is another expected safety application in vehicular networks. Therefore, we have also integrated the MAC protocol implementing our polling scheme into a dissemination protocol in order to study if our protocol is able to support this type of safety services. The suit of protocols is studied and compared to existing standardized protocol IEEE 802.11p in highway and urban scenarios. In highway scenario with 4 traffic flows, we have obtained good results for our proposed suit of protocols. Besides, a low packet delivery rate in highway scenario of 2 traffic flows (sparse network) shows a need for an opportunistic protocol to overcome the fragmentation of the network. In the next chapter, we will discuss the fragmentation of the network which is one of the traits of vehicular communication environment.

Chapter 4

Connectivity enhancement for safety applications in vehicular networks

Besides local communication within a concerned area, multi-hop communication is also important for safety applications in vehicular networks. The nature of vehicular networks requires specific designs for forwarding protocols to disseminate broadcast messages to everyone and/or to deliver a message to predefined destinations. In vehicular networks, the distribution of vehicles in roads are frequently scattered by infrastructure planning. Vehicles commonly move from dense areas to sparse areas [100]. Therefore, communications among vehicles are available in some areas while in another part of the network, vehicles are isolated. The forwarding of a packet from a vehicle to a destination at far distance has to deal with the fragmentation of the network, in the other word, the lack of connectivity problem. Looking back in literature, opportunistic forwarding protocols are good candidates to overcome this problem since they allow the message to be forwarded opportunistically when the connectivity is available. They use different parameters such as positions, trajectories, speed, etc., to determine which vehicles have opportunity to approach the destination and then deliver the forwarded message to. In our work, we use parameters that are inspired by the social characteristics of vehicular networks. We propose a social-based forwarding protocol to support multi-hop communication of some kinds of safety applications in VANETs. Our objective is to support safety applications that deliver slightly urgent but important information from an area of the incidents to points of interest (e.g., special vehicles, roadside stations) in the networks. The position of the destination may be unknown. We evaluate our protocol in urban scenario. The relevant connectivity analysis of the studied scenario is also presented.

This chapter resumes approaches that deal with the temporary disconnection in vehicular networks. These approaches are defined as opportunistic forwarding protocols in our definition. The remainder of the chapter is organized as follows: the first section of the chapter presents the overview of opportunistic forwarding approaches in VANETs and social characteristics of vehicular networks; section 4.1 provides a resume of related opportunistic forwarding protocols that aim to overcome the poor connectivity problem in multi-hop communications; our proposed protocol is described in

section 4.2; section 4.3 presents the setup and connectivity analysis of the studied scenario; The simulation results are discussed in section 4.4; the chapter is concluded in section 4.5.

4.1 Opportunistic forwarding approaches in Vehicular networks

4.1.1 Overview of opportunistic forwarding protocols in VANETs

Opportunistic forwarding protocols are proposed to overcome the temporary disconnection in the network. The disconnection in the network interrupts the forwarding of the safety message. The message is stored by a vehicle but there is no other available vehicle in the forwarding direction. Therefore, the forwarding stops at this point and the packet is dropped. The common idea of opportunistic forwarding protocols is that the packet is stored when the disconnection occurs and it is rebroadcast when the connectivity is available. Whenever a vehicle storing a packet, called a carrier, detects a relay candidate within its transmission range, it decides whether to forward or not the packet to this relay candidate according to the forwarding strategy defined in the forwarding protocol. The question is which vehicles can store and forward the packet toward the destination.

Due to the fragmentation of the network, the paths/routes from the origin to the destination in term of communication do not always exist. Moreover, because the network topology changes quickly, the paths are dynamic. Therefore, when carriers are selected, we can not guarantee the existence of the paths or routes. Carriers belonging to a path (from the origin to the destination) are chosen provided that the path is available with "high probability". A given vehicle storing a packet decides to forward the packet to one of its neighbors, that is the next hop carrier candidate, if this carrier candidate has a high probability of reaching the destination directly or indirectly via several hops. On other words, carrier candidates are weighted by its previous carrier. Depending on the parameters that carrier candidates are weighted, opportunistic forwarding protocols in vehicular networks can be classified into different categories such as position-based protocols and social-based protocols.

Majority of opportunistic forwarding protocols in vehicular [22, 45, 58, 109, 23] are position-based protocols. Vehicles are selected based on their positions since a vehicle which is close to the destination and/or on the way approaching the destination has a high probability of reaching the destination. They may combine different parameters such as geographical information, the traffic condition and mobility patterns, etc..

The geographical information such as road network information is commonly used in opportunistic forwarding protocols due to the availability of digital map which is probably installed in vehicles. A road network can be abstracted by a graph in which vertices are intersections and edges connecting two intersections are road segments. MDDV [106] specifies forwarding trajectory from a source to the destination region

based on the position of the destination and traffic condition reflected by road networks. The forwarding trajectories include high traffic road segments, therefore, they have high vehicle density which often leads to fast information propagation. The packet is stored and forwarded by vehicles moving along the forwarding trajectory.

VADD [109] calculates packet-delivery delay for each road segment based on vehicle density, vehicle velocity and one-hop transmission delay of vehicles at this road segment. In VADD, the packet is carried and forwarded closer to the destination and along the high speed path including low packet-delivery delay road segments. Similarly to VADD, authors in [45] proposes a forwarding protocol that calculates expected forwarding time for each road segment but the calculation for dense road segments is different from sparse road segments. Based on exchanged historical mobility patterns of vehicles, vehicles predict future trajectories of their carrier candidates to decide to forward the packet if the carrier candidate is moving toward dense road segments.

The GeoDTN+Nav[23] protocol allows vehicles to operate in three modes: greedy mode and perimeter mode when the network is connected and DTN (delay tolerant network) mode when the destination is disconnected. Packets are forwarded in greedy manner first then in perimeter mode when they get stuck in the local maximum (there is no further relay to reach the destination). If the perimeter mode also fails, the packets are stored and forwarded in DTN mode. In DTN mode, carriers are chosen based on the route information of vehicles. This route information includes the trajectory, destination, or direction which vehicles move along with certain probabilities, call confidences. The confidence is a parameter defined by a Virtual Navigation Interfaces which is an extra equipment for cars. This route information is broadcast periodically.

In addition to the position information, social properties have been utilized in forwarding protocols, in particular, they may be utilized in opportunistic forwarding protocols to deal with fragmentation in the network, especially, when the position of the destination is unknown. As social properties of a node reflect its ability to encounter other neighbors, utilizing social relation allows packets to be forwarded to the popular area where they have more chance to find clues of their destinations. The social aspect of vehicular networks is elaborated in the following subsection.

4.1.2 Social aspect of vehicular networks

Social properties of vehicular networks

A social network is a network made up by a set of individuals connecting with each other. Their interconnection base on social relationships. Social networks attract a lot of attention of researchers recent years due to its worldwide applications such as Facebook, Twitter, etc. Analysis of social networks reveal several laws, for instances, power-law distribution of node degrees, small world phenomenon and clustering. These laws may bring benefits to designing and implementing social networks applications.

In vehicular networks, cars or vehicles, in general, move following the roads and communicate to each other opportunistically. As vehicles are driven or controlled by humans, they should demonstrate some human social behaviors. Besides, road systems are constructed to supply the transportation demand of their citizens, the movement of vehicles are restricted on the road systems and hence, there may be repetition in the movement of vehicles. Therefore, it may exist social properties in vehicular networks. Indeed, the analysis of Liu et al. [65] shows that several universal laws of social networks are reserved in vehicular networks. Their study shows that vehicle-to-vehicle communication has similarity to human-to-human interaction. Encounters of vehicles are considered as their relationships and VANET is modeled as a social graph. The existence of social properties in vehicular networks is also proved in the work of Cunha et al.[26].

Social perspective of vehicular networks is expressed by relationships of vehicles. For examples, the number of encounters reflects how popular the node is; nodes having a large number of common neighbors are likely to know each other and may meet each other more frequently. In other words, relationships of vehicles in the network are quantified by several social metrics such as centrality[103], tie strength (showing the strength of the relationship)[27], tie predictor or clustering coefficient[26].

There are common social metrics used in social network analysis to investigate human relationships. We will briefly describe some common social metrics that can be used in MANETs and so vehicular networks as follows.

Centrality metrics measure the importance of a node in a social network. A node with higher centrality is extensively involved in relationships with other nodes. Centrality is computed by its attributes: node degree, betweenness and closeness [27]. Node degree measures the number of direct links to a given node, i.e. number of vehicles having direct communication with a given vehicle in a vehicular network. Betweenness reflects mutual knowledge among neighbors of a node. It is calculated from the number of links that can be established between each pair of neighbors. Closeness describes how central the node is in term of geodesic distance. Closeness is measured as a reciprocal of the mean of shortest paths between the given node to all reachable neighbors.

Tie strength indicates how strength the relationship between two nodes is. The tie strength is reflected by frequency and recency metrics which shows how frequent and how recent they meet. There are other attributes to tie strength such as longevity which is duration of time that two nodes are in contact.

Clustering coefficient or tie predictor, individuals having the same interests such as same direction, or trajectory, or destinations in vehicular networks, tend to meet each others more often or travel in the same cluster. There is a chance that they will meet each other in the future[26]. This future encounters of vehicles may be predicted based on this comment. Tie predictor between two nodes is determined by number of their common neighbors [27].

Utilizing social metrics in forwarding protocols in VANETs

Several forwarding approaches in VANETs have been implicating social metrics depending on applications that they support but they have not deal with the problem of disconnection or fragmentation in networks [39][17]. There are not many works that integrate social properties in opportunistic forwarding protocols in vehicular networks. Moreover, selecting which social metrics for efficiently forwarding the information to a destination in vehicular environment is another question to be answered.

Centrality metrics are the most common metrics exploited in proposals for forwarding in VANETs. A social-aware routing protocol based on fuzzy logic algorithm is presented by Gu et al.[39]. The main idea of fuzzy logic algorithm is that a node is selected as the next relay according to its centrality and its distance to the destination. Authors in [17] propose a new centrality metric, called dissemination capacity which indicates the ability of a node to reach others not only direct 1-hop neighbors but also further. The metric is used for selecting rebroadcasting vehicles to support video streaming over VANETs. The fragmentation of vehicular networks is taken into account in proposal of Alganas et al.[4] and Lu et al. [68]. Packets are stored and forwarded by high centrality RSUs. However, the presence of roadside system is vital in these solutions.

Above social-aware opportunistic forwarding protocols work under assumption of availability of roadside system, digital map, knowledge of road system. Furthermore, they do not consider the constraints of radio resources, i.e. exchanged information between neighbors should be very limited, especially in dense and congested areas. In our work, we consider vehicle-to-vehicle communication without the assistance of roadside system. We propose a social delay tolerant approach to support communication between vehicles to special stations that can be emergency vehicles or safety fixed station. The approach has no need for extra equipments in cars. All information used for forwarding is collected via exchanged beacons. We assume that position of the destination is unknown. Additionally, resource constraints are taken into account in our protocol. The information exchanging in periodic messages between neighbors is kept concise. Radio transmission is modeled with its radio environment's nature such as propagation loss, distortion and medium access contention collisions.

4.2 Social-aware forwarding approach for safety services in Vehicular network (SocVe)

Beside hazardous warning application (notification of a hazardous incident), there are other safety applications that are less urgent but important safety related services such as emergency services following an incident to update the status, request for search and rescue service, or support accident preventing. For example, Jagannathan et al. [52] introduce an artificial intelligence methodology that analyzes current traffic flow

data obtained from road sensors and makes a prediction regarding accidents. The communication between traffic controller and relevant vehicles allows an immediate traffic adjustment that may reduce the risk of accidents happen. In order to support this kind of safety applications, we present a studied scenario which describes the communication between vehicles to one or more predefined important nodes in the network denoted by the term "Point of Interest". These nodes can be mobile or static. This type of safety application requires high reliability while accepts loosened delay constraint compared to hazardous warning application.

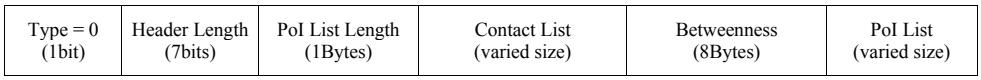
Dealing with the high dynamic topology in vehicular networks, we search for network characteristics which vary more slowly but still reflect the instant topology on the other hand. Social parameters can be a good candidate to reflect the connectivity of the networks. Based on that, suitable carriers can be determined. They have more chance to meet many other vehicles including the destination since they likely have better connectivity compared to others. Addressing to the application's requirement and features of vehicular networks such as fragmentation and intermittent connection, we suggest using specified social metrics in our Social-aware Vehicular delay tolerant protocol (SocVe).

As mentioned before, according to Freeman [34], the centrality metric is defined based on the number of direct links that involve a given node called node degree, the mutual knowledge among its neighbors called betweenness and the number of reachable nodes in the network namely closeness. Because of the mobility, links between nodes are time-varying, tie strength metric is envisioned. The tie strength metric provides the information of how frequent and recent a given node meets its neighbors. The more frequent and recent neighbor is, the stronger relationships they have. Besides, we can predict potential connection by using information from the past, for example, if two nodes have a high number of common neighbors, their future encounter likely occurs. They called it the similarity. In this work, we utilize node degree, betweenness, tie strength and similarity because less control data is needed to be exchanged but rich information is obtained.

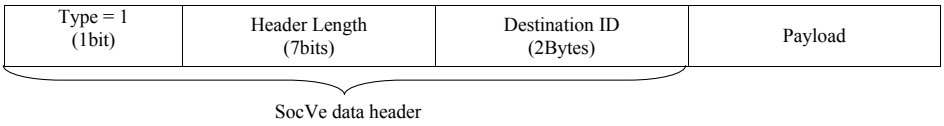
4.2.1 Beacon and SocVe header design

Beacons are periodic messages exchanged among vehicles which are within transmission range of each other. The use of beacons aims to announce the presence of a vehicle and its social metrics. We design the beacon with a concern of optimizing the size of beacons.

A beacon format shown in Fig.4.1(a) comprises a type field kept as 0 for beacon and 1 for data header, a header length field indicating the length of the SocVe header for beacons, PoI List Length that shows the number of encountered PoIs, Contact List field including the list of encountered neighbors, Betweenness field and PoI List including the list of encountered PoIs.



(a) SocVe beacon



(b) SocVe data frame

FIGURE 4.1: Formats of SocVe frames

PoI List is a list of PoI contacts. A PoI contact is a structure of PoI ID, tiestrength and similarity of the given vehicle to an encountered PoI. The size of PoI List and Contact List varies according to values of social metrics of the given vehicle.

A SocVe data header described in Fig.4.1(b) is added to a data packet in order to reserve destination ID during the forwarding process.

4.2.2 Forwarding process

Based on received beacons from neighbors, vehicles calculate their social metrics including centrality, betweenness, and its tie strength and similarity to PoI if any encounter. Then the calculation of their metrics is attached in their own beacons. Social metrics of neighbors and of a given vehicle itself are compared. After that, the given vehicle decides the next carrier who continues the forwarding process.

- **Centrality:**

The centrality metric of a vehicle includes degree – the number of its encounters during a predefined duration, and betweenness – calculated according to the existing indirect paths between each pair of its neighbors. Degree of a given vehicle n_0 is computed as the total number of direct links to n_0.

$$C_D(n_0) = \sum_{k=1}^{N} a(n_0, n_k) \tag{4.1}$$

where N is number of neighbors of vehicle n_0; $a(n_0, n_k) = 1$ if there exists a direct link between n_0 and n_k. The betweeness metric of a given vehicle n_0 is originally computed from the number of paths between each pair of its neighbors [103] as below:

$$Bet(n_0) = \sum_{i=1}^{N} \sum_{\substack{=0,\\ \neq i}}^{N} \frac{g_{i-j}(n_0)}{g_{i-j}} \tag{4.2}$$

where $g_{i-j}(n_0)$ is number of paths linking vehicle n_i and vehicle n_j via vehicle n_0 and g_{i-j} is the total number of indirect paths connecting n_i and n_j. In our protocol, the lists of direct neighbors of vehicles included in beacons are exchanged. Implementing principles of ego networks where only a given vehicle and its direct neighbors are concerned, the betweenness metric can be redefined by building and processing adjacency matrix[32]. The adjacency matrix is a matrix NxN that has elements 1 and 0, determined as below:

$$A_{i,j} = \begin{cases} 1\ ,\ if\ there\ is\ a\ direct\ link\ between\ n_i\ ,\ n_j \\ 0\ ,\ otherwise \end{cases} \tag{4.3}$$

The betweenness metric is computed from matrix $A^{'} = A^2[1 - A]$ where element ${A^2}_{i,j}$ of matrix A^2 is the number of indirect path connecting two vehicles n_i and n_j via another vehicle; 1 is a matrix of 1's. The betweenness metric is the sum of reciprocals of elements $A^{'}_{i,j}$ of matrix $A^{'}$:

$$Bet(n_0) = \sum_{i=0}^{N} \sum_{\substack{=0 \\ \neq i}}^{N} \frac{1}{A^{'}_{i,j}}$$

The adjacency matrix is updated once a new beacon is received.

- **Tie Strength:**

Tie strength metrics include frequency and recency. Frequency indicates the number of times that a given vehicle encounters a given PoI. Frequency metric of vehicle n_0 to PoI p is calculated as below equation:

$$FI_{n_0}(p) = \frac{f(p)}{F(n_0) - f(p)} \tag{4.5}$$

on which $f(p)$ is the number of times vehicle n_0 encountering PoI p, $F(n_0)$ is the total number of times that vehicle n_0 has encountered other vehicles from the beginning of the simulation.

Recency is defined as how recently vehicle n_0 last met PoI p. It is computed as following equation:

$$Rec_{n_0}(p) = \frac{rec_{n_0}(p)}{T(n_0) - rec_{n_0}(p)} \tag{4.6}$$

where $rec_{n0}(p)$ is the duration of time from the time that vehicle n_0 started joining the network to the time that vehicle n_0 last met PoI p, $T(n_0)$ is the duration of time that n_0 has been taken part in the network.

- **Tie predictor:**

Once a vehicle encounters a POI, it computes the similarity to the POI. The higher number of common neighbors results in the higher probability that a given vehicle moves regularly to across this PoI. We use similarity as a core metric for calculating the tie predictor metric.

$$Sim_{n_0}(p) = N_{n_0} \cap N_p \tag{4.7}$$

where N_{n_0} is a set of neighbors of vehicle n_0 and N_p is a set of neighbors of PoI p.

- **Choosing carrier**

The decision of choosing the next carrier is made based on the utility calculation whenever a source or a carrier detects a new neighbor. If the new neighbor has a higher total utility compared to the given vehicle, the packet will be forwarded. The utilities are computed from pair-wise comparisons.

$$DegUtil_n(m) = \frac{C_D(m)}{C_D(m) + C_D(n)} \tag{4.8}$$

$$BetUtil_n(m) = \frac{Bet(m)}{Bet(m) + Bet(n)} \tag{4.9}$$

$$FIUtil_n(m,p) = \frac{FI_m(p)}{FI_m(p) + FI_n(p)} \tag{4.10}$$

$$RecUtil_n(m,p) = \frac{Rec_m(p)}{Rec_m(p) + Rec_n(p)} \tag{4.11}$$

$$SimUtil_n(m,p) = \frac{Sim_m(p)}{Sim_m(p) + Sim_n(p)} \tag{4.12}$$

$$SocVeUtil_n\,(m,p) = \sum u_n(m) + \sum u_n\,(m,p) \tag{4.13}$$

Vehicle n decides next carriers based on total utility $SocVeUtil_n\,(m,p)$ calculation in (4.13). Respecting the corresponding social metrics, utilities $u_n(m)$ and $u_n\,(m,p)$ for vehicle m are normalized by social metrics of the given vehicle n. These utilities are: centrality utilities(4.8)(4.9), tie strength utilities to POI p (4.10)(4.11), similarity utility to PoI p (4.12). For simple, the total utility is the sum of all non-weighted utilities of social metrics.

Packets are stored by carriers within duration of time namely store duration D_s. During the store duration, whenever a carrier detects a better one, it forwards the packet to that new carrier. In early experiments, we choose a fixed value of D_s of 300 seconds.

4.3 Experiment Setup

In this work, we would like to study a new metropolitan city dataset – Hanoi city where old French style transport system and modern roads coexist. This feature of Hanoi's road system leads to a big diversity of road sizes and respectively various network densities.

We evaluate our SocVe protocol in NS-3. We consider a region of 5000 m x 10000 m extracted from the map of urban districts in Hanoi city by SUMO mobility simulator.

4.3.1 City map

In order to set up the simulation, we use Simulator of Urban Mobility (SUMO) to generate nodes' mobility and NS-3 as a communication simulator. SUMO exported map in Fig.4.2 shows bridges crossing the Red River, urban streets and a belt highway. City streets allow speed up to 40 km/h while the highway requires the speed ranging from 70 km/h to 110 km/h. Vehicles move in the network according to the mobility generated by SUMO which respects properties of roads in the city map. They obey the natural regulation of transportation such as reasonable acceleration, distance between cars, traffic lights and speed limit.

For communication protocol, we use NS-3 on which SocVe protocol is implemented and also lower layers are simulated. Specifically, the standard IEEE 802.11p with a bandwidth of 10 Mhz and Nakagami-m propagation loss model are chosen for MAC and physical layers in simulation. They are suggested for Dedicated Short Range Comunication studies[41]. The combination of SUMO and NS-3 allows us to evaluate our protocols in a specific real city where road properties and respective traffic are closely and visually abstracted.

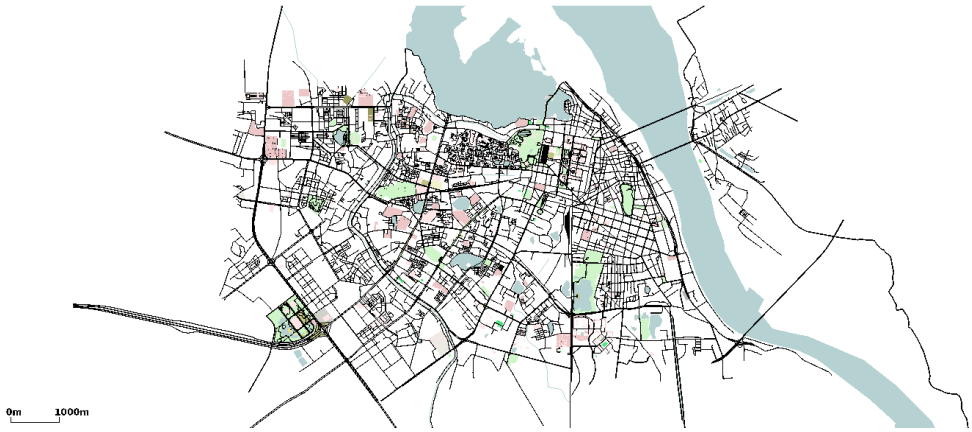


FIGURE 4.2: Extracted map of Hanoi

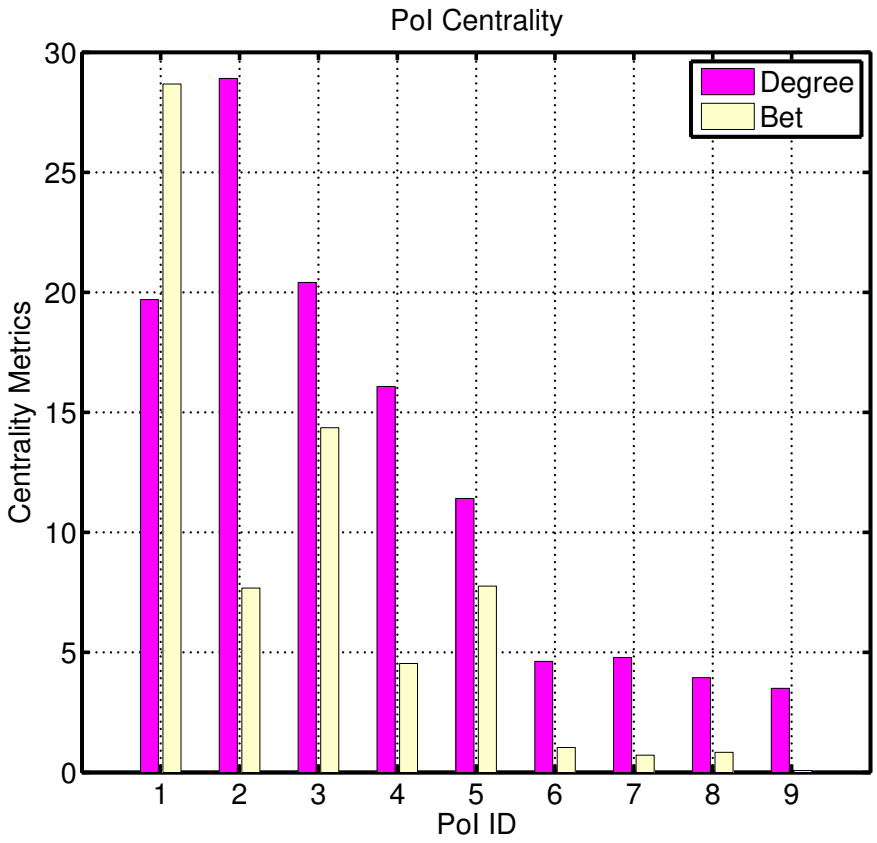


FIGURE 4.3: Centrality of Points of Interest (PoIs)

We evaluate SocVe with regard to the popularity of the PoIs. Depending on positions, PoIs should have different levels of centrality (degree and betweeness), as some PoIs in the central area may encounter more vehicles than the other in the rural area. In order to study separately impact of different PoIs to the performance of the protocol, three groups of common centrality PoIs are picked up in the map for simulation: high centrality (PoI ID 1, 2, 3), medium centrality (PoI ID 4, 5, 6), and low centrality (PoI ID 5, 6, 7). Centrality metrics of PoIs calculated during the simulation are presented in Fig.4.3. High centrality PoIs are located very central in the city such as next to the main train station or coach stations, along main streets and near to the Hoan Kiem Lake which marks the center of Hanoi, main post office and national bank. Medium centrality PoIs are chosen at about 4 to 5 kilometers around the center where we find houses, schools and commercial center. Low centrality PoIs are close to the outskirt of the city.

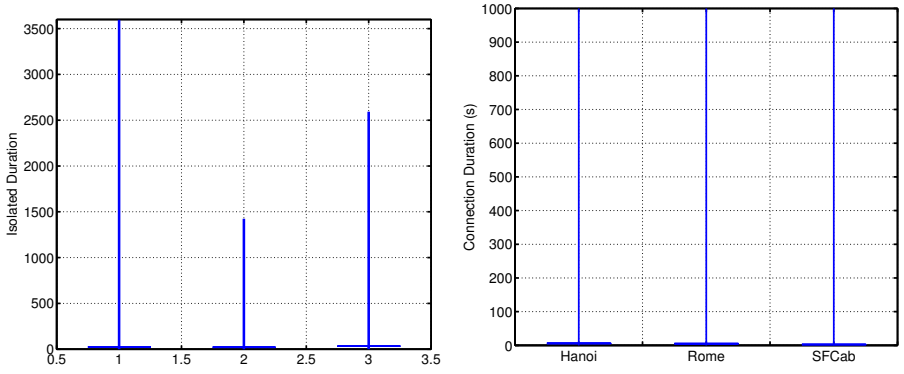
4.3.2 Connectivity analysis

The network topology can be modelized as a graph of social relationships [21]. It reflects the connectivity of the network. The performance of social-aware forwarding protocols is impacted by connectivity properties of the studied network. Hence, it is necessary to analyze the connectivity of the network when implementing forwarding protocol in order to get a relevant evaluation of the protocol in the concerned scenario.

We analyze the connectivity of Hanoi mobility data set that is generated in SUMO as described before. The connectivity is analyzed in term of isolation duration, in-contact duration and the average number of contacts (neighbors) that a vehicle has during each 10 s. We also compare our data set to San Francisco cab data set and Rome taxi data set.

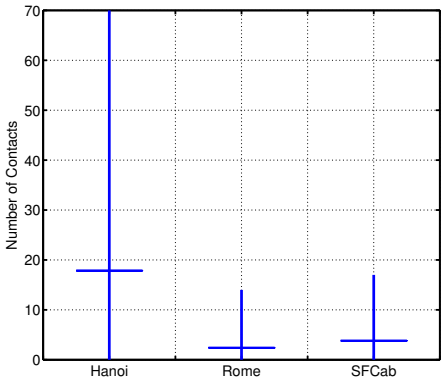
Based on exchanged beacons, information of the connectivity can be collected. Every vehicle sends periodically one beacon every 1 s. A vehicle is assumed to be in contact with another if it receives at least one of his beacons within 3 s. It is considered as isolated if it is not in contact with anyone.

In the context of mobility traces, we perform analysis of 150 vehicles-Hanoi data set, 134 taxis-Rome traces [16] and 100 cabs-San Francisco Cab traces [87]. Hanoi scenario shows some strike differences. Fig.4.4 performs a comparison of traces. Fig.4.4(a) and Fig.4.4(b) show the isolation duration and the connection duration. Hanoi has the mean isolated duration of 24.1 s which is higher than 21.5s in Rome data sets. On the other hand, Hanoi scenario's connection duration has the mean of 5.74s, and maximum of 3600 s which are similar to the two other data sets. It is significantly high compared to transmission duration of a safety message which in milliseconds.



(a) Isolated duration

(b) Connection duration



(c) Number of contacts

FIGURE 4.4: Topology Analysis

Fig.4.4(c) shows a diverse density in the network in Hanoi scenario. Although the

mean number of contacts in Hanoi of 17.8 is much higher than the two others 2.4 and 3.81 respectively, this number varies a lot around the mean value, from 0 to 70. It reflects a high dynamic topology where a given vehicle likely moves from a very sparse region to a very dense one. Moreover, in term of radio medium, it shows a fluctuating connectivity among vehicles in the network, i.e, even vehicles are close but they are probably disconnected temporally due to medium collisions or propagation loss of the communication channel.

As our objectives are safety applications in vehicular networks, we focus on the characteristic of Wireless Ad-hoc Vehicular Environment (WAVE) which includes the short connection, lack of connectivity problem and the strong impact of radio environment. Above features of Hanoi scenario match to our objectives.

4.4 Simulation Results for the studied experiment

The simulation is set up with 120 cars entering the networks during first 100 s and 5 bus lines which have 30 buses alternatively departing every 300s. Cars move in the map with repeated trajectories between random origins and destinations. The simulation is executed in an hour, during that time the total number of vehicles presenting in the network is 153 nodes including 3 PoIs, 30 periodic buses and 120 cars.

Among cars, 3 random cars are chosen as sources sending a group of 10 400-Byte event safety messages to 3 PoIs every 200s. In reality, there may be a situation that an incident occurs and its information can be frequently updated by groups of event messages with the same context. Messages in each group are sent every interval of 10 s. Any message of a group is received at the PoI, the information is considered to be delivered successfully to the destination. The success ratio is the proportion of the number of times the POI receiving the information and the total number of times that the information is transmitted in a form of a group of 10 messages. Delivery delay is the average delay from when the messages are sent until they are received at each PoI. The experiment is repeated 3 times in which sources are changed in order to avoid the case that sources always have high centrality or they are particularly close to PoIs.

The performance of SocVe is shown in Fig.4.5. Respective success ratio and delay to three groups of PoIs are presented. The average success ratio reaches nearly 90% for the scenario of the high centrality PoIs. Besides, the delivery delay shows its independence to the PoIs'centrality. Compared to the higher centrality group, the lower centrality group has a longer delay. The delivery delay at the low centrality group is about 30% longer than at medium centrality group; the delivery delay at the medium centrality group is 40% longer than at the high centrality group.

Also we obtain a significant improvement of 80% - 90% in success ratio of SocVe compared to the scenario without opportunistic protocols (i.e, only flooding protocol is implemented) on which almost packets are lost, only 10 % are received in high centrality PoI scenario due to the availability of connection in central area. This is shown in

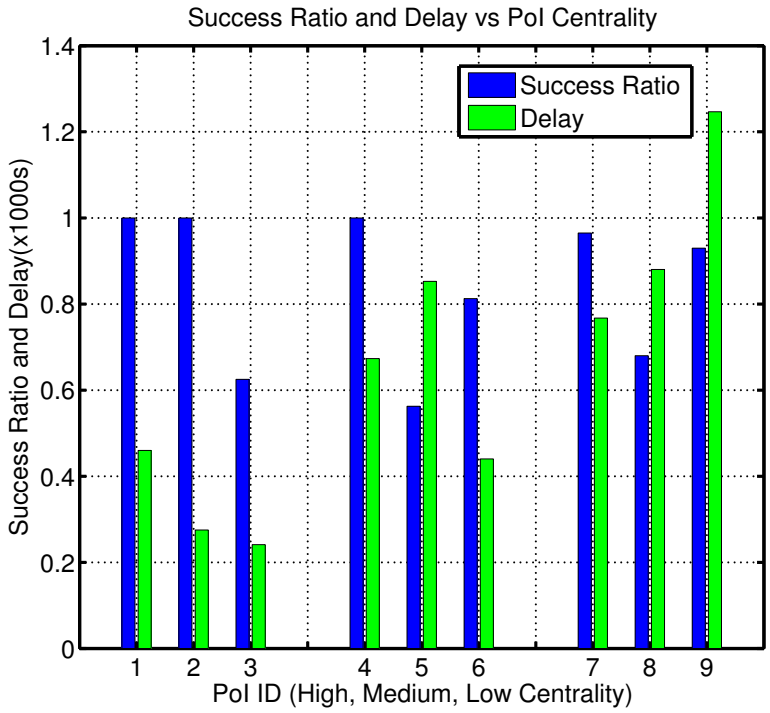


FIGURE 4.5: SocVe Success Ratio versus PoI Centrality

Fig.4.6 which proves that our protocol can deal with the fragmented network in Hanoi scenario.

In Fig.4.6, we compare also SocVe to a position-based opportunistic routing protocol, Distance-Aware Epidemic Routing (DAER) [69]. In DAER, vehicles store and forward packets to other vehicle that is closer to destinations. In order to limit the rapidly expanding number of stored and forwarded packets, carriers stop storing whenever they figure out that they are moving further from the destinations. We assume that positions of the destinations are known in the simulations of DAER protocol, while in simulations of our SocVe, the assumption is released.

SocVe shows a higher average success ratio of 40% compared to DAER for low and medium PoI groups. While both SocVe and DAER perform closely success ratios for high centrality PoIs, 88% and 78% respectively. Forwarding packets to a vehicle that is closer to a PoI brings the packets closer to the PoI instantly. For high centrality PoI, many vehicles have high probability to encounter PoI, many of them have nearly the same social heuristics thus SocVe do not outperform in this case. On the other hand, for PoIs at rural areas, without social- aware, packets do not have a chance to be brought to popular network regions where they have more choices for next carriers and higher probability to meet the best carriers. Therefore our protocol performs better for lower centrality destination.

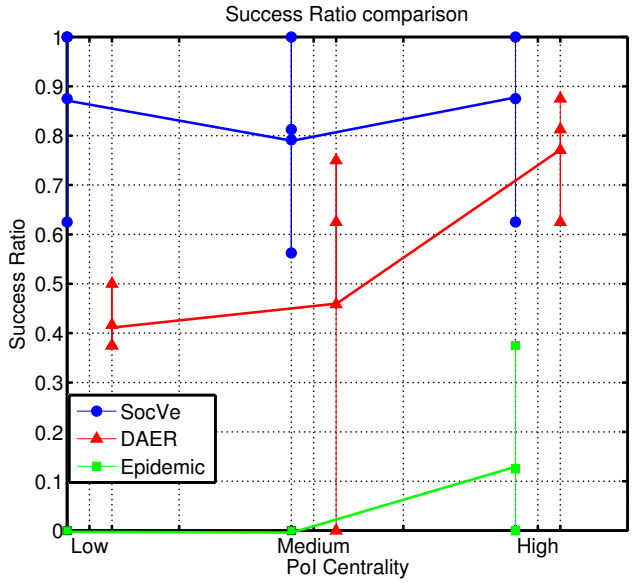


FIGURE 4.6: Success Ratio SocVe, DAER, Epidemic protocol

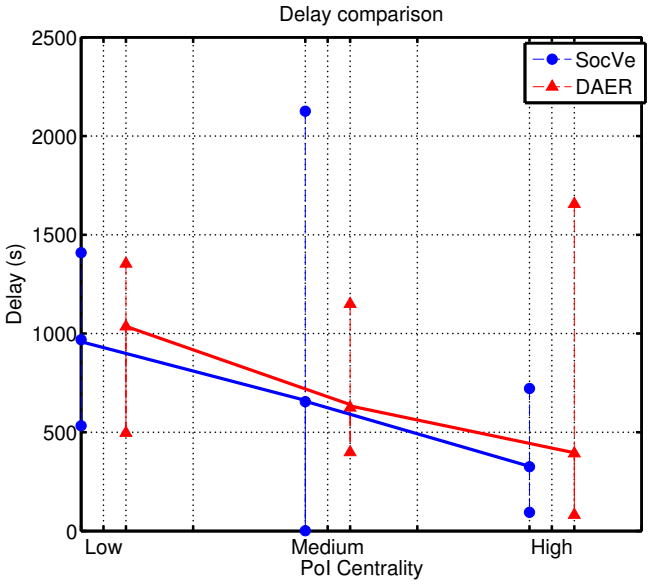


FIGURE 4.7: Average Delay SocVe and DAER

Delays for received packets experiencing two protocols are shown in Fig.4.7. For low centrality PoIs, PoIs are rarely encountered, SocVe presents an average delay similarly to DAER. While in high centrality POI scenario, the average delay of SocVe decreases significantly to 300 s and DAER delay reduces to 400 s. From social aspect, not many vehicles know rural PoIs, thus it takes time for them to search someone in relation with the PoIs, it leads to a longer delay for the low centrality PoIs.

In SocVe, carriers are determined based on social metrics measured by number of contacts (centrality), their encounter frequency, encounter duration and number of common neighbors which vary gradually with respect to the movement of vehicles.

Popular vehicles are likely always in contact with many others. Consequently, these "well-known" vehicles are prone to be selected as carriers, so packets are routed to crowds where potential next carriers are available with high probability no matter the dynamic change in topology. Therefore, social metrics allow SocVe to adapt to the fast changed topology; as a result, success ratio is improved.

4.5 Conclusions

In this chapter, opportunistic forwarding protocols to overcome fragmentation in vehicular networks have been discussed. Studies of the social aspect of vehicular networks reveal an idea of exploiting social properties in vehicular communication, in forwarding protocol in particular. In order to improve the performance of safety applications in term of connectivity, we have introduced a social-aware opportunistic routing protocol for less urgent but important safety messages. Different from other related works, our proposed protocol is implemented in a safety scenario that the positions of the recipients are unknown. For example, our protocol can support the communication between normal vehicles to special vehicles such as police cars, safety mobile station or vehicles assisting search and rescue services, etc.. With consideration of the characteristics of vehicular environment, suitable social metrics are selected in our protocol. The safety messages are stored and forwarded by vehicles that have high centrality, thus they are carried to the crowds that they have more probability of encountering the destination or good carrier candidates. Our proposed protocol performs a significant packet delivery rate in the studied scenario where the short and intermittent connection and temporary disconnection are encountered.

Due to the highly dynamic topology of vehicular networks, connection duration and isolated duration of vehicles have various values and distributions. Some vehicle having higher centrality has longer connection duration and is likely in the connected state than the isolated state. On the other hand, the relation between store duration D_s and connectivity may exist. If D_s is too short, all stored packets are likely neglected before carriers have a chance of forwarding packets, then our protocol does not work. Otherwise, D_s is too long, the high centrality vehicles which have a lot of neighbors overwhelmingly forward packets. The network is probably flooded. Therefore, there should be a consideration of suitable value for D_s with regard to the connectivity condition of each vehicle in the network. An optimal store duration which may support the protocol to adapt to highly diverse network topology should be further investigated.

Chapter 5

Security of safety applications against jamming attacks in Vehicular Networks

The nature of wireless communication makes it exposed to attackers, thus, the wireless communication is prone to be eavesdropped, deliberated by man-in-middle hackers, and disturbed or overwhelmed resources by Denial of service (DoS) attacks. Besides, the environment is opportunistic for selfish participants to occupy more resources than others. As a type of wireless communication networks, vehicular networks are vulnerable to all of these attacks.

Almost safety applications are based on real-time information included in periodically exchanged packets of nearby vehicles, called beacons. Therefore, beacons play a vital role in maintaining the operation of safety applications and the whole ITS systems as well. However, they are prone to be victims of attacks at lower layers (physical and medium access control attacks) due to their limited packet length and short lifespan. Limited packet length does not allow complex cryptography, and it requires more time for complex computation if the attack comes from higher levels (e.g. manipulating content). The jamming attack is a common type of attacks at lower layers.

Due to the above reason, we focus on jamming attacks on beacons in vehicular networks in this chapter. Beacons can become new targets for jamming attacks in vehicular networks, hence it remains problems of modeling and detecting jamming attacks especially on these new targets. In order to analyze the impact of jamming attacks on network performance, we propose a novel jamming model which takes into account features of beacons and vehicular environments. The degradation of network performance caused by jamming attacks can be used as an indication to detect them in the networks. However, the method of using this indication has some shortcomings which make this method unsuitable for safety applications in vehicular networks. Therefore, we introduce a real-time jamming detection method. Since our method allows both central monitor and individual vehicles to detect the jamming in real time, it is feasible for safety applications.

The remainder of this chapter is organized as follows: the first section will discuss

different types of jamming attacks and related works on modeling and detecting jamming attacks; section 5.2 presents our proposed jamming attack model for broadcasting and its application for detecting reactive jamming attack; our real-time detection method will be analyzed in section 5.3 and studied via simulations in different scenarios in section 5.4; the chapter is concluded in section 5.5.

5.1 Jamming attacks in Vehicular Networks

5.1.1 Classification of jamming attacks in Vehicular networks

Jamming is one kind of DoS attacks. It broadcasts radio signal in the physical channel in order to block any beacon exchange within its transmission range. Jamming can be either constant jamming which continually emits radio signals not following any rule of communication protocol, or reactive jamming on which jammer transmits radio signal upon sensing a transmission in radio medium. Reactive jamming is more dangerous and harder to detect as it conforms to legitimate transmission.

Constant jammer and random jammer can be considered as protocol-unaware jammers since they broadcast the jamming radio signal regardless of legitimate activity in the medium.

A constant jammer continuously transmit random data to make the medium always busy. Whenever a legitimate node attempts to access the channel, it finds the channel busy then enters to backoff process. The busy state lasting for a long time leads packets to be dropped before being transmitted after several failed medium access attempts. This kind of jammer totally prevents all neighbors from communicating.

A random jammer operates according to random active and sleep periods. It starts active period and moves from active period to sleep period, and vice versa, randomly. In fact, we consider constant jammer as a special kind of random jammer which is in active mode for all the time.

A reactive jammer is activated only when it detects radio activity in the operating channel. Therefore, it conforms easily to legitimate transmissions. Whenever there is any radio activity, it decides to broadcast jamming signal with probability ρ_a, i.e., legitimate transmissions are partly attacked. Reactive jammer can be considered as a protocol-aware jamming attack as it senses medium and obeys medium access protocol. In this work, we deal with reactive jammer.

Different from other kinds of wireless networks such as sensor networks, mobile networks, etc., vehicular networks have strike characteristics that require adaptation in design whenever we apply technical solutions from general wireless networks to vehicular environment. Jamming attacks in wireless networks are generally well studied in literature [98][107][12] but not in vehicular networks.

5.1.2 Related works and open issues of jamming detection for beacons

In order to detect jamming in wireless networks, different detection methods have been proposed. Most of the related works [107][89][98] detect jamming based on observing network performance metrics such as packet delivery ratio, namely threshold-based detection method. The jamming is detected based on the difference between these metrics in normal scenario and these metrics in attacked scenario. Depending on how jamming impacts the network performance, a threshold value is chosen for a metric as a boundary to differentiate normal scenario and attacked scenario. Therefore, estimating this threshold precisely will enhance the probability of detection of the method. Besides threshold-based method, there is also real-time MAC-based method specified for vehicular networks [70][80].

The jamming attack causes degradation on packet delivery ratio (PDR) measured at a receiver. Based on how much the degradation is, the jamming can be detected. PDR is the ratio of error-free received packets and total received packets. PDRs encountered in normal scenario and jammed scenario are studied experimentally and/or analytically in jamming attack models. In wireless networks, several jamming attack models accompanying detection methods have been proposed [98][107]. Radio Frequency (RF) jamming attacks on VANETs were studied experimentally indoor and outdoor in [89]. Obtained outputs of these models or experimental results are reference values to differentiate a jamming attack and normal network condition. The detection methods that compare observed PDR to a certain reference value are referred as threshold-based detection methods. Obviously, in order to achieve high detection efficiency, the reference values used for jamming detection should be accurate. However, almost existing works investigate only the case of one transmitter without consideration of medium access contention. In vehicular environment, we cannot neglect medium access contention among vehicles because broadcast is the main communication mode supporting safety applications. Therefore, in our work, we propose an analytical model to estimate the threshold in consideration of the contention.

Different jamming attack models in wireless networks and different measurements serving jamming attack detection are studied in the work of Xu et al. [107]. According to their analysis, the measurements of signal strength and carrier sensing time, under certain circumstances, are not a powerful statistic to detect jamming as the difference between normal operation and under attacks is indistinct. While PDR is a powerful metric for detecting jamming attacks. However, it is unable to discriminate between jamming attack and other natural causes of PDR degradation. Therefore, they propose jamming detection with consistency checks that combine measurement of PDR and signal strength and/or PDR and location. An experimental study of RF jamming attacks on VANETs is conducted in [89]. PDR in normal operation and PDR under impacts of different types of jamming attacks are obtained from experiments. Sufyan et al. [98] propose analytical models of protocol-unaware jammers including constant

jammer and constant jammer, and protocol-aware jammers including reactive jammer and other intelligent jammers. Numerical results from their models are used for detecting and classifying different types of jammers. However, all mentioned above related works and their models focus on communication between two nodes and no medium access contentions. Their proposals are suitable for wireless networks but not feasible for broadcasting in vehicular networks.

Besides, in order to compare normal scenario and attacked scenario, thresholds for selected measurements must be identified. This difficulty is investigated in [88]. Although their machine learning-based jamming detection approach improves the accuracy of the threshold identification compared to the previous related works, medium access contention is still not mentioned in their studying case. In order to maximize detection probability, an accurate threshold should be defined in scenarios where medium access contention and physical parameters such as propagation loss and vehicle distribution are taken into account.

Apart from above threshold-based detection methods, there are MAC-based detection methods in vehicular networks that address medium access contention in their works [40][70]. Hamied et al. [40] propose a constant jamming detection method which is based on error distribution. The attack is figured out if the correlation coefficient among the error reception time and the correct reception time passes a threshold. However, again, the issue of threshold identification is not investigated. Authors in [70] proposed a jamming detection method that can detect a missing of one beacon from a vehicle in a platoon. Based on received beacons, a detector divides vehicles into groups whose beacons only collide to beacons sent from members of the same group. Whenever there is a missing of exactly one beacon in at least one group, an alarm will be raised. This method can detect only if there is exactly one beacon in a group is jammed. In fact, due to the nature of radio communication, the jammer interferes not only a vehicle but also several nearby vehicles. The method cannot distinguish between collisions of beacons in a group and a multiple jamming attack (more than one node in a group is jammed). An overhearing mechanism based on cross-layer approach is proposed in [90] to detect the malicious activity of nodes. Comparing the observed number of forwarded packets from neighbors and predicted number calculated from physical and MAC parameters, the monitor node can detect misbehavior nodes. However, the mechanism in [90] is not suitable for beacons. Beacons need only single-hop communication while the mechanism operates essentially based on the routing protocol.

5.1.3 Our contributions

The previous subsection 5.1.2 has presented two open issues on jamming detection as follows:

- How to adopt threshold-based jamming detection method for beacons in vehicular environment where the medium access contention and channel parameters should be taken into account?

- A novel MAC-based detection method specified for beacons may overcome the shortcomings of threshold-based jamming detection method in vehicular networks. It can provide a real-time detection which is suitable for safety applications.

Responding to the two above problems, in this thesis, our contributions on the security aspect of vehicular networks are in two folds. Firstly, we propose an analytical model which helps to estimate PDR threshold more precisely in threshold-based detection methods in vehicular environment. Secondly, we propose a real-time and MAC-based detection method to overcome existing shortcomings of threshold-based detection method such as the high probability of false alarms and requirement of time for statistics. Our method differentiates three phenomena: contention collision, interference, and jamming. This is the first time that the problem of differentiating the three phenomena is concerned in literature when we are looking for a feasible jamming detection solution.

We evaluate the impact of reactive jammer on PDR with consideration of medium access contention following the standard IEEE 802.11p, multi-channel operation IEEE 1609.4 and physical parameters. The study is specified for beacons, periodic safety messages in vehicular networks. The reference value (threshold) of the average PDR in normal operation is obtained. The value can be utilized in threshold-based detection methods. However, PDR must be measured during a specified window of time. The time window should be long enough for measuring a tolerant average PDR. Moreover, our analysis shows an overlap in standard deviation of PDR statistics in normal scenario and attacked scenario. Therefore, even the threshold to claim an attack is determined precisely, false alarms can not be avoided. The detection method based on observing PDR, when medium access contention and physical parameters are taken into account, may improve detection probability but also have a high probability of false alarm. Due to the requirement of observing time and high probability of false alarms, threshold-based detection methods are likely unsuitable for real-time applications in vehicular networks.

In order to overcome shortcoming of the threshold-based method, we propose a real time MAC-based detection method that helps to distinguish contention collision and jamming attacks, namely Contention collision - Jamming Differentiation (CJD) detection method. It can distinguish the missing of beacons due to whether jamming or collisions within groups, which is one of the limitation of proposed method [70]. Our method is studied analytically in our previous work [80]. In this paper, we enhance our method with a Collision - Interference Differentiation (CID) scheme. A failed transmission can be a result of interference, contention collision or jamming attack. Together,

our detection method CJD and CID scheme solve the problem of determining the reason of a failed transmission. Hence, jamming attacks can be detected precisely with low probability of false alarm. Moreover, it does not require any modification to the existing infrastructure and the method can be implemented for both central and distributed detection.

The multi-channel operation is a typical suggestion for vehicular networks. However, in our understanding, there are not many studies of jamming attacks addressing multi-channel operation in vehicular networks. Due to the unawareness of switching channel of higher level, nodes or vehicles likely contend for medium at the beginning of every control channel interval. This impact on communication using IEEE 802.11p is considered in performance evaluation of MAC protocol [20] and [77]. The performance evaluation is carried out analytically under an assumption that nodes start contending at the same time. However, we do not use this assumption in our simulations.

5.2 Modeling reactive jamming attack for broadcasting in vehicular networks

5.2.1 Jamming model at MAC layer

Related works have studied impacts of jamming in wireless networks by some metrics such as throughput [12], packet delivery ratio [46][89][107], etc..However, most of them study jamming in basic scenario of only one node transmitting without considering medium access contention. This studied case is popular in infrastructure-based wireless communication system such as wifi, mobile networks and sometime in sensor networks where unicast, communication between only two stations, is the main communication mode. In vehicular networks, besides Infrastructure to Vehicle (I2V) communication, there is vehicle to vehicle (V2V) communication that requires ad hoc mode and mostly works in broadcasting. In V2V, especially in order to support safety services, vehicles exchange frequently beacons including instant information of their owners. Hence, contention among beacons, when the standard IEEE 802.11p is used, obviously occurs frequently. Therefore, it is necessary to take into account medium access contention when we conduct a study of jamming attacks in vehicular ad hoc networks.

In this subsection, the impact of reactive jamming attacks is investigated with consideration of medium access contention. The study is conducted under below assumptions:

1. Each vehicle broadcasts one fixed-length beacon at each CCHI.
2. If a packet is not transmitted till the end of a CCHI, it will be dropped.
3. All vehicles contend for transmitting at the beginning of CCHI.
4. Any concurrent transmissions of legitimate vehicles or jammer lead to a failed transmission.

We assume that n vehicles having contention window of w slots start contending at the same time, at the beginning of CCHI. During the guard period of 4 ms between SCHI and CCHI, the medium is indicated busy. Each vehicle must choose one of w slots in contention window for transmitting. Thus each contention slot among w slots can be idle or a successful transmission or a failed transmission.

When there is no jammer, the number of successful transmissions respects to the number of slots that are chosen by only one vehicle for each, called l_{s_0}. Respectively, the number of failed transmissions is defined as the number of slots that are chosen by at least two vehicles, called l_{c_0} collided slots. These numbers depend on how many vehicles choose a given slot in contention window. The probability that a slot is chosen by x vehicles is computed as follows:

$$P(w,n,x) = \left(\begin{array}{c} n \\ x \end{array} \right) \left(\frac{1}{w}\right)^x \left(1 - \frac{1}{w}\right)^{n-x} \tag{5.1}$$

Reactive jammers are activated only when they detect ongoing transmissions in the channel. We assume that when the reactive jammer figures out an ongoing transmission, it will broadcast the jamming signal with a probability of ρ_a.

When the reactive jammer presents in the network, ongoing transmissions are jammed with probability ρ_a. If the ongoing transmission is a collision, then the attack is harmless. Otherwise, among l_{s_0} successful slots, l_a slots are attacked, number of successful and failed slots observed by the monitor or detector respectively are $l_s = l_{s_0} - l_a$ and $l_c = l_{c_0} + l_a$; l_s successful slots and l_c collision slots are what can be observed.

A contention slot can be an idle slot or a useful busy slot due to successful transmission or a useless busy slot for a failed transmission due to jamming or collision. All probabilities of events which may occur and respective observations are described in Table.5.1

TABLE 5.1: Probabilities denotes

Probabilities	**Events in a slot**	**Observations**
P_i	no legitimate transmision	idle slot
P_s	one legitimate transmission, not jammed	useful busy slot
P_{c1}	one legitimate transmission, jammed	useless busy slot
P_{c2}	collision	useless busy slot

Probability that there are exactly l_s successful slots, l_c collided slots among w slots in contention windows when there are n vehicles contending, is defined as $H(l_s, l_c, w, n, \rho_a)$.

It is computed recursively one by one slot.

$$\begin{aligned} H(l_s, l_c, w, n, \rho_a) &= P(w, n, 0).H(l_s, l_c, w-1, n, \rho_a) \\ &+ P(w, n, 1).(1-\rho_a).H(l_s-1, l_c, w-1, n-1, \rho_a) \\ &+ P(w, n, 1).\rho_a.H(l_s, l_c-1, w-1, n-1, \rho_a) \\ &+ \sum_{k=2}^{n} P(w, n, k) H(l_s, l_c-1, w-1, n-k, \rho_a) \end{aligned} \tag{5.2}$$

The first term refers to the event of an idle slot, P_i in the Table.5.1. The given slot is idle then there must be l_s successful slots and l_c collided slots occurring in the remain slots in the contention window. The second term refers to the probability of the event of a successful transmission in a slot, P_s. If there is only one vehicle transmits and the jammer does not broadcast, the given slot will be a useful busy slot, a successful transmission, then it remains $(l_s - 1)$ successful slots and l_c collided slots in next part of the contention window. Otherwise, the probability of the event of a failed transmission, P_{c1}, is referred. The given slot is supposed to be successful but it is jammed, so a collided transmission is observed. It remains l_s successful slots and $(l_c - 1)$ collided slots in next part of the contention window. The last term refers to all events of collisions in the given slot, P_{c2}.

Probability mass function of PDR when there is reactive jammer in the network is computed as follows:

$$pmf(PDR) = Pr(PDR = \frac{l_s}{l_s + l_c}) = H(l_s, l_c, w, n, \rho_a) \tag{5.3}$$

Based on probability mass function and possible values of l_s and l_c, standard deviation and mean PDR can be calculated.

5.2.2 Physical parameters

When MAC protocol is evaluated separately, a common assumption that more than one concurrent transmissions lead to a failed received packet is used. However, the assumption is not accurate anymore if physical parameters are taken into consideration. Network performance is impacted by physical factors such as the transmitter-receiver distance, the mobility of vehicles, transmission power, and so on.

In vehicular networks, network topology changes very dynamically; different transmitters are at different positions at a given time. Due to wireless propagation, the receive powers of signals carrying information from different transmitters are different at the receiver. The signal received at the receiver is a total of all parallel transmissions (signals) of transmitters. For the signal that has the highest receive power, other received signals are considered as interferences. Even more than two parallel signals received at the receiver, it is possible that there is one successful received signal which

carries a packet. In order to study the impact of reactive jamming attacks more precisely, we propose an analytical model capturing communication conditions that comprise physical parameters and medium access contention following the standard IEEE 802.11p.

We assume that at each receiver, each received packet from vehicle i has one individual but uniform receive power P_{r_i} over the complete time of the packet reception. The receive power is derived from the chosen radio propagation model which is elaborated later. At the receiver, it includes the sum of receive powers, P_{total}, of parallel legitimate signals at a given time, receive power of jamming signal P_{r_a} (if any), plus the power of interferences and noise.

$$P_{total} = \sum_{i \in TX(x)} P_{r_i} + \mathrm{P}_{r_a} + I + Noise \tag{5.4}$$

where $TX(x)$ is the set of x parallel transmitting vehicles at a slot. For a packet from vehicle i (the signal with the highest receive power), all other ongoing transmissions are considered as its interferences. Thus, the signal to interference and noise ratio (SINR) of a packet from vehicle i can be defined as follows:

$$SINR_i(x) = \frac{P_{r_i}}{\sum\limits_{\substack{j \in TX(x) \\ j \neq i}} P_{r_j} + I + Noise} \tag{5.5}$$

and when there is jamming attack:

$$SINR_i{}^{(a)}(x) = \frac{P_{r_i}}{\sum\limits_{\substack{\mathrm{j} \in TX(x) \\ \mathrm{j} \neq i}} P_{r_j} + P_{r_a} + I + Noise} \tag{5.6}$$

A low SINR leads to high probability of receiving error bits. It influences the probability of successfully receiving a packet. Depending on the applied modulation scheme and coding scheme, a threshold SINR, $SINR_{threshold}$, above which a frame is received successfully, is determined through empirical testing [53] or analytical results [94]. It means that:

$$P_{si}(x) = \begin{cases} 1 & if \quad SINR_i(x) \geq SINR_{threshold} \\ 0 & if \quad SINR_i(x) < SINR_{threshold} \end{cases} \tag{5.7}$$

where $P_{si}(x)$ is the success probability of a packet from vehicle i when there are x packets from other vehicles simultaneously received at the receiver. Jamming signal broadcast at the same time with packet i is considered as an interference. Similarly, success probability of packet i, denoted by $P_{si}^{(a)}(x)$, is computed with receive power of jamming signal counted in the formula. Integrating SINR consideration into the analytical model at MAC layer in previous subsection 5.2.1, probabilities are derived

from (5.2) for reactive jamming model with cross-layer view in (5.8).

Calculation of the probability that there are l_s successful received packets and l_c failed transmissions for reactive jamming is in (5.8).

$$\begin{aligned} H(l_s, l_c, w, n, \rho_a) &= P(w, n, 0).H(l_s, l_c, w-1, n, \rho_a) \\ &+ \sum_{k=1}^{n} P(w, n, k).\{P_s(k).H(l_s-1, l_c, w-1, n-1, \rho_a) \\ &+ P_f(k).H(l_s, l_c-1, w-1, n-k, \rho_a))\} \end{aligned} \tag{5.8}$$

where $P_s(x)$ and $P_f(x)$ are respectively probabilities that the given slot is successful or failed transmission depending on SINR of the packet with the highest receive power (among x parallel received packets). They are computed for both cases that the slot is attacked or not.

$$\begin{aligned} P_s(x) &= P_{si}(x).(1-\rho_a) + P_{si}^{(a)}(x).\rho_a \\ P_f(x) &= (1-P_{si}(x)).(1-\rho_a) + (1-P_{si}^{(a)}(x)).\rho_a \end{aligned} \tag{5.9}$$

SINR value of the highest receive power signal from a vehicle in a set of x transmitters and a jammer (if any attack) can be obtained statistically from simulations or analytically from analytical models. Because SINR of a received packet at the receiver depends on communication links between the transmitters and the receiver, radio propagation loss model and vehicle distribution determine the value of SINR of the received packet and then impact the network performance. In general, we can integrate any radio propagation loss model and vehicle distribution into the above MAC layer part of our analytical model. As our main purpose is to joint physical parameters and MAC protocol modeling in a model, in this work, we give a typical example which adopts law power propagation loss model [12] and Poisson distribution for vehicle distribution.

Radio Propagation Loss Model

Receive power of a signal at the receiver is defined as (5.10) in law power propagation model.

$$P_{ri} = {d_i}^{-\propto}.P_{ti} \tag{5.10}$$

where P_{ti} is the transmit power, the transmitter i is at the distance d_i from the receiver, $\propto$ is an attenuation parameter of the radio environment. Consequently, SINR of a received packet i at the receiver is obtained:

$$SINR_i^{(a)}(x) = \frac{{d_i}^{-\propto}.P_{ti}}{\sum\limits_{\substack{\in TX(x) \\ \neq i}} {d_j}^{-\propto}.P_{tj} + {d_a}^{-\propto}.P_{ta} + I + Noise} \tag{5.11}$$

where d_a and P_{ta} are respectively distance from the jammer to the receiver and transmit power of the jammer; x is the number of vehicles that transmit at the same time with vehicle i (including vehicle i).

Vehicle Distribution

Packets from vehicles transmitting simultaneously within a given range will always collide and fail to be received at the receiver. Therefore, vehicles in the network can be divided into groups whose parallel transmissions always lead to failed received packets at the receiver. Let N define sets of these groups of vehicles. Each group is comprised of k_i vehicles within the range of $(d_i - d_{(i-1)})$. There are m groups.

$$N = \{(k_i, d_i); \sum_{i=1}^{m} k_i = n, d_i \leq R \tag{5.12}$$

where n is the number of vehicles located in the transmission range of the receiver at a given sample CCHI. As CCHI is only 50 ms, the positions of vehicles is supposed to change insignificantly during one CCHI.

We assume that vehicles are distributed along a lane according to Poisson distribution with a density of λ (vehicles/m). Number of vehicles at distance d_i is $\lambda.d_i$. The closest vehicle to the receiver is at a distance of $d_0 = \frac{1}{\lambda}$. All vehicles at distances from $d_{(i-1)}$ to d_i belong to one group where $(d_{(i-1)} < d_i)$. If two vehicles that are furthest from each other in a group transmit concurrently, this results in a failed received packet. As we adopt law power propagation loss model, there is a positive correlation between the receive power and the distance from the sender to the receiver. SINR is calculated for the packet from the closer vehicle as the signal from the closer vehicle has higher receive power. This SINR of the closer vehicle of the two vehicles, $SINR_{(i-1)}(2)$, is always smaller than $SINR_{threshold}$. When there is a collision between transmissions from at least two vehicles, the power of noise and external interference is quite small compared to reception power of legitimate transmissions. Therefore, SINR of the packet from the closest vehicle of group $(i-1)$ at the receiver, denoted by $SINR_{(i-1)}(2)$, can be approximated in (5.13) if all transmitters have the same transmit powers.

$$SINR_{(i-1)}(2) \approx \frac{d_{(i-1)}^{-\propto}}{d_i^{-\propto}} \tag{5.13}$$

$$R^{-\propto} = \frac{SINR_{threshold} * Noise}{P_{tx}} \tag{5.14}$$

Derived from (5.13) and previous mentioned condition of SINR ($SINR_{(i-1)}(2) < SINR_{threshold}$), the value of d_i can be calculated from the relation with the maximum distance of vehicles in closer group $d_{(i-1)}$. Number of vehicles in a group at distance from $d_{(i-1)}$ to d_i is $k_i = \lambda.(d_i - d_{(i-1)})$. Number of groups depends on transmission

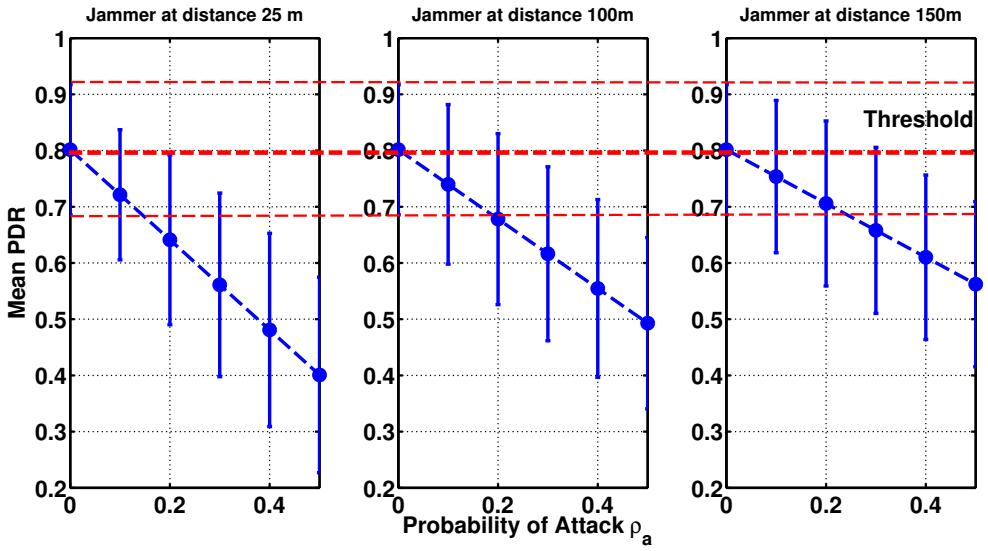


FIGURE 5.1: Mean PDR in normal scenario $\rho_a = 0$ and jammed scenario $\rho_a > 0$

range of vehicles as only transmitters within communication range of the given receiver are concerned. Transmission range of a vehicle, R, is defined as the maximum distance of the transmitter that a receiver can receive successfully a packet without contention collision, i.e. the distance where receive signal has $SINR = SINR_{threshold}$. R is computed in (5.14). When implementing the model in Matlab, the calculator selects a set of x vehicles from the prior conceived groups of vehicles for computation.

5.2.3 Threshold determination

The operation of jammers leads to a degradation of communication performance. We evaluate network performance in term of packet delivery ratio (PDR), which is the ratio of error-free received packets and total received packets. PDRs are measured during a specified window of time, so the threshold should be defined as the average PDR after numbers of CCHIs presenting in the time window. In our analytical model, we consider instant PDR (after each CCHI) as a random variable and we can determine the probability distribution of the instant PDR. From the probability distribution, the mean PDRs and their respective standard deviations under different network conditions are derived. The mean PDR and its standard deviations in the normal scenario are reference values to determine PDR threshold. Referring to the standard IEEE 802.11p [47] and related works in vehicular networks [41], constant parameters are chosen as shown in Table.5.2.

Fig.5.1 presents the mean PDRs and corresponding standard deviations of PDRs under different attack probabilities while vehicles are distributed in the network with the density of $\lambda = 0.05$. Respecting to the three computed results, the jammer is located at the distance of 20 m, 100 m and 150 m from the receiver. The higher attack probability is, the bigger decrease is observed in the average value of PDR. PDR in the normal

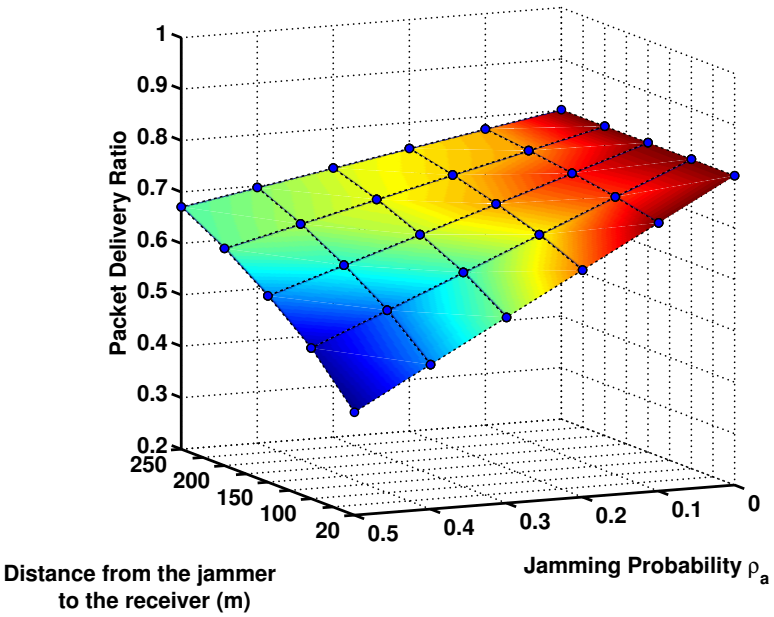


FIGURE 5.2: The influence of jamming probability, distance of jammer on PDR at the receiver

scenario is in the range 0.8 ± 0.11. While in other related works [89][107], PDR when $\rho_a = 0$, i.e. there is no attack, can reach 1. When medium access contention is taken into account, the PDR decreases to the range mentioned above. This range can be chosen as the PDR threshold range for jamming detection. Any observed PDR lower than this range is considered as jamming attacks. However, due to the significant standard deviation of PDR, there is an overlay range of PDR values that can be encountered in both normal scenario and jammed scenario with attack probability from 0.1 to 0.4. Therefore, a certain percentage of attacks is not detected.

The degradation of PDR under reactive jamming is shown as a function of jamming probability and distance of the jammer to the receiver in Fig.5.2. The jammer makes PDR (computed at the receiver) degrade more significantly when it is closer to the receiver. The impact of jamming attack on PDR is more recognizable when the jammer attacks with higher probability.

5.2.4 Is threshold-based detection method feasible for real-time applications?

In order to answer this question, we conduct simulations in NS-3 to validate the analytical model. Moreover, via simulations, we also investigate how big the time window should be. The PDR must be measured within a time window to obtain the average value. Since the time window should be long enough to obtain the average PDR close to the mean value (that we obtain from the analytical model or statistically from simulation with a large number of samples), the threshold-based detection methods may be not suitable for real-time services.

TABLE 5.2: Parameters in analytical model

Denotes	Descriptions	Values
P_t	Transmit power	23 dbm
$SINR_{threshold}$	SINR threshold for BPSK, data rate 3 Mbps	5 dbm
$\propto$	attenuation parameter	5
λ	density	0.05 vehicle/m
Noise	Power of thermal noise at 290 K in bandwidth of 10 MHz	$4.0029e^{-}14$ W

The simulation results are collected during 1000 s simulation time, i.e. 10000 samples of PDR after each CCHI are collected. The statistics of simulation samples are compared to analytical results in order to validate the analytical model. The statistics of simulation results nearly fit the analytical results, shown in Fig.5.3.

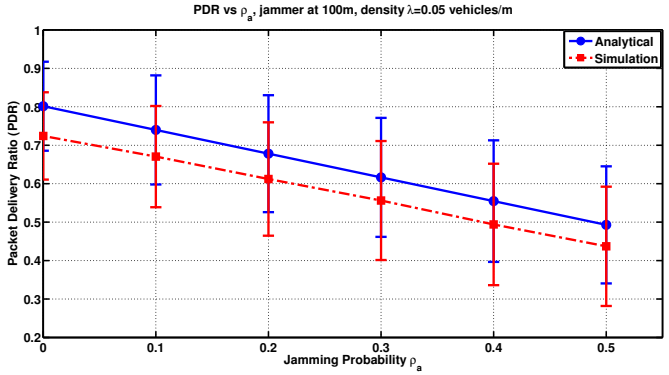


FIGURE 5.3: Analytical jamming model validation

For vehicles moving with the speed of 30 m/s (108 km/h) in the highway, they can go for a distance of 300 m in 10 s. As soon as the jamming is detected, vehicles can react to prevent connections from being disconnected within impacted range of the jammer. Thus, the duration for measuring average PDRs (time window size) in vehicular networks is very limited. Fig.5.4 shows simulation results which are conducted under the same parameters in analytical model. Different measured values of average PDRs within different time window of 10 s and 100 s are also shown. A time window of 10 s comprises 100 CCHIs and 1000 CCHIs for time window of 100 s as vehicles switch between SCH and CCH every 50 ms, i.e. there is 1 CCHI every 100 ms. An average PDR measured during a time window is called a sample. In normal scenario $\rho_a = 0$, the simulation results are shown in the middle figure, all measured average PDR in time windows of 100 s are all within the analytical threshold range. Almost samples of

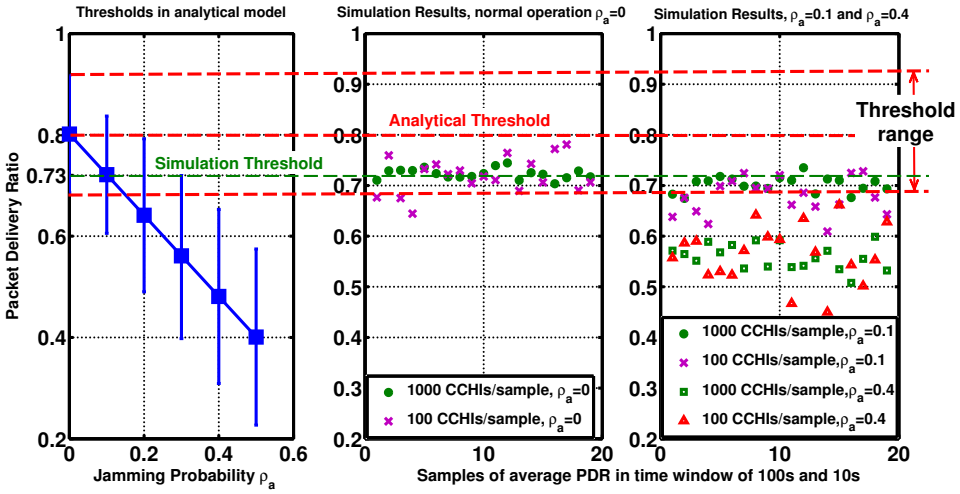


FIGURE 5.4: Analytical Threshold and Simulation Results

network under jamming probability of $\rho_a = 0.1$ fall into threshold range, i.e. it is very difficult to detect jamming attacking with too low attack probability.

On the other hand, we can define the computed mean PDR in the normal scenario as a threshold instead of a range to increase the probability of detection. The threshold can be chosen provided that almost PDR values which can be observed in jamming attacks are below the threshold. It can be approximate 0.72 (mean PDR obtained in simulation) or 0.8 (mean PDR obtained in analytical calculation) that is mean PDR in normal scenario, $\rho_a = 0$, shown in Fig.5.3. However, false alarms are prone to be raised when the time window is not big enough. There are several samples of average PDR in the normal scenario within time window 10 s below the threshold, in the middle figure in Fig.5.4, false alarms will be raised for these cases. The PDR must be measured during a big enough time window in order to obtain the result close to the expected mean value. If the time for collecting PDR values is too short, a low average PDR may be obtained even without attacks.

Different from the scenario of one transmitter, contention among vehicles in medium access leads to the fluctuation in observation of packet delivery ratio. The measurement of PDR has a deviation around the mean values, the bigger time window is, the closer to the mean value, the average PDR value is measured. We would like to remind that the mean PDR value is the statistic value obtained from analytical analysis while the average value is measured within each time window. The threshold is fixed according to many parameters such as density, radio channel characteristics, the number of vehicles. Therefore, we will have to accept a false alarm probability which is especially high if the time window is not big enough. Based on all above observations, we can argue that threshold-based method is not feasible for vehicular networks. It requires real time and more reliable detection methods.

Due to above reason, in the next section, we propose a MAC-based detection method

CJD, no threshold is needed while false alarm probability is kept small. Also, different from related works, this is the first time that we consider together three phenomena: contention-collisions, interferences, and jamming attacks. An enhancement in our detection method, collisions-interferences differentiation scheme CID, helps to reduce false alarm probability. Combining the CJD method and CID scheme, it is possible to distinguish the three phenomena.

5.3 Real-time Jamming Detection Method for beacons in Vehicular Networks

In this chapter, we present a detection algorithm that can be used either centrally in Central Contention-Jamming Differentiation detection method (C-CJD) or distributively in Distributed Contention collision-Jamming Differentiation detection method (D-CJD). In section 5.3.1, we work on the scenario with the presence of a central node (detector or monitor), which observes the channel where vehicles exchange beacons periodically. The detector using C-CJD can be installed along roads or on some preselected vehicles. Besides, the algorithm is probably executed also by individual vehicles using D-CJD. This will be elaborated in section 5.3.1 of D-CJD.

5.3.1 Contention Collision-Jamming Differentiation detection method (CJD)

Jamming detection algorithms

Beacons may be generated out of control channel interval by applications. It leads to synchronous contending beacons at the beginning of CCHI. This phenomenon can be considered as a contention period that vehicles choose their backoff randomly in contention window and transmit their beacons at their chosen backoffs.

We assume that n vehicles having contention window of w slots start contending at the same time, the beginning of CCHI. A malicious node, a reactive jammer in this context, senses the medium and broadcast blindly with probability ρ_a whenever there is any radio activity. Consequently, jamming may occur in successful transmissions or collision transmissions. It impacts only successful transmissions because if the malicious node broadcasts during a collision, it will be harmless.

The detector operates in three phases as shown in Fig.5.5: initialization phase, observation phase and detection phase.

The estimation module initially runs for a duration of time in initialization phase in order to determine all its neighbors. After initialization phase, the detector moves to observation phase in which it senses the medium and records number of successful transmissions and failed transmissions within one contention window. At the same time, estimation module remains working to update the number of neighbors. The obtained parameters of observation phase are inputs for calculation in detection phase.

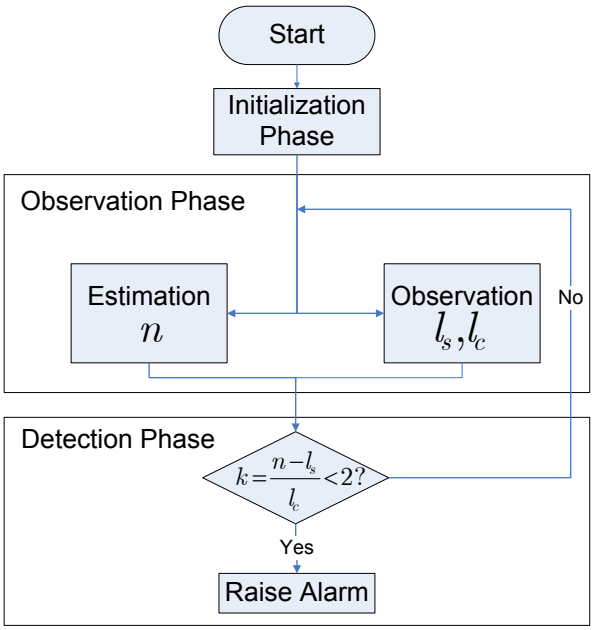


FIGURE 5.5: Detector Operation

- **Initialization Phase**

During the initialization phase, the detector overhears the medium within an area of one transmission range and records its neighbor ids (addresses of neighbors) and creates its neighbor list based on received beacons. Whenever the detector receives a beacon from a new coming neighbor, it adds the new neighbor to the list. If during 1 s, it no longer gets beacon from a given neighbor, it will determine that this neighbor leaves the transmission range. This procedure can be considered as an initial estimation of which the estimation module is in charge. Estimation module works also concurrently with observation module in observation phase in order to keep the number of neighbors up to date. The details of the two modules will be elaborated in next subsection which describes observation phase.

- **Observation Phase**

After the initialization phase, the two modules: estimation module and observation module synchronously work. The number of neighbors may change slightly during the observation. How the detector updates its neighbor list is described previously. The algorithm is depicted in Algorithm 1. It is triggered when the detector receives a beacon. Each vehicle is identified in the neighbor list of the detector by its MAC address. The vehicle id will be deleted from the neighbor list if the detector does not receive its beacon for a long time.

Concurrently with estimating number of neighbors, within each CCHI, the detector observes and records number of successful and failed transmissions. Each vehicle must choose one of w slots in contention window for transmitting. Thus, each slot among

Algorithm 1 Estimation Algorithm

```
1: if receive beacon of node i then
2:    if node i is already in the neighbor list then
3:       update latest time receiving beacon of node i;
4:    else
5:       add node i to neighbor list;
6:    end if
7: end if
```

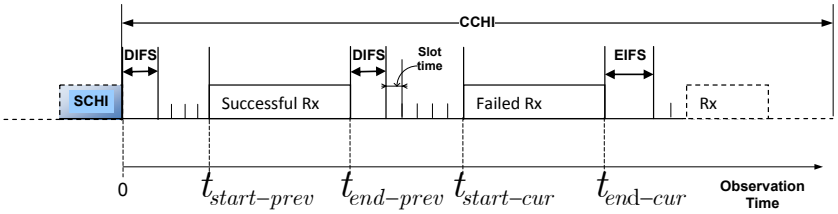


FIGURE 5.6: Observation Process

w slots can be idle or a successful transmission or a failed transmission. Number of successful transmissions, l_s, is the number of slots that are chosen by only one vehicle per slot. Respectively, number of collided transmissions, l_c, is the number of slots that are chosen by at least two vehicles per slot. Let define number of waiting beacons to be transmitted at l^{th} slot from the beginning of CCHI as $r(l)$.

$$r(l) = n - l_s(l) - k(l).l_c(l) \tag{5.15}$$

where $k(l)$ is the average number of collided beacons in a slot till l^{th} slot; $2 \leq k(l) \leq n - l_s(l)$; $l_s(l)$, $l_c(l)$ are respectively the number of successful and the number of failed transmissions till l^{th} slot.

At the end of contention window or the end of observation phase, number of successful slots $l_s = l_s(w)$, number of collided slots $l_c = l_c(w)$. Radio activity reports help detector monitor contention progress and determine when the contention period finishes. Fig.5.6 illustrates how the detector observes neighbors' access contention by sensing the medium. After each busy period in medium or receiving duration, the number of successful slots and the number of failed slots are updated. This process continues till the end of the contention window.

The observation of parameters mentioned above is carried on by observation module which executes Algorithm 2. From line 1 to line 5 are the initial values of parameters. When each transmission starts in the medium, the detector marks the start time of current transmission at line 8 and the end of the transmission at line 12 when the transmission ends. Later, at line 13, the ordinal number of current slot, c, is updated by calculating the number of slots passing from the last transmission till current time. Depending on whether the previous transmission is successful or failed, the value of

parameter IFS is $DIFS$ or $EIFS$ as specified in the standard IEEE 802.11. The process repeats until the current slot is the last one in contention window, i.e. $c = 0$. At the end of contention period, all elements for detection computation are available, the detection phase starts.

Algorithm 2 Observation Algorithm

$t_{end-prev} = 0$;
$IFS = DIFS$;
c = contention window size;
$l_s = 0$;
$l_c = 0$;
while $c > 0$ **do**
  if radio activity occurs **then**
    $t_{start-cur} = currenttime$;
    while medium is busy **do**
      sense medium;
    end while
    $t_{end-cur} = currenttime$;
    $c = c - \frac{(t_{start-cur} - t_{end-prev} - IFS)}{slot\_time} - 1$;
    if receive a successful packet **then**
      $IFS = DIFS$;
      $l_s = l_s + 1$;
    else
      $IFS = EIFS$;
      $l_c = l_c + 1$;
    end if
    $t_{end-prev} = t_{end-cur}$;
  else
    $c = c - \frac{(currenttime - t_{end-prev} - IFS)}{slot\_time}$;
  end if
end while

- **Detection Phase**

After w slots, as soon as all vehicles finish their contentions, the detector can start its computation. At that time, the number of waiting beacons must be 0, i.e. $r(w) = 0$ thus if there is at least one collision noticed, i.e. $l_c > 0$, the average number of collided beacons in a slot $k(w)$ must be determined as below:

$$k(w) = \frac{n - l_s}{l_c} \tag{5.16}$$

As a collision must be involved by at least two participants, the average number of collided beacons in a slot must equal or bigger than 2. Consequently, if there is no attack $k(w)$ must always be equal or bigger than 2. The attack causes value of elements

in (5.16) to vary so that value of $k(w)$ is changed. Based on the number of successful and failed transmission, the detector can calculate and raises an alarm if $k(w) < 2$.

If all observed transmission are successful and the number of successful transmissions is not equal to the number of vehicles, the detector will raise alarm also. This is a special case that we do not need to calculate and easily detect the missing.

Proposed detection method analysis

- **Detection Probability**

Let define l_{s_0} and l_{c_0} respectively as number of successful and collided slots without attacks. From now, we use k instead of $k(w)$. It can be understood that this parameter is calculated only after a w-slot contention window. Based on (5.16) and condition $k \geq 2$, the average number of collided beacons in a slot when there is no attack can be obtained:

$$k_0 = \frac{n - l_{s_0}}{l_{c_0}} \geq 2 \tag{5.17}$$

If there is no attack, there should be l_{s_0} successful slots and l_{c_0} failed slots observed. However, if there is jamming, some slots will be jammed. Therefore, less than l_{s_0} successful slots and more than l_{c_0} failed slots are observed. If among l_{s_0} slots, l_a slots are attacked, number of successful and failed slots observed respectively are $l_s = l_{s_0} - l_a$ and $l_c = l_{c_0} + l_a$; l_s successful slots and l_c collision slots are what the detector can observe. The average number of collided beacons in a slot after a contention period when there are attacks is calculated as below:

$$k_a = \frac{n - (l_{s_0} - l_a)}{l_{c_0} + l_a} \tag{5.18}$$

The attack can be detected if $k_a < 2$. Derived from (5.18), it is possible to detect attacks if the below cases occur:

$$l_{c_0} > \frac{n - l_a - l_{s_0}}{2} \tag{5.19}$$

Detection probability with attack probability ρ_a, n contending vehicles with w-slot contention window, $P_{det}(\rho_a, n, w)$ can be calculated as probability that number of supposed successful slots l_{s0}, number of supposed collision slots l_{c0} and number of attacked slots l_a among l_{s0} meet the condition (5.19) divided by probability that the given contention period is attacked, i.e. $l_a > 0$.

$$P_{det}(\rho_a, w, n) = \frac{P(l_{s_0} + 2l_{c_0} > n - l_a)}{P(l_a > 0)} \tag{5.20}$$

Probability that there are exactly l_a slots among l_{s0} successful slots are attacked, l_{c_0} collided slots among w slots in contention windows when there are n vehicles contending is defined as $Q(l_a, l_{s_0}, l_{c_0}, w, n, \rho_a)$. It is computed recursively one by one slot till the

end of contention window as in (5.21).

$$\begin{aligned} Q^* &= Q(l_a, l_{s_0}, l_{c_0}, w, n, \rho_a) \\ &= P(w,n,0).Q(l_a, l_{s_0}, l_{c_0}, w-1, n, \rho_a) \\ &+ P(w,n,1).\rho_a.Q(l_a-1, l_{s_0}-1, l_{c_0}, w-1, n-1, \rho_a) \\ &+ P(w,n,1).(1-\rho_a).Q(l_a, l_{s_0}-1, l_{c_0}, w-1, n-1, \rho_a) \\ &+ \sum_{k=2}^{n} P(w,n,k) Q(l_a, l_{s_0}, l_{c_0}-1, w-1, n-k, \rho_a) \end{aligned} \tag{5.21}$$

where ρ_a is the attack probability; $P(w,n,x)$ is the probability that a slot is chosen by x vehicles as defined before in (5.1). The first term refers to the event that the given slot is idle, thereafter there must be l_{s_0} successful slots including l_a attacked slots and l_{c_0} collided slots occurring in the remain slots in contention window. If the given slot is a successful transmission, then it remains $l_{s_0} - 1$ successful slots and l_{c_0} collided slots in next part of the contention window. The second term and third term describe whether this successful slot is attacked or not. The last term refers to all collision cases that may happen in the given slot.

The numerator in calculation of detection probability in (5.20) is a sum of all possibilities that l_a, l_{s0} and l_{c0} meet the condition (5.19). While the denominator is a sum of all probabilities at least one successful slot is attacked. Consequently, detection probability can be computed as follows:

$$P_{det}(\rho_a, w, n) = \frac{\sum_{l_a=1}^{\min(n,w)} \sum_{l_{s_0}=l_a}^{\min(n,w)} \sum_{l_{c_0}=\max(s_0,0)}^{(n-l_{s_0})/2} Q^*}{\sum_{l_a=1}^{\min(n,w)} \sum_{l_{s_0}=l_a}^{\min(n,w)} \sum_{l_{c_0}=0}^{(n_0-l_{s_0})/2} Q^*} \tag{5.22}$$

where $s_0 = \frac{n-l_a-l_{s_0}}{2}$. With attack probability ρ_a, not any or up to all successful slots are attacked thus l_a ranges from 0 to minimum of n and w. Number of successful slots l_{s_0} is always bigger than l_a and smaller or equal to n or w. To meet the condition (5.19), l_{c_0} must be bigger than $s_0 = \frac{n-l_a-l_{s_0}}{2}$ and smaller or equal to $\frac{n-l_{s_0}}{2}$ as the proved requirement in (5.17).

- **Precision of proposed method**

Proposed method may perform imprecisely if the detector wrongly estimates the number of neighbors or confuses between an error transmission due to bad link connection and a jamming attack. The first factor, wrong estimation of the number of neighbors, causes false alarms that trigger corresponding reactions of system even network is operating normally, or missing alarms due to eventual computation. The second factor, the confusion of the cause of a failed transmission, will be discussed later in section

5.3.2. In this section, we investigate the improper operation of our method caused by the wrong estimation.

We assume that the detector wrongly estimates Δn vehicles in difference to n_0 vehicles in reality, i.e. estimated number of neighbors which is used in calculation is $(n_0 + \Delta n)$. Respectively, observed average number of collided nodes in a collision (5.16) is $k_f = \frac{n_0+\Delta n-l_s}{l_c}$. The alarm would be raised if $k_f < 2$. The wrong estimation can lead to missing alarm if $k_f \geq 2$ or false alarm if $k_f < 2$ when there is no attack.

- ***Probability of Detection when there is wrong estimation***

A change in the probability of detection is a result of a change in the value of k when the detector wrongly estimates the number of neighbors. Parameter k, which should be smaller than 2 in attacks, becomes k_f that is bigger than 2 due to the wrong estimation then we miss an alarm. The observation of l_s and l_c does not change. If $k \geq 2$ even there is attack, we suppose to be failed to detect, however, the wrong estimation accidentally makes $k_f < 2$ and the attack is detected. Detection probabilities (5.22) when there is a wrong estimation can be calculated:

$$F_{\text{det}}(\rho_a, w, n, \Delta n) = \frac{\sum_{l_a=1}^{\min(n_0,w-1)} \sum_{l_{s_0}=l_a}^{\min(n_0,w-1)} \sum_{l_{c_0}=\max(s,0)}^{(n_0-l_{s_0})/2} Q^*}{\sum_{la=1}^{\min(n_0,w)} \sum_{l_{s_0}=1}^{\min(n_0,w-1)} \sum_{l_{c_0}=0}^{(n_0-l_{s_0})/2} Q^*} \tag{5.23}$$

where $s = \frac{n_0+\Delta n-l_a-l_{s_0}}{2}$.

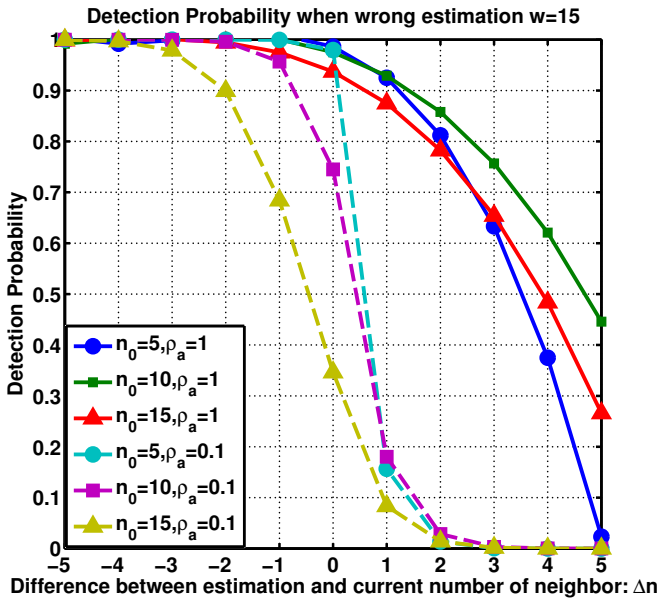


FIGURE 5.7: Impact of wrong estimation on detection probability

Numeric results of the analysis are shown in Fig.5.7. The wrong estimation results in a change in detection probability. The underestimation of the number of neighbors

slightly improves the performance of the method. On the other hand, the overestimation causes a deduction in detection capability of the method. In the scenario of the higher number of neighbors, collisions occur more frequently. Therefore, if the estimated number of neighbors is higher than reality, the detector confuses between attacked slots and collisions more easily.

- ***False alarm probability***

An alarm is considered as a false alarm if it is raised even there is no attack, i.e. $l_a = 0$. The alarm will not be raised and the wrong estimation is detected if the observed values of l_s, l_c are not reasonable, i.e. the set of these values obviously cannot occur with estimated number of participants. Otherwise, probability of raising false alarm is computed from all cases that the values of l_{s_0}, l_{c_0}, n_0 and Δn result in a computation of k_f smaller than 2 while $l_a = 0$.

Probability of false alarm if the detector wrongly estimates Δn neighbors and the jammer attacks with probability ρ_a, $P_{false}(\rho_a, w, n_0, \Delta n)$ can be defined as:

$$P_{false}(\rho_a, w, n_0, \Delta n) = \begin{cases} 0 & if \Delta n \geq 0 \\ \sum_{l_a=0} \sum_{l_{s_0}=0}^{\min(n_0, w-1)} \sum_{l_{c_0}=\frac{n_0+\Delta n-l_{s_0}}{2}}^{(n_0-l_{s_0})/2} Q^* & if \Delta n < 0 \end{cases} \tag{5.24}$$

The first term describes a fact that when there is no attack, the overestimation of the number of neighbors always makes $k_f \geq 2$ (Appendix B) thus no alarm is raised. This phenomenon may lead to missing alarm issue that is analyzed previously. Alarms which are raised during the no attack periods are counted as false alarms. They are addressed in the second term.

The numeric results in Fig.5.8 show that the probability of false alarms is significant for the wrong estimation in the range of 3 vehicles smaller than the real current number of neighbors when n_0 is from 5 to 15. Especially, the overestimation does not create false alarms as it makes the computation always result in non attack decision. For underestimation on which the estimated value of the number of neighbors is lower than in reality, false alarms are raised with the highest probability of nearly 0.4 with the number of 15 neighbors and attack probability of 0.1. While the probability of false alarms are 0.3 and 0.04 when the estimated number of neighbors is closest to the real values of 10 vehicles and 5 vehicles.

Distributed Detection Method (D-CJD)

As mentioned at the beginning of section 5.3.1, the algorithms can be executed by individual vehicles. As local observation at a vehicle is different from observation at the

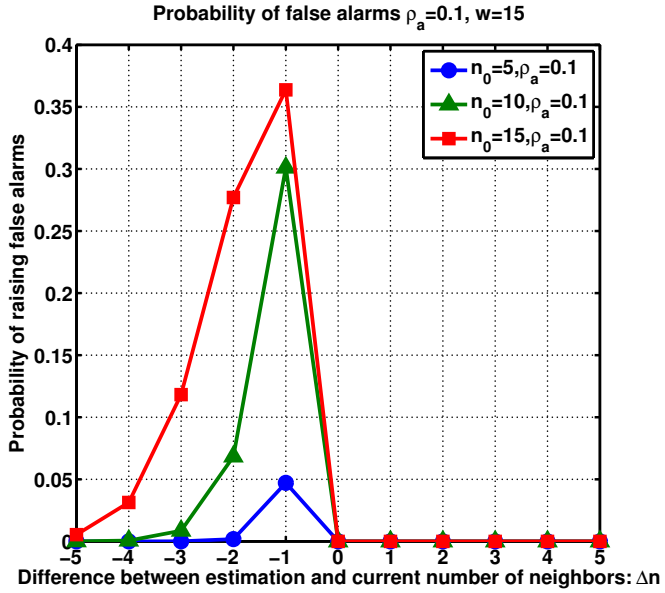


FIGURE 5.8: Probability of false alarms due to wrong estimation

central detector, detection probability of D-CJD at individual vehicle will vary from C-CJD analyzed above.

Compared to a central detector, an individual vehicle locally can observe all successful transmissions and failed transmissions except its own transmissions. The number of its transmitting neighbors will be $n_i = (n-1)$ while n is the number of transmitting vehicles in the transmission range of the central detector. Let l_{s_i} and l_{c_i} define the number of successful transmissions and failed transmissions that the given vehicle observes respectively. While $l_{c_i} > 0$, applying the algorithms described in section 5.3.1 and deriving from (5.16), the average number of collision participants is computed locally at a given vehicle i as below:

$$k_{a_i} = \frac{n_i - l_{s_i}}{l_{c_i}} \tag{5.25}$$

If the vehicle's transmission is successful (whether be jammed or not), the number of successful transmission and failed transmission observed by itself respectively are $l_{s_i} = (l_s - 1)$ and $l_{c_i} = l_c$. Otherwise, if its transmission is a collided transmission, the two parameters are $l_{s_i} = l_s$ and $l_{c_i} = (l_c - 1)$, where l_s and l_c are observed parameters at the central detector. Respectively to the two above cases, parameter k_{a_i} can be obtained as:

$$k_{a_i} = \begin{cases} \dfrac{n - l_s}{l_c} & if(*) \\ \dfrac{n - l_s - 1}{l_c - 1} & if(**) \end{cases} \tag{5.26}$$

$(*)$: its own transmission is successful; $(**)$: its own transmission encounters collision.

In the first case, when the transmission of the given node is successful, the same value of k is obtained at the given vehicle and at the central detector. Therefore, in

this case, the given node has the probability of detection $P_{s-i-det}(\rho_a, w, n)$ equal to detection probability of the central detector under the same condition.

$$P_{s-i-det}(\rho_a, w, n) = P_{det}(\rho_a, w, n) \tag{5.27}$$

Otherwise, in the second case, if the transmission of the given vehicle is a collision, as in (5.18) $l_s = l_{s_0} - l_a$, $l_c = l_{c_0} + l_a$, the obtained k_{a_i} in the second term of (5.26) is below:

$$k_{a_i}(**) = \frac{n - l_{s_0} + l_a - 1}{l_{c_0} + l_a - 1} \tag{5.28}$$

When exactly one slot is jammed, i.e. $l_a = 1$, $k_{a_i} = \frac{n-l_{s_0}}{l_{c_0}} = k_0$. According to (5.17), k_{a_i} is always bigger or equal to 2 when $l_a = 1$. When $l_a > 1$, the attack can be detected by the given individual vehicle if $k_{a_i}(**) < 2$, i.e. $l_{c_0} > \frac{n+1-l_{s_0}-l_a}{2}$. Hence, when an individual vehicle encounters collision in its chosen slot, its respective detection probability $P_{c-i-det}(\rho_a, w, n)$ can be computed similarly to $P_{det}(\rho_a, w, n)$ in (5.22) with s_0 replaced by $s_i = \frac{n+1-l_{s_0}-l_a}{2}$.

For special cases that $l_{c_i} = 0$, the given individual vehicle observes no failed transmission, its transmission can be successful or collision. The alarm should be raised in case that its transmission is successful but jammed. However, the vehicle cannot observe its own transmission, it hence misses an alarm if its own transmission is a successful and jammed transmission. The probability of missing an alarm is the probability that all vehicles except the given vehicle transmit successfully without being jammed. The given vehicle transmits successfully at a slot but this slot is attacked. The probability that the vehicle always misses to detect the attack can be calculated as below:

$$P_{i-miss}(\rho_a, w, n) = Q(1, n, 0, w, n, \rho_a) \tag{5.29}$$

The successful probability of the given vehicle's transmission, $P_s(w, n)$, can be obtained analytically from the related work in [20] and our previous work [77]. In these related works, an analytical for the standard IEEE 802.11p was proposed under the same assumption that all the vehicles start contending at the same time at the beginning of CCHI.

$$P_s(w, n) = \frac{X(T, w, n)}{n} \tag{5.30}$$

where X is the number of successful beacons, T is the number of slots within CCHI, w is the contention window, n is the number of packets or vehicles (as each vehicle has one packet to send). While w and n are not significant compared to T, all contentions finish before the end of CCHI. According to the standard IEEE 802.11p, the lowest priority access category has longest contention window of 15 slots while there are more than 3000 slots within CCHI with the slot time of $13\mu s$. Thus in this analytical model,

we assume that all contentions finish before the end of CCHI, and do not count the parameter T in our calculation.

All probabilities that can happen to the detection at an individual vehicle are analyzed above. Consequently, detection probability of D-CJD can be obtained:

$$\begin{aligned} P_{i-det}(\rho_a, w, n) = (1 - P_{i-miss}) \\ .(P_s(w, n).P_{s-i-det}(\rho_a, w, n) \\ + (1 - P_s(w, n)).P_{c-i-det}(\rho_a, w, n)). \end{aligned} \tag{5.31}$$

The detection probability of D-CJD is computed for all cases that can be observed by an individual node.

Performance Evaluation of the proposed detection method (CJD)

We validate the analytical model to evaluate our detection method by results obtained from network simulation in NS-3. Numerical results and simulation results are concurrently shown in Fig.5.9 and Fig.5.10.

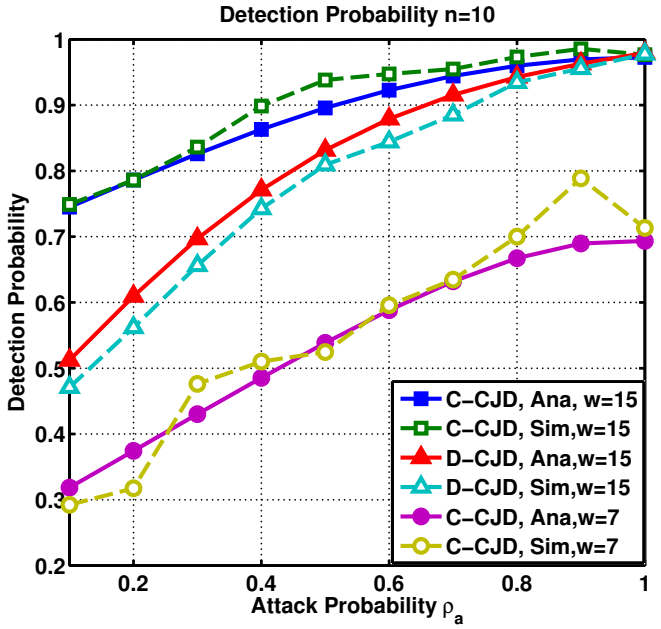


FIGURE 5.9: The influence of detection probability on attack probability

Detection probability is used as a metric to evaluate our proposed jamming detection method. The influences on attack probability, contention window size, and number of vehicles of our method are considered. Fig.5.9 depicts detection probability of Central Detection Method (C-CJD) and Distributed Detection Method (D-CJD) as a function of attack probability with different contention window sizes when $n = 10$. The proposed method performs better in high attack probability. When attack probability reaches 1, i.e. the malicious node jams all radio activity in the medium, our method can

detect 70% attack cases for beacons AC2 (contention window size of 7 slots) and 99% attack cases for beacons AC3 and AC4 (contention window size of 15 slots).

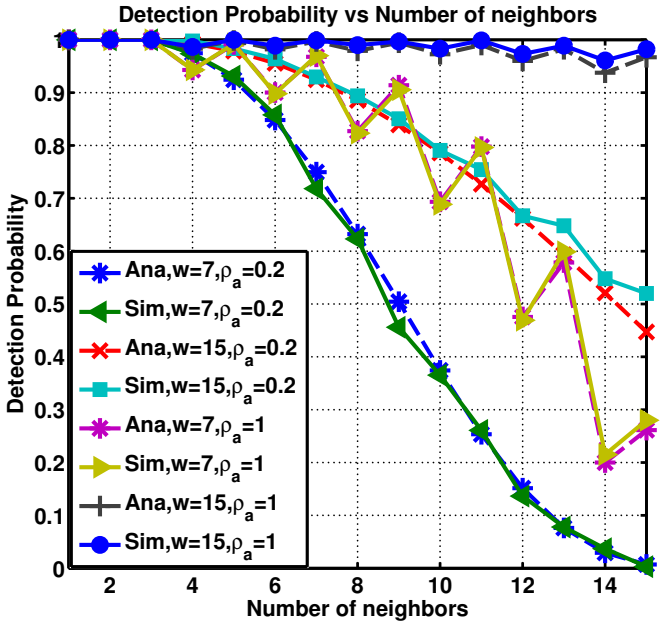


FIGURE 5.10: The influence of detection probability on number of vehicles

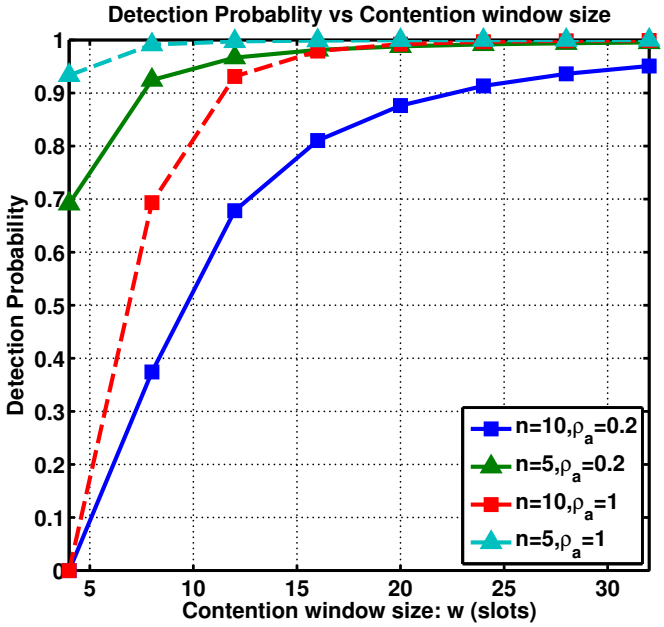


FIGURE 5.11: The influence of detection probability on contention window size

The impact of number of vehicles and contention window size on detection probability of C-CJD is shown in Fig.5.10 and Fig.5.11 with $\rho_a = 0.2$ and $\rho_a = 1$. The more vehicles participate in contention, the more difficultly we can detect the attacks. Detection probability is higher with longer contention window. The medium access

contention becomes more aggressive when there are more vehicles with shorter contention window; consequently, more vehicles take part in each collision. Even some attacked slots lead to a reduction of k, the average number of participants in a collision is still bigger than 2. The detector probably confuses attacks with collisions.

The dependence on contention window size of the method's performance is shown in Fig.5.11. The bigger contention window the better the detection method performs.

As the method works based on calculating average collision participants k, the bigger variation that attacks make to this parameter, the more easily the detector recognizes attacks. This variation depends on how frequent the jammer disturbs the communication and number of participants on each collision. Therefore, detection probability is higher with higher attack probability and fewer collisions occurring, i.e the number of contending vehicles is less and the contention window size is bigger.

5.3.2 Contention-Jamming-Interference Differentiation detection method (CJID)

A low SINR leads to a failed received packet. Poor link connection, contention collision, and jamming may result in low SINR because they play a role of interferences to the main signal. In our proposed CJD detection method above, based on observation of the number of successful transmissions and number of failed transmissions, we can distinguish between contention collision and jamming. However, the method works under the assumption of no interference. If there is interference in the network, failed transmissions can be due to any reason among contention collision, jamming or interference. This makes our method imprecise because we consider a failed transmission as a result of contention collision or jamming. It means that there are at least two transmitters involving in the transmission. While one single vehicle broadcasts in poor link connection due to interference may lead to failed transmission also.

In order to improve our detection method in the environment of low power interference, we propose collision-interference differentiation scheme. The scheme allows us to clarify if the reason of a failed transmission is poor quality connection or collisions. After that, our previous CJD detection method can be applied. The reason leading to the poor quality connection can be interferences from neighborhood or propagation loss, fading in the radio channel.

At the receiver, all received signals are impacted by the same interferences. Therefore, only the signal that has low receive power fails to be received because of low SINR. While a failed transmission due to collisions is a sum of at least two parallel transmissions of legitimate vehicles and/or jammer. For low power interferences, the total receive power of a failed transmission due to collisions at the receiver should be higher than a failed transmission due to interferences. In this work, we define low power interferences as spurious signals that have receive power smaller than the sensitivity of the receiver but higher enough to make a low receive power signal fail to be

Algorithm 3 Collisions-Interferences Differentiation Algorithm

1: $P_{threshold} = P_{sensitivity}$;
2: **while** at CCHI j^{th} **do**
3: **if** receive successfully a packet **then**
4: Update Neighbor list P_{rn};
5: **else**
6: **if** $P_{rx} < P_{threshold}$ **then**
7: Failed transmission due to interference $l_i = l_i + 1$;
8: **else**
9: Failed transmission due to collision $l_c = l_c + 1$;
10: **end if**
11: **end if**
12: **end while**
13: $P_{threshold} = min(P_{rn}) + secondmin(P_{rn})$;
14: back to line 2 at the beginning of next CCHI $(j+1)^{th}$;

received. These interferences may come from transmissions of vehicles out of reception range of the receiver, the signal strength is not enough for the receiver to recognize a transmission but big enough to interfere a low receive power legitimate packet from receiver's reception range. Our scheme is described as follows.

The scheme is described in Algorithm.3. The detector maintains a neighbor list which includes neighbors' identities and their recent receive powers. The neighbor list is updated frequently every CCHI, line 4. The threshold for determining interferences and collisions $P_{threshold}$ used at a given CCHI is calculated at the end of previous CCHI. It is computed as the sum of two smallest receive powers in the neighbor list of the receiver, line 13. P_{rn} defines set of receive powers of all neighbors.

5.4 Simulation Results

We implement the proposed detection method in NS-3 and evaluate our methods via simulations in different scenarios. In all simulations, Nakagami-m fast fading model and Log distance propagation loss model are used for simulating fading and path loss in the radio channel. The mobility of vehicles is generated according to studied scenarios. Other parameters, which are suitable for vehicular networks [47][41], are listed in Table.5.3.

Platooning is a potential application in Intelligent Transportation System. It allows vehicles to move simultaneously in a platoon, one follows another [96]. Traveling in platoons increases capacity of roads. An automated highway system is a proposed technology for applying platooning. In the first part of this section, we investigate our detection method in the scenario of a platoon. We compare the results to the work of Lyamin et al. in [70] under the same scenario and their assumptions. These assumptions are that all vehicles are always at the transmission range of each other and the time between the generation of two subsequent beacons from a vehicle is fixed and the

TABLE 5.3: Parameters in Simulations

Parameters	Values
Transmit power	23 dbm
Data rate	3 Mbps
Beacon Length	500 bytes
Contention window (AC2)	7 slots
Number of vehicles Platoon scenario General scenario	 10 vehicles 10-30 vehicles
Vehicle speed	30 m/s
Sensitivity Vehicles Jammers	 -85 dbm -90 dbm

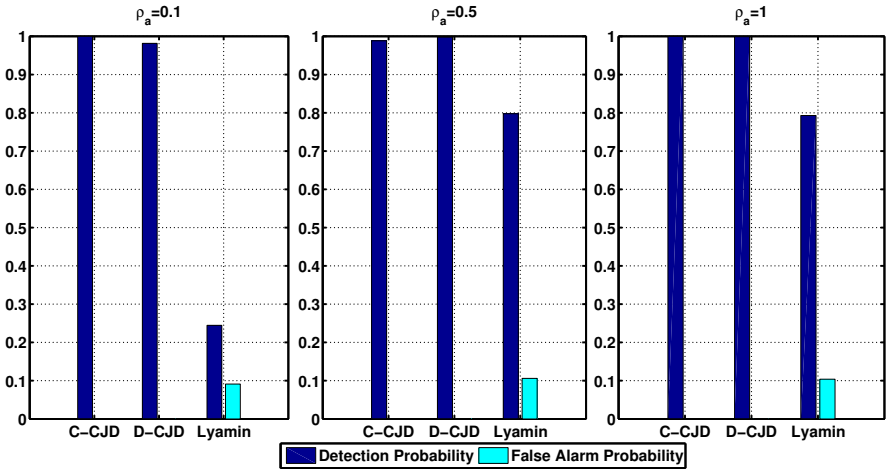
same for every vehicle. In the second part of this section, releasing above assumptions, we study our CJID detection method in more general and realistic scenarios.

Probabilities are measured during 1500 CCHIs, i.e. during simulation time of 150 s, each vehicle broadcasts one beacon each CCHI. Vehicles move to the same direction. Each scenario is run for 3 times in which jammers are located at different positions.

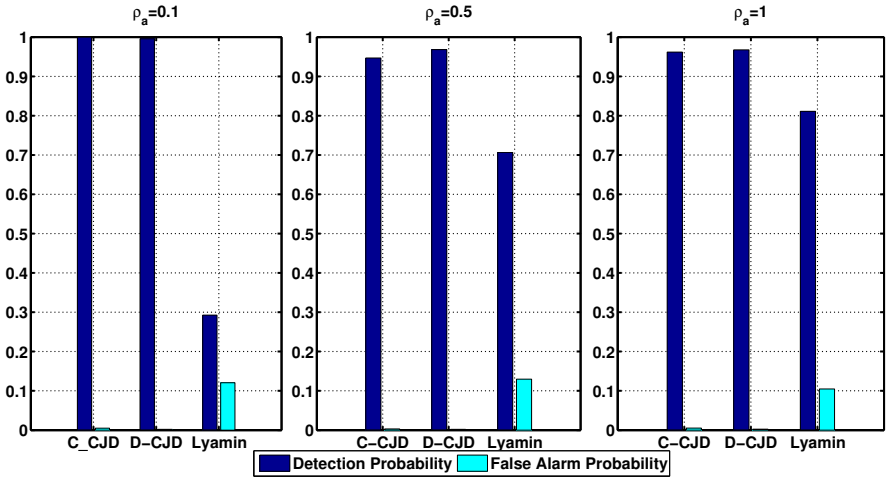
5.4.1 Platoon scenario

We study our CJD detection method in the scenario of a platoon of 10 vehicles. Vehicles move with a constant speed of 30 m/s following each other. The distance between two consecutive vehicles is around 5 meters. The central detector is installed in the head vehicle of the platoon while each vehicle deploys our CJD distributed detection method. Fig.5.12 shows the detection probability and probability of false alarms under attacks of one jammer, in Fig.5.12(b) and two jammers, Fig.5.12(a), with different attack probabilities, $\rho_a = 0.1, 0.5, 1$. Results for our Central-CJD (C-CJD) detection method, Distributed-CJD (D-CJD) detection method and Lyamin detection method are compared. The D-CJD detection probability and false alarm probability are average results reported at all individual vehicles. False alarm probability is computed for the duration when a given vehicle is within the impact range of the jammers.

Our C-CJD and D-CJD detection methods are able to detect up to 100% jammed CCHIs with nearly zero probability of false alarms. The reason is that in platoon scenario, the number of neighbors within a tagged transmission range is stable, and distances between vehicles are small. The communication among vehicles is not highly affected by interference or attenuation of the radio channel. Both factors leading to false alarms for our CJD method are limited. While the method of Lyamin et al. can detect 80% jammed CCHIs in high attack probability scenarios ($\rho_a = 0.5$ and 1) with



(a) Scenario of 1 jammer



(b) Scenario of 2 jammers

FIGURE 5.12: Detection Probability and False Alarm Probability

nearly 5% of false alarms. The false alarms come from the fact that the medium is not ideal, some beacons are not received at the detector due to bad link condition such as fading or high attenuation. In low attack probability $\rho_a = 0.1$, the method of Lyamin et al. fails to detect more than 70% of jammed CCHIs, i.e only 28% jammed CCHIs are detected. On the other hand, our C-CJD and D-CJD detect nearly all the jammed CCHIs even the jammer attacks with small probability $\rho_a = 0.1$.

As mentioned before, the work of Lyamin et al. can detect the jamming only if exactly one beacon in a group is jammed while in the wireless environment, a jamming signal can impact all nearby vehicles. Therefore, several beacons in a group can fail to be received because of the jamming. Our CJD method detects also these cases by distinguishing failed transmissions due to contention collision and jamming attacks. Hence, our method improves the detection probability compare to the related method of Lyamin et al. Besides, the work of Lyamin et al. has not mentioned about the case that more than two beacons arrive at the same time when the medium is idle, a collision

will happen and no backoff process involves. As the beacons come frequently every fix 50 ms in their assumption, collisions happen every CCHIs. Hence, the detector will never get beacons from all neighbors in a row so that the detection phase can start. It means that the initial phase will never end.

5.4.2 General scenarios

Without platooning protocols, a platoon of close vehicles is hard to be formed and it is restrictive. In general scenarios, vehicles may travel in groups but not follow each other. This situation is more common in reality. The vehicles can be distributed randomly in a considered transmission range. In this part, we study our detection method for general scenarios where groups of vehicles move along a two-lane highway. In a group, vehicles are distributed according to Poisson distribution in each lane within a range of 250 m, the distance between vehicles in a lane is minimum 10 m. Jammer attacks with probability $\rho_a = 1$, however due to mobility, not all jamming broadcast leads to dropped beacons. Vehicles are distributed along the concerned transmission range. There are periods that not all vehicles are within sensing range of the jammer. Hence, although $\rho_a = 1$, attack probability reported at individual vehicles is only around $0.2 - 0.3$.

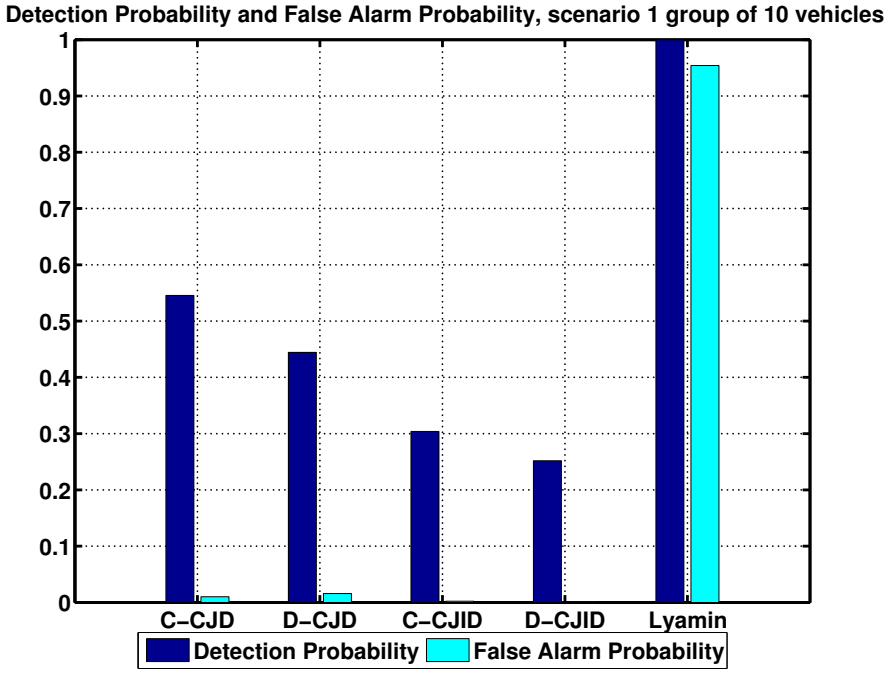


FIGURE 5.13: Detection probability and false probability in scenario 1 group of 10 vehicles

Fig.5.13 shows the performance of our detection method and the detection method of Lyamin in the scenario of a group of 10 vehicles. The monitor or detector, using the method of Lyamin et al., raises alarm all CCHIs during the simulation. That leads to 95% of false alarms. CJD and CJID methods perform not as good as in platoon scenario.

CJD method can detect nearly 45% jammed CCHIs in distributed detection method and 55% in central detection method with certain false alarm probability.

Contrary to platoon scenario, vehicles in the general scenario are distributed randomly within transmission range of each other and distances between them is bigger than in platoon scenario. Therefore, the communication among vehicles suffers from radio channel propagation loss and fading. In some CCHIs, some beacons that are supposed to be received without contention are not received due to low receive power (higher than CCA threshold but lower than sensitivity). Medium is declared busy but no transmission is recorded. This affects to computation of the parameter k in (5.16). The value of l_s (observed number of successful transmissions) is reduced while the value of l_c (observed number of failed transmission) does not change so the value of parameter k increases to over 2. Consequently, the detector will fail to detect jamming attack (if any) in the given CCHIs. Hence, compared to platoon scenario, the detection probability decreases.

Besides, contention collision, jamming attacks and interferences from ongoing transmissions in the neighborhood of the receiver concurrently exist. The CJD and detection method of Lyamin et al. operate less precisely in this scenario. They may confuse between collision (caused by contention and/or jamming attacks) and interferences. Failed transmissions are supposed to be caused by collisions in the two methods while they also can be results of poor quality connection. That leads to false alarms.

In highway scenario, there is not only one group of vehicles traveling. The observation of vehicles in a tagged group can be affected by interferences from neighbor groups. Therefore, we also study our method in scenarios of two groups and three groups of vehicles. The distance between groups, which is distance from the last vehicle in the previous group to the first vehicle in the next group, is 250 m. Performance is evaluated for a tagged group which is the first group in the scenario of 2 groups, and the middle group in the scenario of 3 groups.

The performance of CJD and CJID in scenario 2 groups and 3 groups of vehicles is shown in Fig.5.14. CJD detects with a slightly higher false alarm probability compared to the scenario of 1 group as there are interferences from neighbor groups. While at a given time, vehicles at the edge of the impact range of the jammer receive jamming with low receive power. Jamming plays the same role of interferences (low power transmission) for these vehicles. Our method differentiates interference with jamming based on signal strength. They are distinguishable if the jamming has significant higher signal strength than interference. For a low power signal, we cannot distinguish which one is the cause, jammer or interference source. Also, the vehicles mix jammings with interferences. For that reason, if a failed transmission is due to a jamming, vehicles using CJID miss to detect it. While vehicles using CJD raise false alarms if the failed transmission is due to an interference. Hence, in these scenarios, compared to CJD, CJID reduces the false alarms probability, and also detection probability. Therefore, our CJID detection method operates less effectively when the jammer is located far

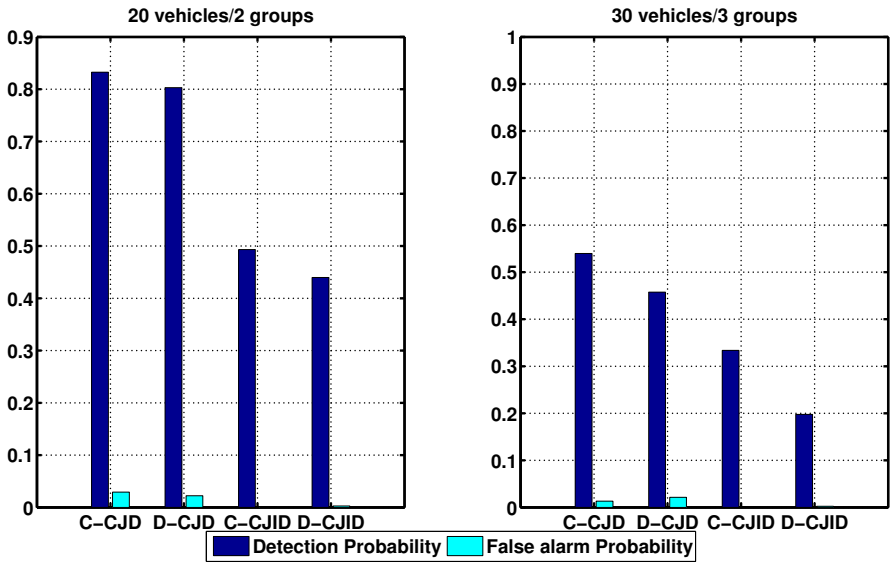


FIGURE 5.14: Detection Probability and False Alarm Probability of CJD and CJID in scenarios of 2 groups and 3 groups of vehicles

from the detector. In other words, our methods perform better for the jamming which has strong signal strength.

5.5 Conclusions

In this chapter, we have raised a discussion of reactive jamming in vehicular networks. We focus on beacons which bring important information that enables many applications, especially safety application, in ITS. An analytical jamming model is proposed in order to study the impact of reactive jamming in broadcast communication that has not been studied before in related works. Medium access contention and physical parameters are taken into account in our model. Moreover, our analytical analysis can be referred to determine thresholds to detect jamming. However, the detection methods using thresholds have shortcomings including the time delay for measuring and a certain probability of false alarms. In order to overcome these shortcomings, we propose a real-time, MAC-based detection method which can be applied for the central detector or individual vehicles. Our method aims to differentiate the three causes of a failed transmission reported at a given receiver. These are interference, contention collision and jamming. We evaluate our method with analytical analysis and network simulations. Our method is investigated in platoon scenario and general scenarios. We also compare our work to the work of Lyamin et. al. who also propose a real-time detection method but limited by strong assumptions. In platoon, distances among vehicles are so small that the observation of successful transmissions and failed transmissions is close to the computed values in our method. The simulation results show that our method detects more effectively in platoon scenarios.

Although our detection method performs not bad in studied scenarios, the precision of the proposed detection methods relies highly on the estimation of the number of neighbors. In studied scenarios, vehicles move with stable speed, consequently, the number of neighbor of a given vehicle does not change during the simulation time. Our estimation algorithm operates precisely in these scenarios. Therefore, our method especially performs well in the scenario of the platoon where the number of neighbors is kept stable and is monitored thanks to platooning technology. However, in order to implement the method in other scenarios, the technique of estimating the number of neighbors should be further investigated.

Chapter 6

Thesis Conclusions

Our contributions to improve the performance of safety applications in vehicular networks have been presented throughout the thesis. This chapter provides a resume of our contributions and proposes future works. We discuss our future research direction to complete the security system for safety applications.

6.1 Summary of Contributions

Motivated by the necessity of studies on ITS safety applications in vehicular networks, the thesis has presented technical solutions to enhance the quality of services and security of safety applications. The broadcast nature of vehicular communication creates many challenges and security threats in supporting safety applications. In order to deal with these challenges, we addressed the three main issues for safety applications in this thesis: reliability for broadcasting, the lack of connectivity in vehicular networks and the threat of jamming attacks on beacons.

With the aim of making the standardized MAC protocol more reliable, we proposed the polling scheme on which safety messages are retransmitted only when they are requested. The redundancy of the retransmissions is reduced. With our scheme, vehicles in vicinity area are noticed and then request for safety-related information that they have missed. Because our polling scheme can be implemented in standardized MAC protocol, it supports both one-hop communication and multi-hop communication when it plays a role of under layer protocol of a dissemination protocol. Hence, our proposed scheme is suitable for both types of safety applications (DEN and CAM) specified for vehicular networks. The performance evaluation of our polling scheme shows a significant improvement in term of packet delivery rate in the scenario of one-hop communication. Moreover, reliability through multi-hop path is provided when our scheme is implemented as a MAC layer for the dissemination protocol.

Considering solutions for the fragmentation of vehicular networks, we studied opportunistic forwarding protocols in vehicular networks. These protocols use different parameters to forward the safety-related information to recipients having bad connectivity in the network. Position and geographical information are commonly used.

However, when the positions of the recipients are unknown, these parameters are infeasible. Different from related works on opportunistic forwarding protocols, we propose a social-aware forwarding protocol to support the forwarding of the safety messages in this situation. As the safety messages are carried by vehicles which are encountered frequently by many other vehicles in the networks, the safety messages are forwarded to crowds where they have more opportunity to find the destination or other potential carriers. We investigated our protocol in urban scenario. From simulations, our proposed protocol performs a significantly high packet delivery rate in the studied scenario where temporary disconnection are commonly encountered.

The security of safety applications was also discussed in this thesis. Besides common threats in wireless communications, the denial of services attack, especially jamming attack, is a big threat for safety applications in vehicular networks due to its adequate operating condition. In order to investigate the degradation caused by jamming attacks on packet delivery rate of beacons, we conducted an analytical analysis. Contrary to the existing works, our work is specified for broadcasting. In our analysis, the medium access contention and physical parameters are taken into account. The analysis quantified different levels of degradation of network performance caused by jamming attacks in different scenarios. The results can be used to determine thresholds which are measured in term of packet delivery rate. These thresholds are used to distinguish the normal scenario and the attacked scenario in threshold-based detection methods. However, the requirement of time for collecting statistic data makes the existing threshold-based detection method infeasible for real-time applications. Therefore, we proposed our real-time and MAC-based detection method for jamming detections in vehicular networks. The method is feasible for both central monitoring vehicle or distributed vehicles, i.e., jamming attacks are detected at central monitor and/or at each individual vehicle in distributed manner. Since our method distinguishes three phenomena that cause a failed transmission (contention collision, interference and jamming attack), the failed transmissions caused by jamming attacks are sorted out. Hence, the jamming attacks are detected every CCHI with a high detection probability while the probability of raising false alarms is nearly eliminated.

Our proposals in this thesis are dedicated for safety applications in vehicular networks. They are studied with concerns of broadcast nature and other features of vehicular communication environment such as the characteristic of radio channel, the mobility of vehicles, etc.. Both one-hop communication and multi-hop communication are considered in our works. According to the obtained results in both analytical analysis and simulations, our technical solutions provide improvements in the performance of safety applications in different dimensions: reliability, connectivity, security.

6.2 Future works

The threat of jamming attacks on basic safety messages (beacons) in vehicular networks have been discussed in chapter 5. We focus on methods to detect this threat in real-time. After detecting, vehicles must react to it. Therefore, it remains the open issue of designing a defense protocol for jamming attacks on beacons in vehicular networks. A completed security system for vehicles to mitigate this threat is our target.

Since the jamming attacks block the communication, the cooperation among vehicles is very limited. Moreover, the time constraint of safety applications requires vehicles to react immediately to the attacks to guarantee the safety of users. All of these challenges must be considered in designing a defense protocol.

In order to defend against the jamming attacks, several strategies have been developed for MANETs, while the designing defense strategies for vehicular networks is still an open issue. The two main strategies proposed in MANETs are retreat strategy and competition strategy. In retreat strategy, when a jamming attack is detected, nodes retreat their communication to another channel (channel surfing) or position (spatial retreat). To implement channel surfing, nodes have to coordinate to switch to the same new channel when the current channel is jammed. Thus channel surfing strategy is more suitable for communication between two nodes. However, this strategy can be deployed for broadcasting if the problem of channel coordination is solved. In spatial retreat strategy, nodes try to move from the jammed regions. This strategy is well suited for mobile ad hoc networks, however, it must be considered carefully if we implement it to vehicular networks. How the vehicles change their trajectory, velocity, etc., may impact the traffic in entire road system. Especially, when there is a lack of centralized management, this may cause danger to commuters. In competition strategy, nodes reduce jamming effects by adjusting their physical-layer parameters such as transmit power, data rate and carrier sensing threshold [85]. As discussed before, the communication in vehicular environment is strongly impacted by radio channel. Thus, the feasibility of competition strategy in vehicular networks should be further investigated.

At higher layer, wireless attacks are easier to predict their operations as they follow some certain strategies. Therefore, it is possible to prevent impacts of attacks at higher layer. However, prevention methods is not limited only for higher layer, they may be also applied for attack at lower layer.

For the future work, we aim to design a security system specified for safety applications to prevent, detect and defend against jamming attacks at lower layer in vehicular networks. Requirements of safety applications and specific characteristics of vehicular networks will be considered in our works.

Appendix A

Dissemination Improvement as a function of MAC and topology parameters

Equation (3.27) can be derived from (3.26) as follows:

$$
\begin{aligned}
&{\chi_{reliable}}^{(h)} \\
&= (2h - 1 - (h-1).(P_0 + \Delta)).(P_0 + \Delta).\lambda.d \\
&= [(2h - 1 - (h-1).P_0 - (h-1).\Delta).(P_0 + \Delta)].\lambda.d \\
&= [(2h - 1 - (h-1).P_0 - (h-1).\Delta).P_0 \\
&+ (2h - 1 - (h-1).P_0 - (h-1).\Delta).\Delta].\lambda.d \\
&= (2h - 1 - (h-1).P_0).P_0.\lambda.d - (h-1).\Delta.P_0.\lambda.d \\
&+ [(2h - 1 - (h-1).P_0).\Delta - (h-1).\Delta^2].\lambda.d \\
&= {\chi_0}^{(h)} + [-(h-1).\Delta^2 + (2h - 1 - 2(h-1).P_0).\Delta].\lambda.d \\
&= {\chi_0}^{(h)} + I(h, P_0, \Delta, \lambda, d)
\end{aligned}
\tag{A.1}
$$

In this appendix, we also explain how graphs in Fig.3.6 are obtained from (3.27). The improvement in dissemination level is abstracted by below function:

$$
\begin{aligned}
&I(h, P_0, \Delta, \lambda, d) \\
&\qquad = \left[-(h-1).\Delta^2 + (2h - 1 - 2(h-1).P_0).\Delta\right].\lambda.d
\end{aligned}
\tag{A.2}
$$

When we rewrite the function according to argument Δ and consider other arguments as parameters, the function is as follows:

$$
I(\Delta) = -(h-1).\lambda.d.\Delta^2 + (2h - 1 - 2(h-1).P_0).\lambda.d.\Delta \tag{A.3}
$$

$I(\Delta)$ is a quadratic function that is in a standard format $I(\Delta) = a.\Delta^2 + b.\Delta + c$, where $a = -(h-1).\lambda.d$, $a \leq 0$; $b = (2h - 1 - 2(h-1).P_0).\lambda.d$ and $c = 0$. If $h = 1$, $a = 0$, the dissemination will become an one hop communication, the improvement at level of dissemination will be identical to the improvement at MAC layer.

If $h > 1$, i.e., $a < 0$, graph of the function is a parabola opening upward that has a turning point of $(\varepsilon, I(\varepsilon))$. The value of a depends linearly on h, λ, d. An increase of any of these parameters can lead to a decrease of a, i.e. a becomes more negative, that makes the graph steeper. The turning point is defined as below:

$$\begin{aligned} \varepsilon &= -\frac{b}{2a} \\ &= -\frac{(2h-1-2(h-1).P_0).\lambda.d}{-2(h-1).\lambda.d} \\ &= \frac{2(h-1)-2(h-1).P_0+1}{2(h-1)} \\ &= (1-P_0)+\frac{1}{2(h-1)} \end{aligned} \tag{A.4}$$

$$\begin{aligned} I(\varepsilon) &= -\frac{b^2-4\mathrm{a}c}{4\mathrm{a}} \\ &= -\frac{(2h-1-2(h-1).P_0)^2.(\lambda.d)^2}{-4(h-1).\lambda.d} \\ &= \frac{(2(h-1)(1-P_0)+1)^2.\lambda.d}{4(h-1)} \end{aligned} \tag{A.5}$$

Because $h > 1$, $\frac{1}{2(h-1)} > 0$. Therefore, $\varepsilon > (1 - P_0)$.

Appendix B

The over estimation of number of neighbors impacts precision of CJD

This appendix proves the clause in section 5.3.1: when there is no attack, the over estimation of number of neighbors, i.e $\Delta n \geq 0$, always makes $k_f \geq 2$. It is involved in equation (5.24). When there is no attack, i.e $l_a = 0$, k_f is computed as below:

$$k_f = \frac{n_0 - l_{s0} + \Delta n}{l_{c0}} = \frac{n_0 - l_{s0}}{l_{c0}} + \frac{\Delta n}{l_{c0}} \tag{B.1}$$

Moreover, when there is no attack, the parameter $k = k_0$ is always equal or bigger than 2. The fact is shown in (5.17):

$$k_0 = \frac{n - l_{s0}}{l_{c0}} \geq 2 \tag{B.2}$$

As mentioned before, parameter k is computed only when there is at least one collision noticed, i.e $l_{c0} > 0$. Therefore, if $\Delta n \geq 0$ then

$$\frac{\Delta n}{l_{c0}} \geq 0 \tag{B.3}$$

Based on (B.2) and (B.3) and computation of k_f (B.1), it can be proved that $k_f \geq 2$ when there is no attack and $\Delta n \geq 0$.

Bibliography

[1] ETSI TR 102 638 (V1.1.1) (2009-06). *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*.

[2] ETSI TS 102 637-2 V1.1.1 (2010-04). *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*.

[3] Saif Al-Sultan et al. "A comprehensive survey on vehicular Ad Hoc network". In: *Journal of network and computer applications* 37 (2014), pp. 380–392.

[4] Abdulelah Alganas, Xiaodong Lin, and Ali Grami. "EVSE: An efficient vehicle social evaluation scheme with location privacy preservation for vehicular communications". In: *Communications (ICC), 2011 IEEE International Conference on*. IEEE. 2011, pp. 1–5.

[5] Sina Asadallahi and Hazem H Refai. "Modified R-ALOHA: Broadcast MAC protocol for Vehicular Ad hoc Networks". In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*. IEEE. 2012, pp. 734–738.

[6] Abdelmalik Bachir and Ahderrahim Benslimane. "A multicast protocol in ad hoc networks inter-vehicle geocast". In: *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*. Vol. 4. IEEE. 2003, pp. 2456–2460.

[7] Soheila V Bana and Pravin Varaiya. "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks". In: *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE*. IEEE. 2001, pp. 962–967.

[8] Abderrahim Benslimane. "Optimized dissemination of alarm messages in vehicular ad-hoc networks (VANET)". In: *high speed networks and multimedia communications*. Springer, 2004, pp. 655–666.

[9] Abderrahim Benslimane and Abdelmalik Bachir. "Inter-vehicle geocast protocol supporting non-equipped GPS vehicles". In: *International Conference on Ad-Hoc Networks and Wireless*. Springer. 2003, pp. 281–286.

[10] Abderrahim Benslimane, Saman Barghi, and Chadi Assi. "An efficient routing protocol for connecting vehicular networks to the Internet". In: *Pervasive and Mobile Computing* 7.1 (2011), pp. 98–113.

[11] Abderrahim Benslimane, Saman Barghi, and Chadi Assi. "An efficient routing protocol for connecting vehicular networks to the Internet". In: *Pervasive and Mobile Computing* 7.1 (2011), pp. 98 –113. ISSN: 1574-1192. DOI: http://dx.doi.org/10.1016/j.pmcj.2010.09.002. URL: http://www.sciencedirect.com/science/article/pii/S1574119210000982.

[12] Abderrahim Benslimane, Abdelouahid El Yakoubi, and Mohammed Bouhorma. "Analysis of jamming effects on IEEE 802.11 wireless networks". In: *Communications (ICC), 2011 IEEE International Conference on*. IEEE. 2011, pp. 1–5.

[13] Abderrahim Benslimane, Tarik Taleb, and Rajarajan Sivaraj. "Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G heterogeneous wireless networks". In: *IEEE Journal on Selected Areas in Communications* 29.3 (2011), pp. 559–570.

[14] Yuanguo Bi et al. "Efficient and reliable broadcast in intervehicle communication networks: A cross-layer approach". In: *Vehicular Technology, IEEE Transactions on* 59.5 (2010), pp. 2404–2417.

[15] Jeremy Blum, Azim Eskandarian, and Lance Hoffman. "Mobility management in IVC networks". In: *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*. IEEE. 2003, pp. 150–155.

[16] Lorenzo Bracciale et al. *CRAWDAD dataset roma/taxi (v. 2014-07-17)*. Downloaded from http://crawdad.org/roma/taxi/20140717. July 2014. DOI: 10.15783/C7QC7M.

[17] Abbas Bradai and Toufik Ahmed. "ReViV: selective rebroadcast mechanism for video streaming over VANET". In: *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*. IEEE. 2014, pp. 1–6.

[18] L. Briesemeister, L. Schafers, and G. Hommel. "Disseminating messages among highly mobile hosts based on inter-vehicle communication". In: *Intelligent Vehicles Symposium, 2000. IV 2000. Proceedings of the IEEE*. 2000, pp. 522–527. DOI: 10.1109/IVS.2000.898398.

[19] Linda Briesemeister, Lorenz Schäfers, and Günter Hommel. "Disseminating messages among highly mobile hosts based on inter-vehicle communication". In: *Intelligent Vehicles Symposium, 2000. IV 2000. Proceedings of the IEEE*. IEEE. 2000, pp. 522–527.

[20] Claudia Campolo et al. "Modeling prioritized broadcasting in multichannel vehicular networks". In: *Vehicular Technology, IEEE Transactions on* 61.2 (2012), pp. 687–701.

[21] Augustin Chaintreau et al. "Impact of human mobility on opportunistic forwarding algorithms". In: *Mobile Computing, IEEE Transactions on* 6.6 (2007), pp. 606–620.

[22] Wai Chen et al. "A survey and challenges in routing and data dissemination in vehicular ad-hoc networks". In: *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*. 2008, pp. 328–333. DOI: 10.1109/ICVES.2008.4640900.

[23] Pei-Chun Cheng et al. "GeoDTN+ Nav: a hybrid geographic and DTN routing with navigation assistance in urban vehicular networks". In: *MobiQuitous/ISVCS* (2008).

[24] Ioan Chisalita and Nahid Shahmehri. "A context-based vehicular communication protocol". In: *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*. Vol. 4. IEEE. 2004, pp. 2820–2824.

[25] W Crowther et al. "A system for broadcast communication: Reservation-ALOHA". In: *Proc. 6th Hawaii Int. Conf. Syst. Sci*. 1973, pp. 596–603.

[26] Felipe D Cunha et al. "Is it possible to find social properties in vehicular networks?" In: *Computers and Communication (ISCC), 2014 IEEE Symposium on*. IEEE. 2014, pp. 1–6.

[27] Elizabeth M Daly and Mads Haahr. "Social network analysis for information flow in disconnected delay-tolerant MANETs". In: *Mobile Computing, IEEE Transactions on* 8.5 (2009), pp. 606–621.

[28] João AFF Dias, Joel JP Rodrigues, and Liang Zhou. "Performance evaluation of cooperative strategies for Vehicular Delay-Tolerant Networks". In: *Transactions on Emerging Telecommunications Technologies* 25.8 (2014), pp. 815–822.

[29] Bertrand Ducourthial, Yacine Khaled, and Mohamed Shawky. "Conditional transmissions: Performance study of a new communication strategy in VANET". In: *Vehicular Technology, IEEE Transactions on* 56.6 (2007), pp. 3348–3357.

[30] Richard Gilles Engoulou et al. "VANET security surveys". In: *Computer Communications* 44 (2014), pp. 1–13.

[31] EN ETSI. "302 665 (V1. 1.1)," in: *Intelligent Transport Systems (ITS)* (2010), pp. 2010–09.

[32] Martin Everett and Stephen P Borgatti. "Ego network betweenness". In: *Social networks* 27.1 (2005), pp. 31–38.

[33] Ghazal Farrokhi et al. "Improving Safety Messages Dissemination in IEEE 802.11 e Based VANETs Using Controlled Repetition Technique". In: *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*. IEEE. 2010, pp. 395–399.

[34] Linton C Freeman. "Centrality in social networks conceptual clarification". In: *Social networks* 1.3 (1978), pp. 215–239.

[35] Holger Füßler et al. "Mobicom poster: location-based routing for vehicular ad-hoc networks". In: *ACM SIGMOBILE Mobile Computing and Communications Review* 7.1 (2003), pp. 47–49.

[36] T. Gazdar et al. "A distributed advanced analytical trust model for VANETs". In: *Global Communications Conference (GLOBECOM), 2012 IEEE*. 2012, pp. 201–206. DOI: 10.1109/GLOCOM.2012.6503113.

[37] Tahani Gazdar et al. "A secure cluster-based architecture for certificates management in vehicular networks". In: *Security and Communication Networks* 7.3 (2014), pp. 665–683. ISSN: 1939-0122. DOI: 10.1002/sec.772. URL: http://dx.doi.org/10.1002/sec.772.

[38] Ali J. Ghandour et al. "Dissemination of safety messages in {IEEE} 802.11p/WAVE vehicular network: Analytical study and protocol enhancements". In: *Pervasive and Mobile Computing* 11 (2014), pp. 3 –18. ISSN: 1574-1192. DOI: http://dx.doi.org/10.1016/j.pmcj.2013.03.003. URL: http://www.sciencedirect.com/science/article/pii/S1574119213000424.

[39] Xiaoqin Gu, Lun Tang, and Jie Han. "A social-aware routing protocol based on fuzzy logic in vehicular ad hoc networks". In: *High Mobility Wireless Communications (HMWC), 2014 International Workshop on*. 2014, pp. 12–16. DOI: 10.1109/HMWC.2014.7000205.

[40] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. "Detection of radio interference attacks in VANET". In: *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE. 2009, pp. 1–5.

[41] Hannes Hartenstein and Kenneth Laberteaux. *VANET vehicular applications and inter-networking technologies*. Vol. 1. John Wiley & Sons, 2009.

[42] Hannes Hartenstein and Kenneth P Laberteaux. "A tutorial survey on vehicular ad hoc networks". In: *Communications Magazine, IEEE* 46.6 (2008), pp. 164–171.

[43] M.I. Hassan et al. "Effect of Retransmissions on the Performance of the IEEE 802.11 MAC Protocol for DSRC". In: *Vehicular Technology, IEEE Transactions on* 61.1 (2012), pp. 22–34. ISSN: 0018-9545. DOI: 10.1109/TVT.2011.2172964.

[44] B. Hassanabadi and S. Valaee. "Reliable Periodic Safety Message Broadcasting in VANETs Using Network Coding". In: *IEEE Transactions on Wireless Communications* 13.3 (2014), pp. 1284–1297. ISSN: 1536-1276. DOI: 10.1109/TWC.2014.010214.122008.

[45] Seyedali Hosseininezhad and Victor Leung. "Data dissemination for delay tolerant vehicular networks: using historical mobility patterns". In: *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications*. ACM. 2013, pp. 115–122.

[46] A. Hussain et al. "Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks". In: *Communications and Networks, Journal of* 16.4 (2014), pp. 397–406. ISSN: 1229-2370. DOI: 10.1109/JCN.2014.000069.

[47] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments". In: *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)* (2010), pp. 1–51. DOI: 10.1109/IEEESTD.2010.5514475.

[48] "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages". In: *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)* (2013), pp. 1–289. DOI: 10.1109/IEEESTD.2013.6509896.

[49] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multichannel Operation". In: *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)* (2011), pp. 1–89. DOI: 10.1109/IEEESTD.2011.5712769.

[50] SAE International. *DSRC Implementation Guide. A Guide of Users of SAE J2735 Message Sets Over DSRC*. 2010. URL: http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf.

[51] J.N.G. Isento et al. "Vehicular Delay-Tolerant Networks?A Novel Solution for Vehicular Communications". In: *Intelligent Transportation Systems Magazine, IEEE* 5.4 (2013), pp. 10–19. ISSN: 1939-1390. DOI: 10.1109/MITS.2013.2267625.

[52] Rupa Jagannathan et al. "Predicting Road Accidents Based on Current and Historical Spatio-temporal Traffic Flow Data". In: *Computational Logistics*. Springer, 2013, pp. 83–97.

[53] Daniel Jiang, Qi Chen, and Luca Delgrossi. "Optimal Data Rate Selection for Vehicle Safety Communications". In: *Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*. VANET '08. San Francisco, California, USA: ACM, 2008, pp. 30–38. ISBN: 978-1-60558-191-0. DOI: 10.1145/1410043.1410050. URL: http://doi.acm.org/10.1145/1410043.1410050.

[54] Brad Karp and Hsiang-Tsung Kung. "GPSR: Greedy perimeter stateless routing for wireless networks". In: *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM. 2000, pp. 243–254.

[55] Shanmukh Katragadda et al. "A decentralized location-based channel access protocol for inter-vehicle communication". In: *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*. Vol. 3. IEEE. 2003, pp. 1831–1835.

[56] Gökhan Korkmaz et al. "Urban multi-hop broadcast protocol for inter-vehicle communication systems". In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 76–85.

[57] Gökhan Korkmaz et al. "Urban multi-hop broadcast protocol for inter-vehicle communication systems". In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 76–85.

[58] Kevin C Lee and Mario Gerla. "Opportunistic vehicular routing". In: *Wireless Conference (EW), 2010 European*. IEEE. 2010, pp. 873–880.

[59] Fan Li and Yu Wang. "Routing in vehicular ad hoc networks: A survey". In: *Vehicular Technology Magazine, IEEE* 2.2 (2007), pp. 12–22.

[60] Ming Li, Kai Zeng, and Wenjing Lou. "Opportunistic broadcast of event-driven warning messages in vehicular ad hoc networks with lossy links". In: *Computer Networks* 55.10 (2011), pp. 2443–2464.

[61] X. Lin et al. "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications". In: *IEEE Transactions on Vehicular Technology* 56.6 (2007), pp. 3442–3456. ISSN: 0018-9545. DOI: 10.1109/TVT.2007.906878.

[62] X. Lin et al. "Security in vehicular ad hoc networks". In: *IEEE Communications Magazine* 46.4 (2008), pp. 88–95. ISSN: 0163-6804. DOI: 10.1109/MCOM.2008.4481346.

[63] Genping Liu et al. "A routing strategy for metropolis vehicular communications". In: *Information networking. networking technologies for broadband and mobile networks*. Springer, 2004, pp. 134–143.

[64] Te-Kai Liu, John A Silvester, and Andreas Polydoros. "Performance evaluation of R-ALOHA in distributed packet radio networks with hard real-time communications". In: *Vehicular Technology Conference, 1995 IEEE 45th*. Vol. 2. IEEE. 1995, pp. 554–558.

[65] Xin Liu et al. "Exploring social properties in vehicular ad hoc networks". In: *Proceedings of the Fourth Asia-Pacific Symposium on Internetware*. ACM. 2012, p. 24.

[66] Christian Lochert et al. "A routing strategy for vehicular ad hoc networks in city environments". In: *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*. IEEE. 2003, pp. 156–161.

[67] Matthias Lott et al. "Medium access and radio resource management for ad hoc networks based on UTRA TDD". In: *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. ACM. 2001, pp. 76–86.

[68] R. Lu, X. Lin, and X. Shen. "SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks". In: *INFOCOM, 2010 Proceedings IEEE*. 2010, pp. 1–9. DOI: 10.1109/INFCOM.2010.5462161.

[69] Pei'en Luo et al. "Performance evaluation of vehicular dtn routing under realistic mobility models". In: *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*. IEEE. 2008, pp. 2206–2211.

[70] Nikita Lyamin et al. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 p Vehicular Networks." In: *IEEE Communications letters* 18.1 (2014), pp. 110–113.

[71] Xiaomin Ma et al. "Capture effect on R-ALOHA protocol for inter-vehicle communications". In: *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*. Vol. 4. IEEE. 2005, pp. 2547–2550.

[72] Xiaomin Ma et al. "Design and analysis of a robust broadcast scheme for VANET safety-related services". In: *Vehicular Technology, IEEE Transactions on* 61.1 (2012), pp. 46–61.

[73] Christian Maihöfer, Tim Leinmüller, and Elmar Schoch. "Abiding geocast: time–stable geocast for ad hoc networks". In: *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*. ACM. 2005, pp. 20–29.

[74] Andreas Mann and Johannes Rückert. "A new concurrent slot assignment protocol for traffic information exchange". In: *Vehicular Technology Conference, 1988, IEEE 38th*. IEEE. 1988, pp. 503–508.

[75] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions". In: *Vehicular Communications* 1.2 (2014), pp. 53–66.

[76] Khaleel Mershad, Hassan Artail, and Mario Gerla. "ROAMER: Roadside Units as message routers in {VANETs}". In: *Ad Hoc Networks* 10.3 (2012), pp. 479 –496. ISSN: 1570-8705. DOI: http://dx.doi.org/10.1016/j.adhoc.2011.09.001. URL: http://www.sciencedirect.com/science/article/pii/S1570870511001922.

[77] Huong Nguyen Minh and Abderrahim Benslimane. "Polling scheme for reliable broadcasting in vehicular networks". In: *Communications (ICC), 2014 IEEE International Conference on*. IEEE. 2014, pp. 330–335.

[78] Tomotaka Nagaosa and Takaaki Hasegawa. "Code assignment and the multicode sense scheme in an inter-vehicle CDMA communication network". In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 81.11 (1998), pp. 2327–2333.

[79] Vinod Namboodiri, Manish Agarwal, and Lixin Gao. "A study on the feasibility of mobile gateways for vehicular ad-hoc networks". In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 66–75.

[80] H. Nguyen-Minh, A. Benslimane, and A. Rachedi. "Jamming detection on 802.11p under multi-channel operation in vehicular networks". In: *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*. 2015, pp. 764–770. DOI: 10.1109/WiMOB.2015.7348039.

[81] Hassan Omar, Weihua Zhuang, and Li Li. "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs". In: *Mobile Computing, IEEE Transactions on* 12.9 (2013), pp. 1724–1736.

[82] Chia-Ching Ooi and N Fisal. "Implementation of geocast-enhanced AODV-bis routing protocol in MANET". In: *TENCON 2004. 2004 IEEE Region 10 Conference*. IEEE. 2004, pp. 660–663.

[83] Panos Papadimitratos et al. "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation". In: *Communications Magazine, IEEE* 47.11 (2009), pp. 84–95.

[84] Yongtae Park and Hyogon Kim. "Collision control of periodic safety messages with strict messaging frequency requirements". In: *Vehicular Technology, IEEE Transactions on* 62.2 (2013), pp. 843–852.

[85] K. Pelechrinis et al. "A Measurement-Driven Anti-Jamming System for 802.11 Networks". In: *IEEE/ACM Transactions on Networking* 19.4 (2011), pp. 1208–1222. ISSN: 1063-6692. DOI: 10.1109/TNET.2011.2106139.

[86] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. "Denial of service attacks in wireless networks: The case of jammers". In: *Communications Surveys & Tutorials, IEEE* 13.2 (2011), pp. 245–257.

[87] Michal Piorkowski, Natasa Sarafijanovic-Djukic, and Matthias Grossglauser. *CRAWDAD dataset epfl/mobility (v. 2009-02-24)*. Downloaded from http://crawdad.org/epfl/mobility/200902 Feb. 2009. DOI: 10.15783/C7J010.

[88] O. Punal et al. "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation". In: *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a*. 2014, pp. 1–10. DOI: 10.1109/WoWMoM.2014.6918964.

[89] Oscar Punal et al. "Experimental Characterization and Modeling of RF Jamming Attacks on VANETs". In: *Vehicular Technology, IEEE Transactions on* 64.2 (2015), pp. 524–540.

[90] Abderrezak Rachedi and Abderrahim Benslimane. "Toward a cross-layer monitoring process for mobile ad hoc networks". In: *Security and communication networks* 2.4 (2009), pp. 351–368.

[91] F. J. Ros, P. M. Ruiz, and I. Stojmenovic. "Acknowledgment-Based Broadcast Protocol for Reliable and Efficient Data Dissemination in Vehicular Ad Hoc Networks". In: *IEEE Transactions on Mobile Computing* 11.1 (2012), pp. 33–46. ISSN: 1536-1233. DOI: 10.1109/TMC.2010.253.

[92] Pietro Salvo et al. "Timer-based distributed dissemination protocols for VANETs and their interaction with MAC layer". In: *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*. IEEE. 2013, pp. 1–6.

[93] Rául Aquino Santos et al. "Performance evaluation of routing protocols in vehicular ad-hoc networks". In: *International Journal of Ad Hoc and Ubiquitous Computing* 1.1-2 (2005), pp. 80–91.

[94] Henrik Schulze and Christian Lüders. "Basics of Digital Communications". In: *Theory and Applications of OFDM and CDMA*. John Wiley Sons, Ltd, 2006, pp. 1–49. ISBN: 9780470017401. DOI: 10.1002/0470017406.ch1. URL: http://dx.doi.org/10.1002/0470017406.ch1.

[95] Boon-Chong Seet et al. "A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications". In: *Networking 2004*. Springer. 2004, pp. 989–999.

[96] M. Segata et al. "Plexe: A platooning extension for Veins". In: *Vehicular Networking Conference (VNC), 2014 IEEE*. 2014, pp. 53–60. DOI: 10.1109/VNC.2014.7013309.

[97] S. I. Sou. "Advanced Detection of Selfish Vehicles for Local File Sharing in Sparse Vehicular Networks". In: *IEEE Communications Letters* 17.5 (2013), pp. 880–883. ISSN: 1089-7798. DOI: 10.1109/LCOMM.2013.040913.122787.

[98] Nadeem Sufyan, Nazar Abbass Saqib, and Muhammad Zia. "Detection of jamming attacks in 802.11 b wireless networks". In: *EURASIP Journal on Wireless Communications and Networking* 2013.1 (2013), pp. 1–18.

[99] Min-Te Sun et al. "GPS-based message broadcasting for inter-vehicle communication". In: *Parallel Processing, 2000. Proceedings. 2000 International Conference on*. IEEE. 2000, pp. 279–286.

[100] Gautam S Thakur, Pan Hui, and Ahmed Helmy. "Modeling and characterization of vehicular density at scale". In: *INFOCOM, 2013 Proceedings IEEE*. IEEE. 2013, pp. 3129–3134.

[101] Zan Tonguz et al. "Broadcasting in VANET". In: *2007 mobile networking for vehicular environments*. IEEE. 2007, pp. 7–12.

[102] A. M. Vegni, A. Stramacci, and E. Natalizio. "SRB: A Selective Reliable Broadcast protocol for safety applications in VANETs". In: *Mobile and Wireless Networking (iCOST), 2012 International Conference on Selected Topics in*. 2012, pp. 89–94. DOI: 10.1109/iCOST.2012.6271297.

[103] Anna Maria Vegni and Valeria Loscri. "A survey on vehicular social networks". In: *Communications Surveys & Tutorials, IEEE* 17.4 (2015), pp. 2397–2419.

[104] Albert Wasef and Xuemin Sherman Shen. "REP: location privacy for VANETs using random encryption periods". In: *Mobile Networks and Applications* 15.1 (2010), pp. 172–185.

[105] Axel Wegener et al. "AutoCast: An adaptive data dissemination protocol for traffic information systems". In: *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*. IEEE. 2007, pp. 1947–1951.

[106] Hao Wu et al. "MDDV: a mobility-centric data dissemination algorithm for vehicular networks". In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 47–56.

[107] Wenyuan Xu et al. "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*. ACM. 2005, pp. 46–57.

[108] L. Yang, J. Guo, and Y. Wu. "Piggyback Cooperative Repetition for Reliable Broadcasting of Safety Messages in VANETs". In: *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*. 2009, pp. 1–5. DOI: 10.1109/CCNC.2009.4784944.

[109] Jing Zhao and Guohong Cao. "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks". In: *Vehicular Technology, IEEE Transactions on* 57.3 (2008), pp. 1910–1922.

[110] Jing Zhao, Yang Zhang, and Guohong Cao. "Data pouring and buffering on the road: A new data dissemination paradigm for vehicular ad hoc networks". In: *Vehicular Technology, IEEE Transactions on* 56.6 (2007), pp. 3266–3277.