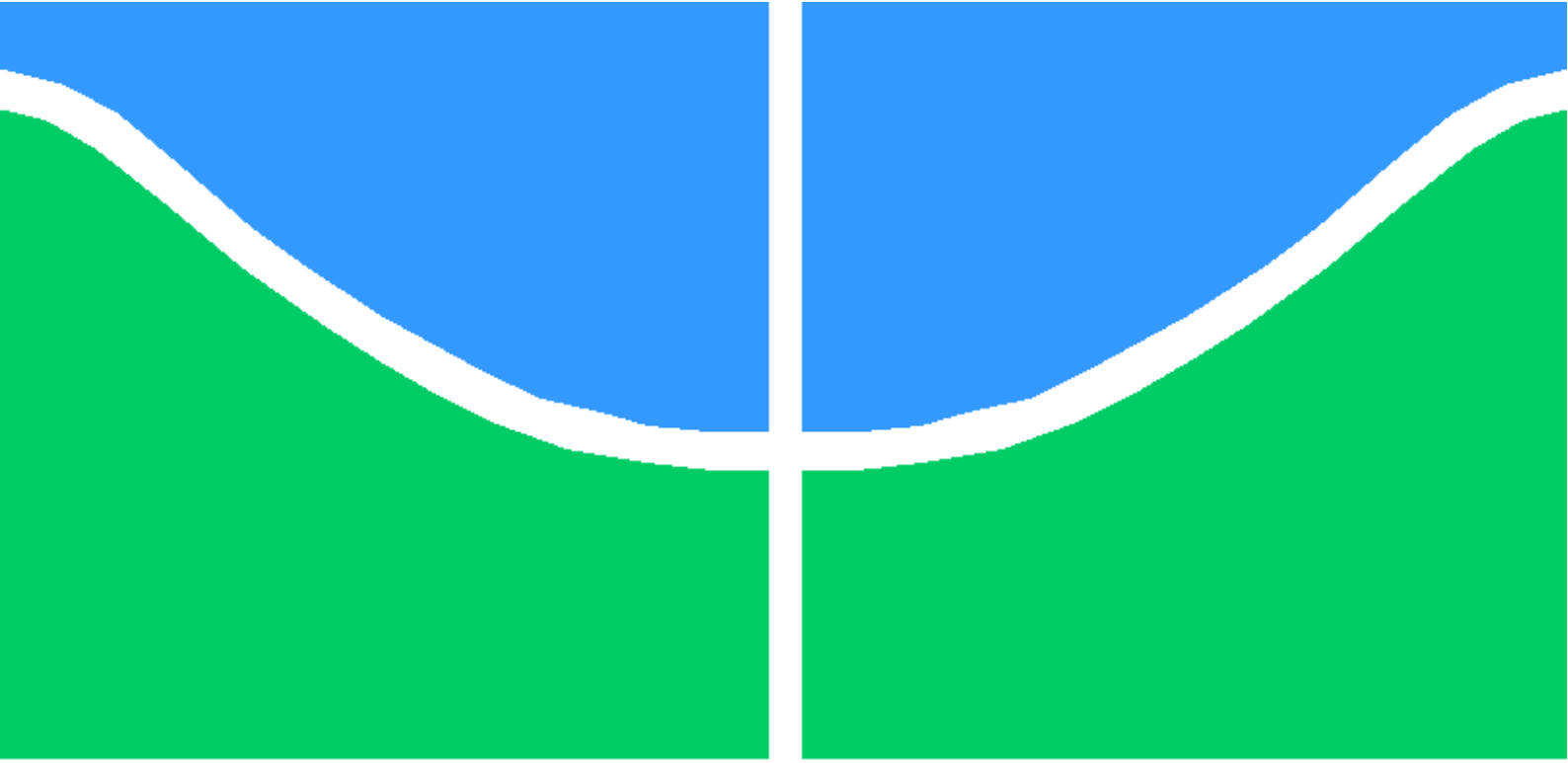


DISSERTAÇÃO DE MESTRADO

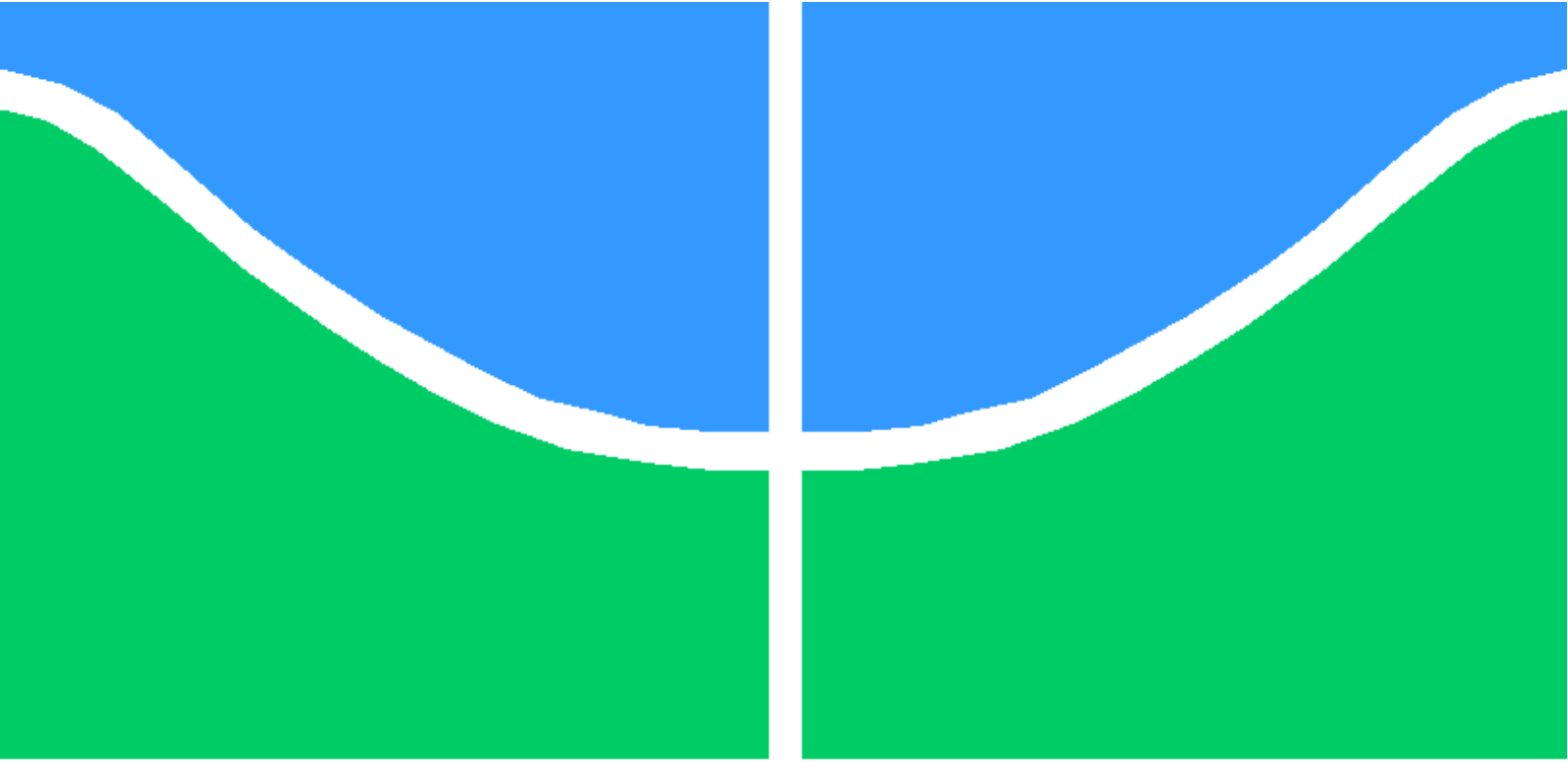
# DIFUSÃO PERIÓDICA ÓTIMA EM REDES VEICULARES COM RESTRIÇÃO DE TEMPO CONSIDERANDO O TERMINAL ESCONDIDO

**Juan Camilo Montealegre Rivera**

**Brasília, janeiro de 2015**

**UNIVERSIDADE DE BRASÍLIA**

FACULDADE DE TECNOLOGIA



DISSERTAÇÃO DE MESTRADO

# DEADLINE CONSTRAINED OPTIMAL PERIODIC BROADCASTING UNDER HIDDEN TERMINALS IN VEHICULAR NETWORKS

**Juan Camilo Montealegre Rivera**

**Brasília, janeiro de 2014**

**UNIVERSIDADE DE BRASÍLIA**

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO

# DIFUSÃO PERIÓDICA ÓTIMA EM REDES VEICULARES COM RESTRIÇÃO DE TEMPO CONSIDERANDO O TERMINAL ESCONDIDO

**Juan Camilo Montealegre Rivera**

*Relatório submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Sistemas Eletrônicos e de Automação*

Banca Examinadora

Prof. Renato Mariz de Moraes, ENE/UnB _____
*Orientador*

Prof. Marcelo Carvalho, ENE/UnB _____
*Co-Orientador*

Prof. Priscila América Solís Mendez, CIC/UnB _____
*Examinador externo*

Prof. Paulo Gondim, ENE/UnB _____
*Examinador interno*

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO

# DEADLINE CONSTRAINED OPTIMAL PERIODIC BROADCASTING UNDER HIDDEN TERMINALS IN VEHICULAR NETWORKS

**Juan Camilo Montealegre Rivera**

*Relatório submetido ao Departamento de Engenharia*
*Elétrica como requisito parcial para obtenção*
*do grau de Mestre em Sistemas Eletrônicos e de Automação*

Banca Examinadora

Prof. Renato Mariz de Moraes, ENE/UnB _____
*Orientador*

Prof. Marcelo Carvalho, ENE/UnB _____
*Co-Orientador*

Prof. Priscila América Solís Mendez, CIC/UnB _____
*Examinador externo*

Prof. Paulo Gondim, ENE/UnB _____
*Examinador interno*

**Dedicatória**

*A minha família que me apoia na distância, a minha esposa que me acompanhou nesta aventura e a todos aqueles que de uma forma ou outra estiveram envolvidos neste trabalho. Obrigado!!*

*Juan Camilo Montealegre Rivera*

## Agradecimentos

*A minha esposa Maribel, pelo carinho, paciência e ajuda nestes anos, por ter tido a coragem de me acompanhar nesta aventura e me ajudar em cada passo. Aos meus caros amigos, Jose Daniel Echeverri e Juan Esteban García, por ter-me motivado a vir ao Brasil para fazer o mestrado, e sua valiosa ajuda e acompanhamento. Ao meu caro amigo Alvaro García, pelas agradáveis conversas e companhia na distância. Aos meus colegas do GPDS pelo companheirismo e ajuda nestes anos. Ao meu orientador, o professor Renato Mariz e meu co-orientador, o professor Marcelo Menezes de Carvalho, por terem acreditado e depositado sua confiança em mim e pela paciência e motivação durantes estes dois anos.*

*Juan Camilo Montealegre Rivera*

## RESUMO

Este trabalho faz uma análise para o acesso aleatório ótimo na transmissão de mensagens com prazo de entrega final em uma rede de rádio cognitivo, considerando que a mensagem deve ser entregue para todos os nós da rede em um prazo de entrega definido. O transmissor é um usuário secundário (SU) que acessa o canal usado pelos usuários primários de forma oportunista. O protocolo de controle de acesso ao meio usado é o Slotted-Aloha onde uma transmissão por difusão tem sucesso se todos os nós receptores, dentro do alcance de transmissão do emissor, recebem a mensagem dentro do prazo de entrega definido previamente. Uma abordagem com re-transmissão de mensagens é utilizada para melhorar a confiabilidade da entrega, que necessita ter uma taxa de sucesso maior ou igual a 99,9 %, com uma latência máxima de 100 ms para cumprir as regulamentações de segurança das redes veiculares. Além disso, um novo método de análise de transmissão periódica é proposto usando uma abordagem com coeficientes multinomiais e outra baseada na função de distribuição de probabilidade geométrica.



## ABSTRACT

This work analyses an optimal random access for broadcasting messages with deadline in a cognitive radio (CR) network considering that the message must be delivery to all nodes in the network in a strict known delivery time. The transmitter is a secondary user (SU) that accesses the primary users (PUs) channel opportunistically. The slotted-Aloha medium access control (MAC) protocol is considered assuming that a successful broadcast transmission from a SU happens if all the receiver nodes within the SU transmission range receive the SU message within a given deadline. A re-broadcast approach is used to improve the reliability of the message delivery which requires a probability of success greater than or equal to 99.9% with a latency of 100 ms. Also a novel method of analysis for periodic broadcast using multinomial coefficients is introduced, as well as a method that considers a geometric distribution approach.

# Contents

# List of Figures

# List of Tables

# List of Acronyms

| | |
|---|---|
| ACK | Acknowledge |
| C2C | Car to Car Consortium |
| CALM | Continuous air interface long and medium range |
| CAMP | Vehicle safety communications consortium |
| CCH | Control channels |
| CR | Cognitive radio |
| CSMA | Carrier sense multiple access |
| CTS | Clear to send |
| DSCR | Digital short range communications |
| ETSI | European telecommunication standards institute |
| HT | Hidden terminal |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International organization of standardization |
| IVC | Inter-vehicle communications |
| LAN | Local area network |
| LLC | Logical link control |
| MAC | Medium access control |
| MANET | Mobile *ad hoc* network |
| NHTSA | National Highway Traffic Safety Administration |
| OBU | On board Units |
| PHY | Physical layer |
| PU | Primary user |
| QoS | Quality of Service |
| RSU | Roadside Units |
| RTS | Request to send |
| SAE | Society of Automotive Engineers |
| SCH | Services channels |
| SU | Secondary user |
| V2I | Vehicle to infrastructure |
| V2V | Vehicle to vehicle |
| VANET | Vehicular *ad hoc* network |
| WAVE | Wireless access in vehicular environments |
| WHO | World organization on traffic injury prevention |
| WSM | Wave short message |
| WSMP | Wireless short message protocol |

# Chapter 1

# Introdução

Em 2013, a Organização Mundial sobre Prevenção de Lesões de Trânsito (WHO) relatou que anualmente, os acidentes de trânsito causam 1,5 milhões de mortes e 60 milhões de lesões e que, em 2020, os acidentes de trânsito serão a sexta maior causa de morte no mundo. Em média, nos Estados Unidos, seis milhões de acidentes envolvendo mais de 10 milhões de veículos ocorrem todos os anos. Em 2009, estima-se que 5.505.000 acidentes de carros aconteceram, deixando 33.808 mortos e 2.217.000 pessoas feridas, com uma média de 93 mortes por dia ou uma a cada 16 minutos [1], [2]. Acidentes veiculares são realmente a principal causa de morte de pessoas entre as idades de 3 e 34 nos Estados Unidos [3].

Em 2007, aconteceram 2.392.061 acidentes localizados em interseções, respondendo por 39,7 % de todos os acidentes nos Estados Unidos [4]. Destes acidentes, 8.061 foram fatais e 1.711.000 causaram ferimentos. Estimou-se que, em média, todos os anos, 250.000 acidentes envolvem veículos que passam a intersecção com luz vermelha, colidindo com um outro veículo que cruza a intersecção em direcção lateral [3]. Para evitar acidentes com veículos, é importante compreender os eventos de pré-colisão proeminentes. O estudo constatou que 36,2 % de todos os acidentes ocorreram enquanto o veículo estava virando ou atravessando um cruzamento. Viajar fora da borda da estrada é o segundo evento de pré-colisão mais frequente, correspondendo a 22,2 % de todos os acidentes. Viajar ao longo da linha da pista é um evento pré-colisão crítico com 10,8 % de todas as colisões. Um veículo parado serviu como evento de pré-colisão crítica em 12,2 % de todos os casos. Prevenção e mitigação dessas causas comuns de acidentes, portanto, devem ter prioridade na investigação e o desenvolvimento de mecânismos de segurança. Acidentes com veículos também afetam a mobilidade no trânsito. Estima-se que cerca de 25 % dos engarrafamentos estão relacionadas a acidentes ou outros incidentes de trânsito.

O custo econômico anual devido a acidentes com veículos, apenas nos Estados Unidos, foi estimado em US $ 230.000 milhões dólares, alÃĺm dos custos estimados anuais médios de congestionamento de tráfego por pessoa em pequenas, grandes e as maiores áreas metropolitanas dos Estados Unidos são de US$ 214, US$ 407, e US$ 575, milhões de dolares respectivamente [5].

As redes veiculares ad hoc (VANETs) são redes de veículos se comunicando uns com os outros através de um canal sem fio, sem a necessidade de pontos de acesso. Nas VANETs, a mobilidade

é feita sobre rodovias e estradas e os nós não têm nenhuma restrição de consumo de energia. As VANETs podem fornecer um sistema confiável e rápido para as comunicações de segurança e transmissão de mensagens de emergência. Por outro lado, mensagens de difussão podem fornecer uma notificação precoce de um acidente ou colisão e ajudar ao motorista a assumir diferentes estratégias de condução e, potencialmente, evitar situações perigosas.

Mensagens broadcast são frequentemente usadas em varias aplicações importantes na operação de redes sem fio *ad hoc*. Exemplos dessas aplicações incluem esquemas de endereçamento dinâmico, [2] disseminação de informações de roteamento [6] e topologia ou controle de potência [7, 8]. Recentemente, o uso da camada de controle de acesso ao meio (MAC) para transmitir mensagens de segurança e alerta, tem recebido uma grande atenção, especialmente no contexto das redes veiculares *ad hoc* (VANETs). As aplicações das VANETs vão desde os serviços de emergência, tais como aplicações de segurança nas rodovias e de assistência ao condutor, até a notificação automática de acidentes ou informações sobre o estado das estradas [9, 10, 11, 12, 13, 14]. Devido a isso, o problema de entrega confiável de mensagens de difusão dentro de um determinado prazo tornou-se uma grande preocupação [15].

No cenário específico onde os nós de uma rede *ad hoc* são usuários secundários (SUs) de canais de frequência (ou slots de tempo) originalmente atribuídos a outros usuários primários (PUs), o chamado paradigma da rede cognitiva, o problema de entrega confiável de mensagens broadcast de camada MAC dentro de um determinado prazo torna-se uma questão muito difícil: neste caso, só são permitidos os SUs transmitir quando não está presente algum PU no(s) cana(is) designado(s) ou slot de tempo. Para resolver este problema, Y. Bae [16] investigou a *probabilidade de acesso ótima ao canal* que maximiza a probabilidade de entrega com sucesso de uma mensagem broadcast com restrições de tempo no prazo de entrega em uma rede cognitiva, usando o protocolo Slotted Aloha. Assume-se na pesquisa de Y. Bae que as mensagens broadcast não são confirmadas nem retransmitidas. Por isso, mensagens broadcast enviadas por um determinado SU são consideradas bem sucedidas se todos SUs dentro do raio de transmissão do emissor receberem a mensagem com sucesso dentro do prazo. Infelizmente, nesse trabalho, Y. Bae se concentra apenas no caso em que os SUs estão dentro do alcance um do outro (ou seja, uma rede *single-hop*), mas na realidade, alguns nós podem não estar dentro do alcance um do outro, o que é considerado como o problema dos *terminais escondidos* que merece ser levado em consideração. Com base nisso, esta dissertação estende os resultados de Y. Bae [16] incluindo o impacto de terminais escondidos sobre o cálculo da probabilidade de acesso que maximiza a probabilidade de entrega com sucesso (de acordo com uma determinada densidade espacial de nós). Além disso, a mensagem será retransmitida pelo nó transmissor para garantir que todos os nós dentro de seu alcance de transmissão vão receber a mensagem. O desvanecimento do canal e a probabilidade de falha na recepção também serão levados em consideração neste trabalho.

A transmissão de mensagens periódicas e suas aplicações relacionadas à confiabilidade são uma das principais forças motoras para a implementação das VANETs [17]. Nas VANETs, as mensagens de segurança são enviadas periodicamente para os nós receptores para garantir a recepção das mensagens por todos vizinhos mais próximos dentro do raio de segurança. A transmissão periódica é considerada um bom artífício para transmitir esse tipo de mensagem em baixas densidades de

nós [18], mas numa rede densa, o congestionamento torna-se uma preocupação importante, porque pode produzir um número excessivo de pacotes e resultar em métricas de confiabilidade inaceitáveis para aplicações de emergência. Devido a isso, a probabilidade de acesso ótima aplicada pelo Slotted Aloha será encontrada para melhorar o desempenho do sistema de segurança e garantir que todos os nós receberão a mensagem em um rigoroso prazo final de entrega $D_f$. Embora o objetivo principal das VANETS seja aplicações relacionadas à segurança, comunicação de dados e acesso à Internet são outras aplicações interessantes.

## 1.1 Tema da pesquisa

O tema principal da pesquisa é o desenvolvimento de um esquema para transmissão periódica confiável de mensagens de segurança com limitações de prazo de entrega. O foco do trabalho são as Redes Veiculares VANETs. Para o desenvolvimento do modelo será usado o protocolo Slotted Aloha, e para aproximar o modelo da realidade incorporar-se-á a análise de terminais escondidos, nós interferentes e o desvanecimento do canal.

## 1.2 Proposta

A proposta consiste em encontrar a probabilidade de acesso ótima, que maximiza a probabilidade de entrega com sucesso de mensagens de emergência, em uma rede cognitiva para transmitir uma mensagem periodicamente com um prazo de entrega estrito, a fim de criar um modelo de transmissão confiável. Em nossa análise serão considerados terminais escondidos, e o desvanecimento do canal também é incluído, para fazer um modelo mais aproximado da realidade. O modelo será desenvolvido matematicamente e serão feitas simulações numéricas para validá-lo.

## 1.3 Objetivos

- Desenvolver um modelo matemático para a probabilidade de acesso ótima do Slotted Aloha, que maximiza a probabilidade de entrega com sucesso, em uma rede coginitiva para transmissão de mensagens broadcast periódicas em uma VANET usando o protocolo Slotted Aloha.
- Propor esquemas para modelar a retransmissão de mensagens de emergência que aumentem a probabilidade de entrega com sucesso dessas mensagens.
- Incorporar aspectos da camada física, como desvanecimento de canal, ganho das antennas, potência de transmissão entre outras, na análise para avaliar o modelo proposto.
- Atingir os requisitos de confiabilidade e de atraso para as mensagens de segurança em redes veiculares garantindo transmissão confiável, utilizando o modelo proposto.

## 1.4 Contribuição

A principal contribuição deste trabalho é apresentar um modelo de retransmissão periódica para a comunicação broadcast em redes veiculares. O modelo proposto é apropriado para a transmissão de mensagens de segurança periódicas emitidas pelos veículos para informar aos outros sobre algum problema ou outras informações úteis. Nesta dissertação, nós também estudamos a probabilidade de acesso em uma rede cognitiva para otimizar a confiabilidade da transmissão em VANETs. Nós investigamos também o desempenho com base na probabilidade de sucesso na entrega da mensagem.

Cada veículo gera uma mensagem de emergência no início de um período de tempo. A probabilidade de sucesso é definida como a probabilidade de que todos os veículos, dentro do raio de cobertura estabelecido, recebam a mensagem no final de um período de tempo pré-definido. Foi usada uma cadeia de Markov para modelar a ocupação do canal. Mensagens broadcast periódicas foram propostas para melhorar a confiabilidade do sistema. Por outro lado, desvanecimento de canal, terminais escondidos, e nós interferentes foram incorporados à análise, e foi provado que a transmissão períodica pode ser eficaz. Mais especificamente, observa-se que a utilização de diferentes parâmetros no modelo proposto, melhora o desempenho do sistema e garante a confiabilidade.

Parte deste trabalho foi apresentado e publicado na 8a. Conferência Latinoamericana de Redes 2014 (Latin American Network Conference LANC 2014), em Montevidéu, Uruguai, com o título 'Deadline-Constrained Optimal Broadcasting under Hidden Terminals in Cognitive Networks' [19].

## 1.5 Esboço da dissertação

No capítulo 2 uma versão em inglês da introdução é apresentada. No Capítulo 3 são revisados alguns dos trabalhos anteriores sobre a aplicação de mensagens broadcast em VANETs, alguns protocolos MAC propostos e alguns parâmetros importantes que vão ser aplicados na análise. No Capítulo 4, é proposto o modelo para a probabilidade de entrega com sucesso das mensagens, incorporando os terminais escondidos. O modelo de desenvolvimento para o protocolo de re-transmissão de emergência broadcast pode ser encontrado no Capítulo 5. Também neste capítulo é apresentada a probabilidade de acesso ótima do Slotted Aloha para aplicação de transmissão periódica de mensagens de segurança em dois casos: o primeiro caso usando a distribuição geométrica e o segundo onde são usados os coeficientes multinomiais para ilustrar todos os casos de sucesso na recepção de mensagens. No Capítulo 6, é incluido o desvanecimento de canal e utilizando alguns parâmetros reais, típicos de algumas normas, como o IEEE 1609 para avaliar o protocolo. Finalmente, conclui-se a dissertação com trabalhos futuros e conclusões no Capítulo 7.

# Chapter 2

# Introduction

In 2013, the World Organization on Traffic Injury Prevention (WHO), reported that annually, road traffic crashes cause 1.5 million of deaths and 60 million of injuries, and by 2020, traffic crashes will be the 6th largest cause of death worldwide, specifically in United States, on average six million crashes involving over 10 million vehicles occur every year. In 2009, an estimation of 5,505,000 car crashes occurred, leading to 33,808 fatalities and 2,217,000 injured people, averaging 93 deaths every day or one every 16 minutes [1], [2]. Vehicular accidents are actually the leading cause of death for people between the ages of 3 and 34 in the United States [3]. In 2007, there were an estimated 2,392,061 intersection crashes, accounting for 39.7 % of all crashes in the United States [4]. From these accidents, 8061 were fatal and 1,711,000 caused injuries. It has been estimated that, on average, 250,000 accidents every year involve vehicles running a red light and colliding with another vehicle crossing the intersection from a lateral direction [3], the majority of them could be avoided if there was a reliable notification system to take actions before the accident.

The annual economic cost due to vehicle crashes, just in United States, was estimated in US$ 230 billion. To prevent vehicle crashes, it is also important to understand prominent pre-crash events. The study has found that 36.2% of all accidents occurred while a vehicle was turning at or crossing an intersection. Traveling off the edge of the road is the second most frequent pre-crash event, accounting for 22.2% of all crashes. Traveling over the lane line constituted the critical pre-crash event for 10.8% of all collisions. A stopped vehicle served as the critical pre-crash event in 12.2% of all cases. Prevention and mitigation of these common causes of accidents therefore take top priority in safety research. Vehicle crashes also affect traffic mobility. It has been estimated that approximately 25% of traffic jams are related to crashes or other traffic incidents. The estimated average annual costs of traffic congestion per person in small, large, and very large metropolitan areas in the United States are US$214, US$407, and US$575, millions of dollars respectively [5].

Vehicular *ad hoc* network (VANET) is a network of vehicles communicating with others through a wireless channel without a need for a base station. In VANETs, mobility is over highways and roads and nodes do not have any energy constraint. VANETs can provide a reliable and fast system for active safety communications. Broadcast message can provide early notification of an accident or collision and greatly help the driver to choose other driving strategies and potentially

avoid upcoming dangerous situations. Broadcast messages are frequently used in many important tasks needed in the operation of wireless ad hoc networks. Examples of such applications include dynamic addressing schemes [2], routing information dissemination [6], and topology or power control [7, 8]. Recently, the use of medium access control (MAC)-layer broadcast messages in safety-related mechanisms has received a great deal of attention, especially within the context of vehicular ad hoc networks (VANETS). VANET applications span from emergency services, such as road safety and driver assistance applications, to automatic crash notification or hazardous road condition reports [9, 10, 11, 12, 13, 14]. Because of that, the issue of *reliable* delivery of broadcast messages within a given *deadline* has become a major concern [15].

In the specific scenario where nodes of an ad hoc network act as secondary users (SUs) of frequency channels (or time slots) originally assigned to other primary users (PUs) the so called *cognitive network paradigm*, the problem of reliable delivery of MAC-layer broadcast messages within a given deadline becomes a much harder problem: in this case, SUs are only allowed to transmit when no PU is present on the designated channel(s) or time slot(s). To address this problem, Y. Bae [16] has investigated the *optimal access probability* that maximizes the successful delivery probability of a deadline-constrained broadcast message in a slotted-Aloha cognitive network. It is assumed in his work that broadcast messages are neither acknowledged nor re-transmitted. Hence, a broadcast message sent by a given SU is considered to be successful only if *all* SUs within its transmission range receive the broadcast message successfully within the deadline. Unfortunately, his work focuses only on the case where SUs are within the range of each other (i.e., a single-hop network). In reality, some nodes may not be within the range of each other, and the problem needs to take into account the impact of *hidden terminals*. Based on that, this work extends Bae's results [16] by including the impact of hidden nodes on the computation of the optimal access probability that maximizes the successful delivery probability (according to a given spatial node density). In addition, this work proposes to re-transmit periodically the message in order to guarantee that all nodes in its transmission range are going to receive the message.

Periodic broadcast and its related safety applications are one of the major driving forces for VANETs implementation [17]. In VANETs, safety messages are sent periodically for the receivers nodes for guaranteed message reception by all nodes in the system. The periodic broadcast is shown to be a good approach to transmit this kind of message in low node densities [18], but in a dense network, the congestion becomes a major concern because it can produce excessive number of collisions and result in unacceptable reliability measures for safety applications. Accordingly, the goal of this work is to determine the optimal access probability and improve the performance of the safety system, and ensure that all nodes receive the message in an strict delivery final deadline $D_f$. Although the primary objective of vehicular networks is safety related applications, data communications and internet access are other interesting applications [20].

## 2.1 Research Topic

The main theme of the research is to develop an scheme to transmit periodically a reliable periodic broadcast deadline-constrained safety messages, with special focus on Vehicular Networks VANETs. It will be used a simple MAC protocol as Slotted Aloha. To try to approximate the model to reality, will be involved in our model hidden terminals, interference nodes and fading channel.

## 2.2 Dissertation Proposal

The main proposal is to find the optimal access probability, that maximize the successful delivery probability of safety message, in a cognitive network to transmit a message periodically under a strict delivery deadline in order to create a reliable scheme, as it has been defined by multiple agencies involved in vehicular security, to transmit safety messages. Our analysis will consider hidden terminals and fading channel, for characterize a realistic model. The model will be developed mathematically and numerical simulations are presented.

## 2.3 Objectives

- Develop a mathematical model for the optimal access probability, that maximize the successful delivery probability, in a cognitive network to transmit a periodic broadcast message in a VANET using Slotted Aloha protocol.
- Propose schemes to model re-transmission of safety broadcast message in order to increase the successful delivery probability to achieve reliability metrics established in regulations.
- Incorporate in the analysis physic layer components, as channel fading, antennas gain, modulation, among others to test the proposed model.
- Develop the reliability and delay requirements for safety messages in vehicular networks to guarantee a reliable transmission, using the proposed model.

## 2.4 Contributions

The main contribution of this work is to present a novel scheme for broadcast communication in vehicular communication networks. The proposed model is suitable for transmission of periodic safety messages issued by vehicles to inform others of some problem and any other useful information. In this dissertation, we also study the optimal access probability for the Slotted Aloha in a cognitive network for optimizing the reliability of periodic safety broadcasting in VANETs. We investigate the performance of the successful delivery in periodic safety broadcasting, and consider $M$ vehicles in a cluster.

Each vehicle generates a safety message at the beginning of a time frame. The successful delivery probability is defined as the probability that all vehicles, inside a broadcast area, receive the emergency message by the end of a strict delivery deadline. We consider the modeling of the PU channel occupancy according to a Markov chain. Safety message repetition has been shown to improve the reliability of IEEE 802.11p broadcast mode [21]. Additionally, fading, hidden terminal, and interference nodes were incorporated in the analysis. In addition, we investigate the implications of that and investigate when the repetitive broadcast can be effective. More specifically, we observe that using different parameters in the model, more vehicles can be accommodated to achieve the same reliability.

Additionally, part of this work was presented and published in the 8th Latin America Networking Conference 2014 (LANC 2014) in Montevideo, Uruguay, with the title Deadline-Constrained Optimal Broadcasting under Hidden Terminals in Cognitive Networks [19].

## 2.5 Outline

In Chapter 3, we review some of the previous works on the application of broadcast messages in VANETs, a few proposed MAC protocols in literature and some important information that is applied in our analysis. In Chapter 4, we propose a model for successful delivery probability in function of access probability, with hidden terminals. Chapter 5 develops an analytically model for the re-broadcasting strategy. Also in this chapter, its presented the optimal access probability for periodic safety broadcasting application in two cases: geometric case and multinomial coefficient case. In Chapter 6, we include the channel fading in our analysis and we use some real parameters, typical of the IEEE 1609 standard, to test the protocol. Finally, we conclude with future works and conclusion remarks in Chapter 7.

# Chapter 3

# Fundamentals

## 3.1 Introduction

In this section, a review of important concepts related to VANETs is presented, especially focused in safety applications. We investigate the regulation focusing on the reliability in safety broadcast communication. The protocol used for the development of our proposal, Slotted Aloha is studied, as well as the information of the physical layer in vehicular environments. In the following sections, we look into periodic safety communication and application requirements. We discuss the problems in designing new transmission schemes with the presence of hidden terminals and interference nodes.

## 3.2 VANETs

VANETs (vehicular *ad hoc* networks) are wireless networks formed among vehicles and road units. Vehicles are equipped with network interfaces and control modules in order to participate in a VANET and acts as network nodes. VANET is also called as inter-vehicle communications (IVC) or vehicle to vehicle (V2V) communications [22]. In a VANET, all the participating vehicles are individual nodes that are connected to form a wide network. The range of transmission in a VANET is limited to 1 km [13], so hidden terminals, fading channel and interference are also considered in our work.

As VANETs are *ad hoc* networks, they do not require any network infrastructure, although it can use infrastructure as roadside units to improve their communication. Roadside units can serve as a wide range of applications like serving geographical localization. VANETs are a special subset of mobile *ad hoc* networks (MANETs) that can be formed either with vehicles and infrastructure communication or vehicles with vehicle to vehicle (V2V) communication as shown in Fig. 3.1. VANETs have some unique characteristics as:

- Vehicles move at high speed.

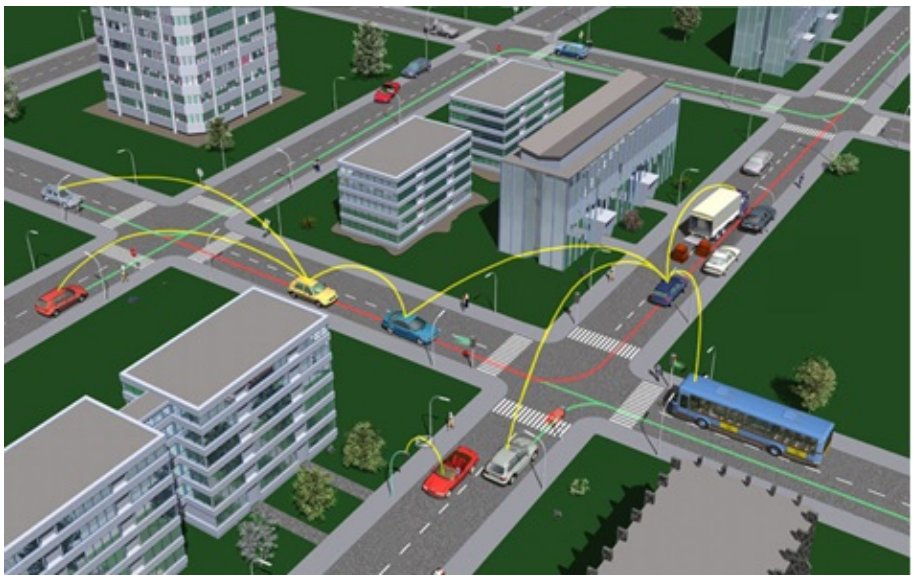


Figure 3.1: Vehicular *ad hoc* Network (VANET) [1].

- Large coverage area. Vehicles travel over long distances and traffic information may be useful to vehicles hundreds of meters away.
- Power consumption is not a major concern. Vehicles are mobile power plants.
- Vehicles have a high cost and therefore can be equipped with additional sensors without significantly impacting the total cost.
- VANETs topology is extremely dynamic as vehicles go in and out transmission range quite rapidly.
- Vehicles travel long distances in a small amount of time when compared to other mobile networks.

For the purpose of this thesis we will classify VANET applications into two major categories: safety and non-safety [23].

1. Safety applications: Safety applications has the ability to reduce traffic accidents and to improve general safety. These can be further categorized as safety-critical and safety-related applications.

   (a) Safety-critical: These are used in the case of hazardous situations. It includes the situations where the danger is high or danger is imminent Such applications can access the communication channel with highest priority. In this case delay (100 ms) and reliability of messages play an important role in realizing the safety function. Safety-critical applications involve communication between vehicles (V2V) or between vehicles and infrastructure/infrastructure and vehicles (V2I/I2V).

(b) Safety-related: These include safety applications where the danger is either low (curve speed warning) or elevated (work zone warning), but still foreseeable. In safety-related applications, the delay requirements are not as stringent as in the case of safety-critical ones. Safety-related applications can be V2V or V2I/I2V.

2. Non-safety applications: These are applications that provide traffic information and enhance driving comfort. Non-safety applications mostly involve a V2I or I2V communication. These services access the channels in the communication system, except the control channel. They access the channel in a low priority mode compared to safety applications. Non-safety applications include applications for:

   (a) Traffic optimization: Traffic information and recommendations, enhanced route guidance etc.

   (b) Infotainment: Internet access, media downloading, instant messaging, etc.

   (c) Payment services: Electronic toll collection, parking management, etc

   (d) Roadside service finder: Finding nearest fuel station, restaurants, etc. This involves communication of vehicles with road side infrastructure and the associated database.

## 3.3 Overview of Vehicular Communication Standards

IEEE 802.11a was originally adopted as the base MAC/PHY layer standard for DSRC (Digital Short Range Communications) [24]. The IEEE 802.11p standard for Wireless Access in Vehicular Environments (WAVE) [13] was a modification of the 802.11a standard, to make it capable for vehicular communications and also for supporting applications in VANETS. WAVE is based on testing and analysis of wireless communications in mobile environment [25].

According to IEEE 802.11p, vehicular communication network supports vehicular on-board units (OBU) and roadside units (RSU). An RSU has similar characteristics with a wireless LAN access point and give communications with infrastructure to VANETs [13]. Also, an RSU can control the communication between vehicles allocating channels to OBUs. There is also a third type of communicating node called Public Safety OBU (PSOBU) which is a vehicle with capabilities of providing services normally offered by RSUs. These units are mainly utilized in police cars, trucks, and ambulances in emergency situations.

DSRC provides seven channels with 10 MHz each (North America) for communications which are divided into two categories: a control channel and service channels. The control channel is reserved for broadcasting and coordinating communications for service channels. DSRC devices are permitted to switch to a service channel, and they must continuously monitor the control channel. There is no scanning and association as in the conventional 802.11. All such operations are done via a beacon sent by RSUs in the control channel, while OBUs and RSUs are allowed to broadcast messages in the control channels. Only RSUs can send beacon messages.

## 3.4 Vehicular Networks Standards

The standardization projects for VANETS are grouped geographically [26]. In Japan the development of these projects is implemented during the deployment of vehicular networking infrastructures, such as the deployment of ETC (Electronic Toll Collection) infrastructure vehicle safety communications [27]. In Europe and United States, the result of these projects is used for standardization efforts carried out by industry consortia, such as C2C-CC (Car 2 Car Communication Consortium). In particular, in United States the research and development activities are mainly contributing to the standardization of the IEEE 1609 protocol suite (Wireless Access for Vehicular Environments). In Europe the results of such activities are contributing to the ETSI (European Telecommunications Standards Institute) ITS and ISO (International Organization for Standardization) CALM (Continuous Air interface Long and Medium range) standardization. Moreover, in Japan such research and development activities are contributing to the ARIB (Association of Radio Industries and Businesses) and ISO CALM standardization, via the ISO TC (Technical Committee) 204 committee of Japan [26].

In this work we will use the parameters of the American standard called IEEE 1609 WAVE Wireless standard for vehicular environments. The complement of WAVE in higher layers is the IEEE 1609 which is a family of standards dealing with issues such as management and security of the networks and also is includes IEEE 802.11-2012 and SAE J2735-2009:

- IEEE Std 802.11-2012, IEEE Standard for Information technology Telecommunications and information exchange between systems (Local and metropolitan area networks) Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
- IEEE Std 1609.2-2013, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages.
- IEEE Std 1609.3-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Networking Services.
- IEEE Std 1609.4-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) MultiChannel Operation.
- IEEE Std 1609.11-2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Over the Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS).
- IEEE Std 1609.12, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Identifier Allocations.
- SAE J2735-2009, Dedicated Short Range Communications (DSRC) Message Set Dictionary.

The combination of IEEE 802.11p and the IEEE 1609 protocol suite is denoted as WAVE (Wireless Access in Vehicular Environments). Other ITS standardization research that is active

in the USA is the SAE (Society of Automotive Engineers) International. SAE is working in many areas, specially in standardization and with cooperation of the IEEE 1609 group, it is working on standardizing the message format to be used by the IEEE 1609 protocols. An example is the SAE J2735 standard that is meant to be used by the IEEE 1609.3 WSMP (Wave Short Message Protocol) for safety messages transmission.

The effectiveness of IEEE 802.11p amendment for traffic safety applications which require low delay, reliable, and real time communication is analyzed in [28], [29] and [30]. It has been observed that the CSMA/CA mechanism of 802.11p does not guarantee channel access before a finite deadline and therefore it gives poor performance.

## 3.5 VANET Applications

VANET applications can be dived into two types: safety applications and user applications [23]. Each type are subdivided as it is shown in Fig. 3.2 where there are 2 groups of safety (Hard, and Soft safety applications) and 3 user applications (Mobility, Connectivity and Convenience).

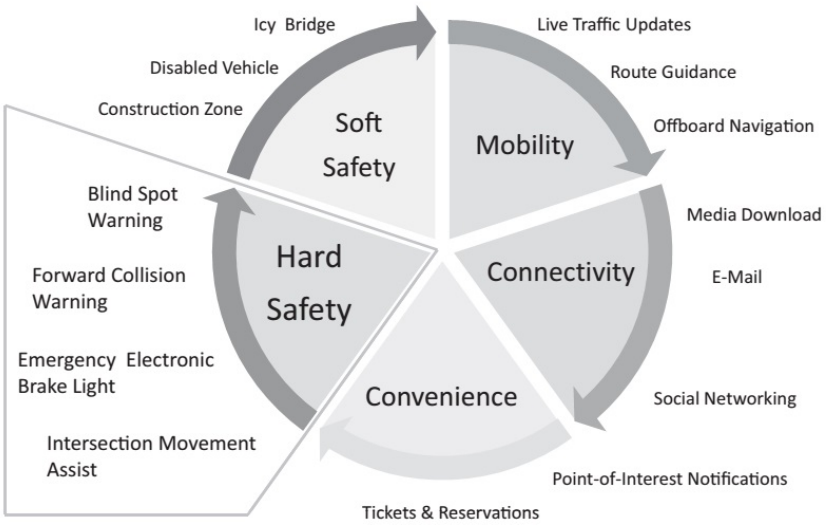



Figure 3.2: Connected vehicle applications [3].

In the next subsection we present some of safety applications for VANETs.

### 3.5.1 Safety applications

Safety applications are very important in reducing the number of accidents. More than half of the accidents can be avoided if the driver is informed with a warning half a second before the moment of accident [31]. Examples of scenarios where safety applications can avoid accidents are:

- **Accidents warning**
  In roads the vehicles are at high speed, which gives a short span for time of reactions to

the driver avoid an accident. In [32], it is presented the results about the drivers perception response time, and they concluded that it is 1.6 seconds (s) for 95 percentile of people. The results show in [33] that this reaction time is not enough to avoid an accident in most emergency cases, especially if the driver has no line of sight, due to weather condition, geography, and in some cases when exist violation of traffic rules.

The main purpose of safety applications is warn the driver early by giving an alert message of an accident occurred ahead of the road, thus, preventing the accident by giving some extra time for the driver to react.

- **Intersections warning**
  The possibility of accidents is higher in intersections because two or more traffic flows intersect in junctions which makes it a complex task for the driver. According to the Department of Transportation of the United States, in 2009, total fatalities were around 33,808. Out of the total fatalities occurred, fatalities caused in intersections are around 7,043 which is 21% of the total fatalities [34]. These accidents could be avoided if the driver is early warned by some safety application.

- **Road Congestion warning**
  Road Congestion warning applications are designed to provide for the drivers the best route to their destinations and could help to decrease road congestion, ensures smooth traffic flow and prevents traffic jams [35]. Avoiding road congestion could help the drivers job by providing a better route and makes them less stressed and indirectly it could reduces the number of accidents.

- **Passive safety applications**
  Passive safety applications are designed to work inside the vehicles and protect the drivers and passengers from injuries during the accident occurrence [34]. Air bags and safety belts are some examples of passive safety applications. It does not help to avoid accidents but they are useful to avoid fatalities and serious injuries. Post crash emergency applications are an effective subset of passive applications.

- **Lane change assistance**
  The risk of lateral collisions for vehicles that are accomplishing a lane change with blind spot for trucks is reduced.

- **Rear end collision warning**
  The risk of rear-end collisions for example due to a slow down or road curvature (e.g., curves, hills) is reduced. The driver of a vehicle is informed of a possible risk of rear-end collision in front.

- **Emergency vehicle warning**
  An active emergency vehicle, e.g., ambulance or police car, informs other vehicles in its neighborhood to free an emergency corridor. This information can be re-broadcasted in the neighborhood by other vehicles and road side units.

- **Emergency electronic brake lights**
  Vehicle that has to hard brake informs other vehicles, by using the cooperation of other vehicles and/or road side units, about this situation.

- **Wrong way driving warning**
  A vehicle detecting that it is driving in wrong way, e.g., forbidden heading, signals this situation to other vehicles and road side units.

- **Stationary vehicle warning**
  In this use case, any vehicle that is disabled, due to an accident, breakdown or any other reason, informs other vehicles and road side units about this situation.

- **Hazardous location notification**
  Any vehicle or any road side unit signals to other vehicles about hazardous locations, such as an obstacle on the road, a construction work or slippery road conditions.

## 3.6 Slotted Aloha Protocol

Slotted ALOHA is an improved version of pure ALOHA protocol. It requires that time be segmented into slots of a fixed length $T$ exactly equal to the packet transmission time. Every packet transmitted must fit into one of these slots by beginning and ending in precise synchronization with the slot segments [36]. A packet arriving to be transmitted at any given station must be delayed until the beginning of the next slot. In contrast, for pure ALOHA, a packet transmission can begin at any time.

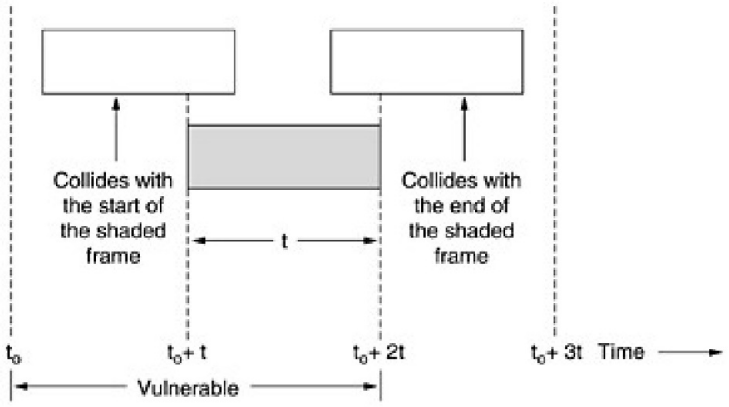



Figure 3.3: Aloha vulnerable period [36].

Slotted ALOHA requires additional overhead to provide the synchronization required between the different stations in the network [36]. In the case of slotted ALOHA, with packets synchronized to slots, it is clear that the vulnerable period is reduced to T seconds since only packets transmitted in the same slot with the reference packet can interfere with it, which makes the vulnerable period equals to $2T$ as shown in Fig. 3.3. When a node has a packet to send, it waits until the start of the next slot to send it. If no other nodes attempt transmission during that slot, the transmission is

successful, otherwise a collision happens and the collided packets are re-transmitted after a random delay.

### 3.6.1 Throughput of the Slotted-Aloha

The throughput $S$ (frames/s) defines the average number of frames successfully transmitted per unit time. We first focus on a specific packet $x$ and calculate the probability that $x$ is successfully delivered. There are a total number of $N$ users in the system, all packets have length $T$, and each user transmits with probability $p$ within a time period of $T$. Then it must be calculated the probability that $\{x$ is successfully delivered$\}$, $p$ and the probability that {No other packets within the vulnerable period $T\}$ which equals $(1-p)^{N-1}$.

To calculate the throughput of the system, we focus on a time period of length $T$. The best possible is to transmit one packet within this time period. In the Slotted-Aloha protocol, there are about $N$ transmission attempts and each one has a probability of $p$ to go through. Thus the average total number of packet that can successfully go through is

$$S = Np(1-p)^{N-1}. \tag{3.1}$$

To obtain the maximum value of the Slotted-Aloha, Eq. (3.1) should be differentiated with respect to $p$ and equated it to zero, i.e., $\frac{dS}{dp} = 0$. Using Eq. (3.1)

$$\frac{dS}{dp} = N\left[(1-p)^{N-1} + p\,(N-1) + (1-p)^{N-1}\,(-1)\right] = 0$$

$$(1-p)^{N-1} = p\,(N-1)\,(1-p)^{N-2}\,(1-p) = p(N-1).$$

$$1 - p = pN - p \tag{3.2}$$

From Eq. (3.2) it is obtained that

$$p = \frac{1}{N}. \tag{3.3}$$

To find the total throughput, we use $p$ obtained in Eq. (3.3) and replace it in Eq. (3.1)

$$S = N\frac{1}{N}\left(1 - \frac{1}{N}\right)^{N-1} = \left(1 - \frac{1}{N}\right)^{N-1}$$

Rearranging the terms in Eq. (3.4),

$$S = \frac{\left(1 - \frac{1}{N}\right)^{N}}{1 - \frac{1}{N}}. \tag{3.4}$$

Taking the limit, when $N$ goes to infinity, we have

$$S = \lim_{N \to +\infty} \frac{\left(1 - \frac{1}{N}\right)^{N}}{1 - \frac{1}{N}} = \frac{1}{e}. \tag{3.5}$$

Eq. (3.5) represents the throughput of the Slotted Aloha.

## 3.7 Hidden Terminal Problem

An *ad hoc* network has the advantage that multiple concurrent transmissions can take place simultaneously at geographically separated locations. However, such a capacity gain may be offset by the hidden terminal problem. Hidden terminals are two terminals that, although they are outside the interference range of one another, share a set of terminals that are within the transmission range of both [1].

The problem of hidden terminals is a critical issue in the performance of *ad hoc* networks. In order to prevent data packet collisions due to hidden nodes, IEEE 802.11 [13] supports virtual carrier sensing or the RTS/CTS mechanism in addition to physical carrier sensing which detects the channel to determine if it is busy or idle. In this mode of DCF operation, a pair of small control packets, called RTS and CTS, it is transmitted initially in order to avoid costly data packet collisions [13].

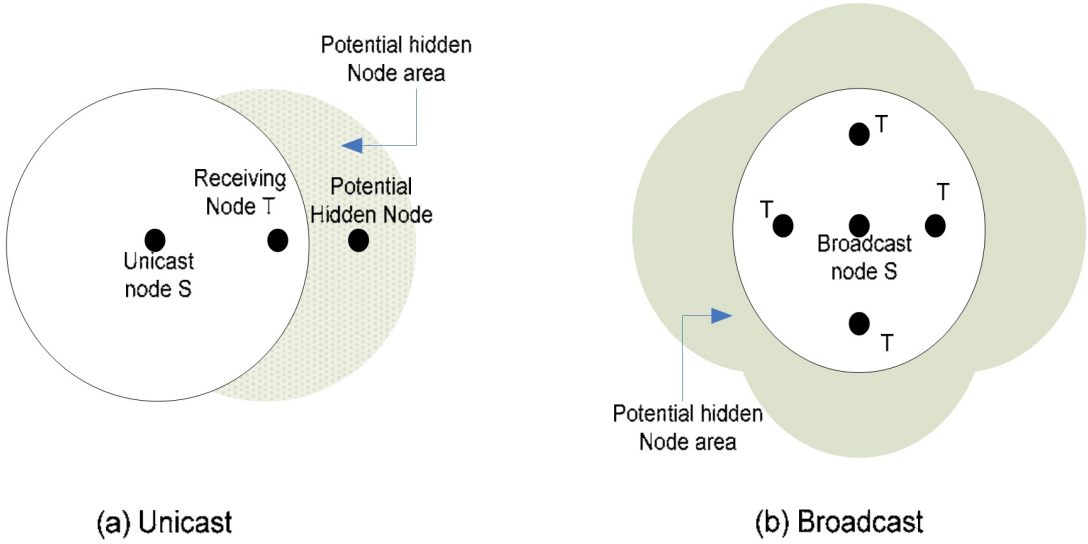



Figure 3.4: Hidden terminal for unicast and broadcast [1].

As seen in Fig. 3.4, terminals in the receiving region of terminal T but not in the receiving region of terminal S (shaded area in Fig. 3.4), may cause hidden terminal problem. We call the area as a potential hidden terminal area. For unicast communications (see Fig. 3.4 (a)), the size of the potential hidden terminal area can be identified and calculated using the distance between the sender and the receiver. However, broadcast in IEEE 802.11 does not use virtual carrier sensing and thus only relies on the physical carrier sensing to reduce collisions. In case of broadcast communication (see Fig. 3.4 (b)), the potential hidden terminal area needs to include the receiving range of all the terminals within the transmission range of the senders. Thus, the potential hidden terminal area in broadcast can be dramatically larger than that of unicast. In other words, the broadcast fashion of V2V safety communications makes them very sensitive to hidden terminals.

### 3.7.1 Reliable Protocols

Broadcasting in VANETS are used in several applications where reliability is necessary and time is a critical variable [37]. The safety message in VANETs opened a new research topic of deadline constrained reliable broadcasting that intended to serve public safety related applications. The main concern for reliable protocols is to develop a protocol that can deliver a message from a single node to all nodes within its transmission range with the highest probability of success and minimum latency [38]. The main performance metrics for reliable protocols are [1]:

- Probability of Success: the probability of all the receiver nodes successfully receive the broadcast message.
- Delay: the total time required in a single broadcast phase to transmit the message.

## 3.8 Reliability and Delay in Vehicular Networks

Vehicle Safety Communications (VSC) consortium specified several performance requirements derived from the traffic safety applications [17]. From these requirements, the most significant ones are: (1) safety messages should have a maximum delay of 100 ms, (2) a generation frequency of 10 messages per second and (3) they should be able to travel for a minimum range of 150 meters.

On the other hand, ASV (Advanced Safety Vehicle) program is divided into four phases [26]; ASV-1, which was conducted during 1991 to 1995, ASV-2 between 1996 to 2000, ASV-3 between 2001-2005 and ASV-4 between 2006 to 2010. ASV-1 and ASV-2 mainly focused on traffic safety and efficiency applications supported by vehicle to infrastructure communications, while ASV-3 and ASV-4 focused on the direct communication between vehicles and the infrastructure-based communication is only used for augmentation. The main purpose of ASV-3 and ASV-4 is to develop a vehicle to vehicle based driver information and warning system. The demonstration project results took place on a test track in Hokkaido in October 2005.

Partial market introduction is envisaged soon. ITS-Safety 2010 [27] defines the frequency bands that will be used for vehicle to vehicle, vehicle to road and for radar communication. In particular, one interesting point to observe in Japan is that the frequency band of 700 MHz is expected to be introduced for V2V safety applications. In 2008 and 2009 verification testing on public roads has been accomplished. The start for a nation-wide deployment is planned to take place soon.

### 3.8.1 Reliability

Reliable local information dissemination is the primary concern for periodic safety broadcasting in VANETs [20]. In order to establish a metric of reliability the "CAMP vehicle safety communications consortium Safety applications" defined that a safety message require at least a 99.9% probability of successful transmission in order to be effective [39]. In the same way the ITS-Safety 2010 Ministry of Transport and Telecommunications of Japan defined that the probability of the

message delivery failure in a vehicular network should be less than 0.01 (or packet delivery ratio greater than 0.99)[40].

Also, The Society of Automotive Engineers SAE - SAE J2735 (Society of Automotive Engineers DSRC), a vehicle needs to receive the messages of all its neighbors by the end of a CCH interval in order to be sure of safety condition. Even if $n-1$ messages are received successfully, the missing vehicle state can be hazardous and the received messages do not guarantee local safety [1]. So a delivery is defined to be successful if and only if the messages from all other neighbor nodes are received successfully.

Car-2-Car Communication Consortium Europe (C2C), defines reliability in Safety applications as strong demands on reliability in the sense that a broadcast safety message should reach the highest number of intended destinations [5]. The probability of the message delivery failure in a C2C must be less than 0.01. Further development and standardization of communications protocols for V2V ensure scalability and reliability of 99.9%.

### 3.8.2 Delay Requirement of Vehicular Communication

A vehicular safety system is successful if it can recognize a dangerous situation before the driver of a vehicle does and transmit an emergency message to all neighbors in order to avoid an accident. For example, if the car immediately in front suddenly stops, the driver needs to detect the brake lights, decide that the brakes should be applied, and move the appropriate muscles to apply the brakes. The mental processing time, i.e, the time from the moment an event occurs until the moment a decision is made, it is between 500 ms to 1.2 s, depending on how unexpected the event is [41]. Noting that the warning message alerting a driver, itself needs to be processed, it was conclude that communication delay must not exceed 100 ms. This value is, henceforth, called the lifetime of a safety message [17].

## 3.9 Vehicular Broadcast MAC for Safety Messages

Safety-related applications of VANETs, such as emergency electronic brake light, require the vehicle to transmit the safety message to its local neighborhoods [42]. To support that applications, broadcast communication should be highly reliable. As we said before, broadcast safety messages should be delivered to the vehicles in the local neighborhood within a maximum delay constraint with a high probability of success. Thus, the vehicular broadcast MAC mechanism must ensure a guaranteed quality of service (QoS) for these periodic safety messages.

The safety messages size are comparable to that of the control packets, so they are not so big as the service messages. The current MAC layer of DSRC is based on the IEEE 802.11 Distributed Coordination Function (DCF) [13]. In broadcast communication with 802.11p experiment collisions due to the hidden terminal problem is worsened by realistic radio propagation models [43]. Simulations of 802.11p in vehicular scenarios showed that in some cases, with special conditions, it is possible to meet the 100 ms delay requirement for safety applications with single-hop

broadcast safety packets, however reliability could not be guaranteed [44]. [38] and [45] provide analytic studies of the IEEE 1609 MAC and show its deficiencies in providing reliable broadcast, and cite packet collisions from hidden terminals and packet loss due to the harsh fading channel as limiting factors. These two problems are solved in part in the unicast case with RTS/CTS/ACK handshaking control packets in 802.11's unicast protocol, respectively, but are not possible for the broadcast messages.

For reliable broadcast CSMA-based MAC protocols, it has been proposed adaptations of the RTS/CTS/ACK mechanism for broadcasting transmissions, performing it with all receivers [46], [47], [48] or by selecting a single (farthest) neighbour [49], [50]. The safety messages are short and could be comparable with those of the control packets. Besides, control packets consumes more network resources and adds a contention period and a probability of collision.

### 3.9.1 Rebroadcasting

To improve the broadcast reliability it has been proposed the technique of re-transmitting the same message several times [20]. The problem of re-transmitting the message is that it impacts directly the size of the message and also there is the issue of how many times are considered practically enough to guarantee reliability. Xu et al. [51] investigated the effect of re-transmission to increase the reliability and developed six MAC protocols:

- Asynchronous Fixed Repetition (AFR): the message is repeated in each time-slot for a fixed number of times.
- Asynchronous p-persistent Repetition (APR): the transmitter node transmits the message in each time-slot with probability $p$, where $p$ is a configurable parameter.
- Synchronous Fixed Repetition (SFR): is the same as AFR except that all nodes in the network are synchronized to a global clock.
- Synchronous p-persistent Repetition (SPR): is the same as APR except that all nodes in the network are synchronized to a global clock.
- Asynchronous Fixed Repetition with Carrier Sensing (AFR-CS): is the same as AFR except that the channel is sensed before transmission.
- Asynchronous p-persistent Repetition with Carrier Sensing (APR-CS): is the same as APR except that the channel is sensed before transmission.

Although both SFR and AFR-CS protocols gave the best success rate, the author suggests using the AFR-CS as it does not require a global synchronization and it uses the minimum overhead. He was the first to address re-transmission as a method of increasing reliability. Although it did not solve the hidden node problem, and the AFR-CS protocol requires the same number of repetitions neglecting the effect of network condition and traffic volume.

Alshaer, et al. [41] proposed an adaptive rebroadcasting algorithm where each vehicle determines its own probability of re-transmission according to an estimate of the density of vehicles around it within two-hops. The density information is obtained from periodical packets that are involved in the operation of the *ad hoc* routing protocols. The operation of this protocol depends on the routing protocol used. Besides, it ignored the effect of hidden node problem.

## 3.10 PHY Layer in VANETs

The wireless radio channel causes a great impact in the reception of packets. Path loss and shadowing cause the variation in received signal power as well as distance. Path loss, [52], is caused by dissipation of the power radiated by the transmitter as well the effects of the propagation channel. Shadowing is caused by obstacles between transmitter and receiver that attenuate signal power through absorption, reflection, scattering and refraction. Variations due to path loss occurs over long distances while shadowing occurs over distances proportional to the obstructing length. Since both are relatively long distances they are considered as large-scale propagation effects. Multipath is due to the reception of multiple components of the signal. These components may be delayed, attenuated, shifted in phase and/or frequency from the LOS (Line of Sight) signal path at the receiver [53]. Variations due to multipath are on the order of the wave length and are considered as small-scale propagation effects.

The Free Space Model considers a perfectly reception of the signal over one path at distance $d$ [52]. The reception is on Line of Sight (LOS) and free of obstacles, so that

$$P_r = \frac{P_t G_t G_r \lambda^2}{4\pi^2 d^2 L}, \tag{3.6}$$

where $P_r$ and $P_t$ are the receiving and transmitting power, respectively, $G_r$ and $G_t$ are the receiving and transmitting antennas gains, $\lambda$ is the wave length, $L$ is the system loss and $d$ is the distance between receiver and transmitter.

Free space propagation can be also expressed in relation to a reference point $d_0$,

$$P_r(d) = P_t K \left(\frac{d_0}{d}\right)^L, \tag{3.7}$$

where K is a unit-less constant that depends on the antenna characteristics and free-space path loss up to distance $d_0$, and $L$ is called the path loss exponent.

## 3.11 Path Loss and Shadowing

### 3.11.1 Nakagami Distribution

The probability density distribution (PDF) that is frequently used in VANETs to characterize the statistics of signals transmitted through multipath fading channels is the Nakagami-m distri-

bution [54]. The pdf for this distribution is given by Nakagami [55] as

$$p(x) = \begin{cases} \frac{2}{\Gamma(m)} \left(\frac{m}{\Omega}\right)^m x^{(2m-1)} e^{(\frac{-mx^2}{\Omega})} & \text{if } x > 0; \\ 0 & Otherwise, \end{cases} \tag{3.8}$$

where $\Omega$ is defined as the expected value of the received power

$$\Omega = E[X^2], \tag{3.9}$$

and the parameter $m$ is the fading figure

$$m = \frac{\Omega^2}{E[(X^2 - \Omega)^2]}. \tag{3.10}$$

By setting $m = 1$, we observe that Eq. (3.8) reduces to a Rayleigh pdf. For values of $m$ in the range $\frac{1}{2} < m < 1$, we obtain pdfs that have larger tails than a Rayleigh-distributed random variable. For values of $m > 1$, the tail of the pdf decays faster than that of the Rayleigh. Fig. 3.5 illustrates the Nakagami pdf for different values of m.

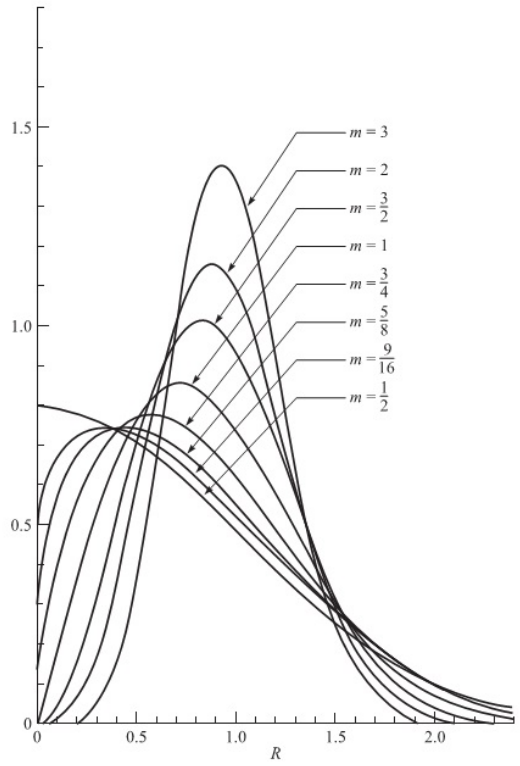



Figure 3.5: The PDF for the Nakagami-m distribution, shown with $\Omega = 1$. $m$ is the fading figure [4].

### 3.11.2 Fading Channel

In VANETs the most used modulation for emergency transmissions is the binary shift keying (PSK) modulation [20]. The error probability rate performance for binary shift keying (PSK)

modulation, when these signals are transmitted over a frequency-nonselective, slowly fading channel is [53]

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right). \tag{3.11}$$

where $E_b$ is the energy per bit and $N_0$ is the noise power spectral density. By setting $\gamma_b = \frac{E_b}{N_0}$ we have that

$$P_b(\gamma_b) = Q(\sqrt{2\gamma_b}). \tag{3.12}$$

We view Eq. (3.12) as conditional error probability, where the condition is that the attenuation parameter is fixed. To obtain the error probabilities when the attenuation $\alpha$ is random, we must average $P_b(\gamma_b)$, given in Eq. (3.11) , over the probability density function $\gamma_b$. That is, we must evaluate the integral

$$P_b = \int_0^\infty P_b(\gamma_b)p(\gamma_b)d\gamma_b. \tag{3.13}$$

where $p(\gamma_b)$ is the probability density function of $\gamma_b$ when $\alpha$ is random.

### 3.11.3 Nakagami Fading

According to [53] if the attenuation parameter $\alpha$ is characterized statistically by the Nakagami-m distribution, the random variable $\gamma = \frac{\alpha^2 E_b}{N_0}$ has the pdf

$$P(\gamma) \quad = \quad \frac{m^m}{\Gamma(m)\overline{\gamma}^m}\gamma^{m-1}e^{\frac{-m\gamma}{\overline{\gamma}}}. \tag{3.14}$$

where $\overline{\gamma} = \frac{E(\alpha^2)E_b}{N_0}$.

The average probability of error for any of the modulation methods is simply obtained by averaging the appropriate error probability for a nonfading channel over the fading signal statistics. It has been shown that Nakagami distribution with properly estimated parameters would be a more realistic channel model for vehicle-to-vehicle communications [37], [54], [56]. In this work we use the Nakagami channel model for the vehicle-to-vehicle communication link. The probability density function of the signal amplitude is given as in Eq. (3.14) and $m$ is the fading figure. The path loss component can take values from 1.61 to 4.0 in VANETs. For example, Table. 3.1 has been reported for highways [57]. Values of $m$ in VANETs are typically represented by [54]

$$m_1 = \begin{cases} 1.75 & \text{if } d < 80; \\ 0.75 & \text{if } d > 80. \end{cases} \tag{3.15}$$

## 3.12 Conclusions

In this section, a review of the research topic was presented. We investigated previous works focused on the reliability of broadcast communication in vehicular networks, discussing its applicability for safety broadcast messages in vehicular environments. Safety applications are very

Table 3.1: Reported path loss values for V2V propagation channels [5],[6] and [7]

| **Scenario** | **Path-loss** |
|---|---|
| Highway | 1.9 - 4.0 |
| Rural | 2.3 - 4.0 |
| Suburban | 2.1 - 4.0 |
| Urban | 1.61 |

important for avoiding vehicle accidents and prevent fatalities and serious injuries. Metrics of reliability and delay have been presented, where a probability of success of 99.9 % in a final deadline 100 ms has been proposed by regulations, and they are going to be used as metrics of performance in this work. The standard IEEE 1609 was proposed to provide and standardize vehicular communications, but it was not intended to ensure safety, security health or environmental, and health practices or regulatory requirements [58]. Thus, new mechanisms to guarantee safety and security should be studied. An overview of path loss and shadowing were presented. The free space model was used to obtain the reception power as function of the distance, antennas gains, system path loss and transmitted power, and the Nakagami-m model for characterizing the signal transmitted in a multipath fading channels is considered.

# Chapter 4

# Nonperiodic Broadcast with Hidden Terminals

## 4.1 Introduction

In this Chapter, a model for non-periodical broadcast message will be developed, and the presence of hidden terminals will be included. The successful delivery probability $p_s$ will be analyzed to find the optimal access probability in order to improve the performance of the system. The first sections presents the model for the cognitive network used and all the assumptions that we made in our analysis. Two scenarios will be analyzed: with and without primary user (PU) present in the system to test the model in these two environments. Some numerical results will be presented at the end of the chapter to compare the performance of the protocol.

## 4.2 System Model

We follow Bae's assumptions [16], which are *i*) the wireless channel is time-slotted with the Aloha protocol [59] as the MAC scheme of choice in the cognitive network; *ii*) multiple SUs contend for channel access using a common access probability to send broadcast messages to other SUs; *iii*) a broadcast message is not re-transmitted nor acknowledged, and *iv*) the broadcast message has a delivery final deadline $D_f$, after which the message is considered useless for purposes of the safety application in question. Each node attempts to transmit a message with a certain probability $a$ at each slot, and it will try a transmission in every slot. There will be a successful transmission if the node: i) transmits a packet; ii) the packet is successful (no one transmits in the same slot); and iii) it happens in a slot within the deadline limit $D_f$ ($D_f$ is given in terms of slots). Additionally, we assume that there are multiple hidden terminals that can interfere with the broadcasting node. Next, the channel occupancy is described, followed by the modeling approach to handle hidden terminals and the channel access policy needed to derive the optimum successful delivery probability.

### 4.2.1 Primary user channel occupancy model

We assume that the wireless channel is time-slotted and indexed by $t$ ($t = 0, 1, 2, ...$). Primary users (PUs) occupy the channel according to a two-state Markov chain model with state space {0, 1}, where state 0 indicates that the channel is occupied, while state 1 represents that the time slot is available for opportunistic use by secondary users (SUs), such an occupancy model has been used by other works, such [60] and [47]. Fig. 4.1 illustrates the state transition diagram of the Markov chain, in which $\alpha$ represents the transition probability from state 0 to state 1, and $\beta$ is the transition probability from state 1 to state 0. An SU must sense the channel at the beginning of each slot in order to verify whether the channel is available. It is assumed that there is no sensing error.

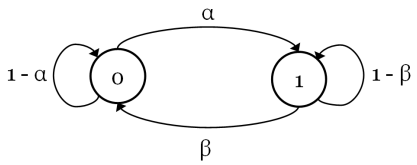



Figure 4.1: State diagram for channel occupation in a cognitive network.

The stationary probability distribution vector $\boldsymbol{\pi} = (\pi_0, \pi_1)$ for the states 0 and 1 can be found by solving the linear system $\boldsymbol{\pi} = \boldsymbol{\pi}\boldsymbol{P}$ and using the normalization condition $\pi_0 + \pi_1 = 1$, where $\boldsymbol{P}$ is one-step probability matrix of a Markov chain represented by

$$\boldsymbol{P} = \begin{bmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{bmatrix}. \tag{4.1}$$

Then, using $\boldsymbol{\pi} = \boldsymbol{\pi}\boldsymbol{P}$, we have that

$$\begin{bmatrix} \pi_0 \\ \pi_1 \end{bmatrix} = \begin{bmatrix} \pi_0 & \pi_1 \end{bmatrix} \begin{bmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{bmatrix} \tag{4.2}$$

Solving Eq. (4.2) we have

$$\pi_0 = (1-\alpha)\,\pi_0 + \beta\pi_1, \tag{4.3}$$

$$\pi_1 = \alpha\pi_0 + (1-\beta)\,\pi_1. \tag{4.4}$$

$$\pi_0 + \pi_1 = 1, \tag{4.5}$$

Now solving Eqs. (4.3, 4.4 and 4.5), it gives

$$\pi_0 = \frac{\beta}{\alpha+\beta}, \quad \pi_1 = \frac{\alpha}{\alpha+\beta}. \tag{4.6}$$

That are the stationary distribution $\boldsymbol{\pi}$ of this Markov Chain. Given $\pi_0$ and $\pi_1$, we can later compute the successful delivery probability of a broadcast message as function of the PU activity on the channel.

### 4.2.2 Network topology

In real wireless communication environments, the assumption that each node can hear every other node in the network does not hold because the transmission range is limited. For example, in Fig. 4.2, vehicles in a road are subject to the hidden terminal problem, that is, the dark gray car can simultaneously hear the transmissions from the blue and light gray cars respectively, while the blue and light gray cars cannot hear each other. Such effect can cause collision of messages at the dark gray car if both the blue and light gray cars decide to transmit concurrently.

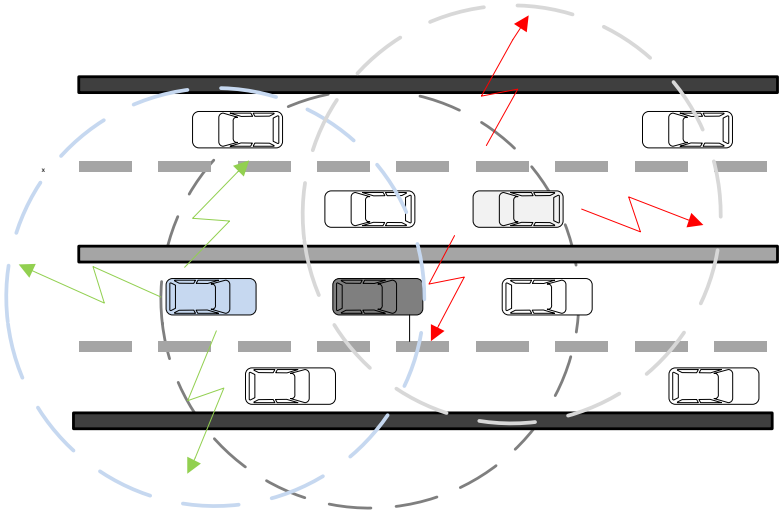


Figure 4.2: The hidden-terminal problem VANET example.

This dissertation addresses the hidden-terminal problem by considering Fig. 4.3, in which nodes are randomly located in an infinity area according to a bi-dimensional Poisson distribution with parameter $\lambda$ that expresses the average number of nodes per unity area, i.e., the probability $p(i, A)$ of finding $i$ nodes in an area of $A$ $m^2$ is given by

$$p\left(i, A\right) = \frac{(\lambda A)^i}{i!}. \tag{4.7}$$

Accordingly, the average number of nodes ($N_R$) in a circular area of radius $R$ meters is given by

$$N_R = \lambda \pi R^2 = \lambda A, \tag{4.8}$$

where $A = \pi R^2$ and $R$ represents the transmission range of the nodes. From Fig. 4.2(b), the area of the outer circular crown conceals the hidden nodes that can interfere with a broadcast transmission inside the circular area of the tagged SU broadcasting node (located in the center) initiated by the tagged SU node inside the inner circle of radius $R$. Thus the average amount of hidden terminals ($N_H$) in the crown area is obtained by

$$\begin{aligned} N_H &= 4\lambda \pi R^2 - \lambda \pi R^2 = 3\lambda \pi R^2 \\ &= 3\lambda A. \end{aligned} \tag{4.9}$$

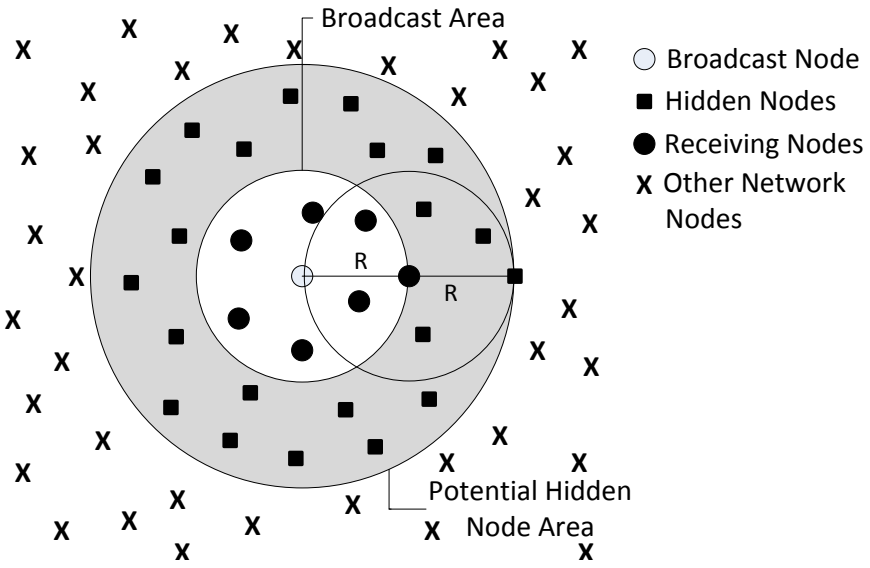



Figure 4.3: Hidden-terminal region for analysis.

### 4.2.3 Channel Access Policy

Following the work by to [16], this chapter assumes that the only source of errors in the radio channel is due to packet collisions. However, the presence of hidden terminals is also considered. As mentioned before, a common channel access probability $a$ is defined for all SUs. Consequently, if the channel is sensed not occupied by a PU at the beginning of a slot, each SU transmits (broadcasts) a packet with probability $a$. At most, each SU transmits one packet per slot, the size of a slot is assumed to be equal to the duration of a packet and all packets are assumed to be of equal size. It is assumed that each packet has a common delivery deadline $D_f$ (in units of slots), where $D_f$ is defined as the *maximum allowed* time interval from the instant a packet arrives at the head of the MAC queue to the instant it is successfully transmitted by the SU (i.e., all neighboring SUs receive the broadcast message). Let $p_s(a, D_f, \lambda)$ denote the successful delivery probability, i.e., the probability that a broadcast message is successfully transmitted before the deadline $D_f$ is reached(since its arrival at the head of the MAC queue), when each SU employs an access probability $a$, and the node density is $\lambda$. The following analysis determines the optimal access probability $a^*$ that maximizes the successful delivery probability $p_s(a, D_f, \lambda)$ under hidden terminals.

## 4.3 Optimal Access Probability

The optimal access probability for every node is obtained for two scenarios: the case $\pi_1 = 1$, i.e., the channel is unoccupied by PUs, and it is available for use by the SUs, and the case $0 < \pi_1 < 1$. As in [14], [16] this dissertation assumes that all SUs are saturated, i.e., every node has always another packet to send right after a packet is transmitted. The following analysis is performed by tagging an arbitrary SU and considering a packet in the head of its MAC queue (or head-of-line (HoL) packet), that is, the first packet to be transmitted.

### 4.3.1 Case 1: PU is not present ($\pi_1 = 1$)

Given that the packet transmission probability in a given slot is $a$, a successful transmission of a tagged HoL packet happens in the $k^{th}$ slot if the packet has not been transmitted in any of the previous $k-1$ slots, and no other node transmits in the broadcast area, as well as in the hidden-terminal area in the $k^{th}$ slot. Accordingly, the probability of successful transmission of the HoL packet since its arrival at the head of the queue is $a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}$. Therefore, the successful delivery probability $p_s(a, D_f, \lambda)$ is obtained by noting that the successful transmissions at each slot, up to the deadline $D_f$, are mutually exclusive events. Hence,

$$\begin{aligned} p_s(a, D_f, \lambda) &= \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H} \\ &= \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{\lambda A-1}(1-a)^{3\lambda A} \\ &= \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{4\lambda A-1} \\ &= (1-a)^{4\lambda A-1}\Big[1-(1-a)^{D_f}\Big]. \end{aligned} \tag{4.10}$$

The optimum access probability $a^*$ is obtained by differentiating $p_s(a, D_f, \lambda)$ in relation to $a$ and equating to zero, i.e.,

$$\begin{aligned} \frac{d}{da}p_s(a, D_f, \lambda) &= -(4\lambda A-1)(1-a)^{4\lambda A-2}\Big[1-(1-a)^{D_f}\Big] + D_f(1-a)^{4\lambda A-1}(1-a)^{D_f-1} \\ &= (1-a)^{4\lambda A-2}\Big[(1-a)^{D_f}(4\lambda A-1+D_f) - (4\lambda A-1)\Big] \\ &= 0, \end{aligned} \tag{4.11}$$

which, by solving for $a$, it follows that

$$a^* = 1 - \left(\frac{4\lambda A-1}{4\lambda A-1+D_f}\right)^{\frac{1}{D_f}}. \tag{4.12}$$

The successful delivery probability $p_s(a^*, D_f, \lambda)$ for the optimum value $a^*$ is obtained by substituting Eq. (4.12) into Eq. (4.10), resulting in

$$p_s(a^*, D_f, \lambda) = \left(\frac{4\lambda A-1}{4\lambda A-1+D_f}\right)^{\frac{4\lambda A-1}{D_f}} \frac{D_f}{4\lambda A-1+D_f}. \tag{4.13}$$

Analogous to [16], note that $a^* \to 0$ and $p_s(a^*, D_f, \lambda) \to 1$ as $D_f \to \infty$, which indicates that, the successful delivery probability $p_s(a^*, D_f, \lambda)$ tends to 1 as the allowed deadline $D_f$ increase, which follows from the fact that by waiting a sufficiently large time, it is almost sure that the tagged SU will obtain a valid slot to successfully transmit its HoL packet. The price paid is, of course, an increase in the delivery delay.

On the other hand, for the classic slotted-Aloha, in which the access probability is typically given by $a = \frac{1}{N_R+N_H} = \frac{1}{4\lambda A}$ where, $N_R + N_H = 4\lambda A$ is the amount of nodes inside the influence

range of $(2R)$ over the tagged SU node, it follows that

$$p_s\left(\frac{1}{N_R+N_H}, D_f, \lambda\right) = \left(1-\frac{1}{4\lambda A}\right)^{4\lambda A-1}\left[1-\left(1-\frac{1}{4\lambda A}\right)^{D_f}\right] \tag{4.14}$$

which is upper-bounded by $\left(1-\frac{1}{4\lambda A}\right)^{4\lambda A-1}$ when $D_f$ tends to infinity.

### 4.3.2 Case 2: PU Occupies the channel $0 < \pi_1 < 1$ :

In this case, SUs can use the network only when the PU is not present on the channel. According to our model, this happens with probability $\pi_1 \in (0,1)$. For analysis, we assume that the PU may be present on a given time slot independently of its presence in any other time slot. Moreover, because the probability of finding the PU on any time slot is the same and given by $\pi_1$ the probability of having $N$ free slots in a total of $D_f$ slots follows a binomial distribution with parameters $D_f$ and $\pi_1$ (assuming steady state). By using the law of total probability, the successful delivery probability taking into account hidden terminals given by

$$\begin{aligned}
&p_s\left(a, D_f, \lambda, A, \pi_1, \right) \\
&= \sum_{d=1}^{D_f} P\left(N=d\right) p_s\left(a, d, \lambda\right) \\
&= \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} (1-a)^{4\lambda A-1}\left[1-(1-a)^d\right] \\
&= (1-a)^{4\lambda A-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} \\
&\quad -(1-a)^{4\lambda A-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1 - a\pi_1)^d (1-\pi_1)^{D_f-d} \\
&= (1-a)^{4\lambda A-1}\left[1-(1-\pi_1)^{D_f}\right] - (1-a)^{4\lambda A-1}\left[(1-a\pi_1)^{D_f} - (1-\pi_1)^{D_f}\right] \\
&= (1-a)^{4\lambda A-1}\left[1-(1-a\pi_1)^{D_f}\right].
\end{aligned} \tag{4.15}$$

Differentiating $p_s(a, D_f, \lambda)$ with respect to $a$, and equating to zero, it results that $p_s(a, D_f, \lambda)$ is maximized at the value $a^*(D_f)$ that satisfies

$$D_f \pi_1 \left(1-a\right)\left(1-a\pi_1\right)^{D_f-1} = \left(4\lambda\pi - 1\right)\left[1-\left(1-a\pi_1\right)^{D_f}\right], \tag{4.16}$$

which can be solved numerically for $a$ (no closed-form solution).

## 4.4 Network Throughput

An important performance metric is network throughput, which is defined as the percentage of time that the slotted-Aloha channel is actually used for successful data transmission by secondary

users. The following analysis is carried out by considering the case where PUs are not present on the channel, i.e., $\pi_1 = 1$.

Since the successful delivery probability for an HoL packet for any SU is given by Eq. (4.13) for a given deadline $D_f$, then the network throughput $S$ can be obtained by adding this probability for all SU users that are within the radius range $2R$ of a given SU node, that is, the area that influences the tagged SU. The amount of nodes within an area of $2R$ is $4\lambda\pi R^2 = 4\lambda A$. Note that the maximum network throughput per slot for a given deadline $D_f$ is obtained by taking the limit of the aforementioned sum, as the number of users increases to infinity, i.e., by making $\lambda \to \infty$, normalized to the given deadline $D_f$. Consequently, from Eq. (4.13)

$$\begin{aligned}
\lim_{\lambda\to\infty} S &= \lim_{\lambda\to\infty} \frac{1}{D_f} \sum_{n=1}^{4\lambda A} p_s(a^*, D_f, \lambda) \\
&= \lim_{\lambda\to\infty} \frac{4\lambda A}{D_f} p_s(a^*, D_f, \lambda) \\
&= 4\lambda A \lim_{\lambda\to\infty} \left[ \left( \frac{4\lambda A - 1}{4\lambda A - 1 + D_f} \right)^{\frac{4\lambda A - 1}{D_f}} \frac{1}{4\lambda A - 1 + D_f} \right] \\
&= \lim_{\lambda\to\infty} \left[ \frac{1}{\left(1 + \frac{D_f}{4\lambda A - 1}\right)^{4\lambda A - 1}} \right]^{\frac{1}{D_f}} \frac{1}{1 + \frac{D_f - 1}{4\lambda A}} \\
&= \left( \frac{1}{e^{D_f}} \right)^{\frac{1}{D_f}} \\
&= \frac{1}{e}, \qquad (4.17)
\end{aligned}$$

where it was used the fact that $\lim_{x\to\infty} \left(1 + \frac{D_f}{x}\right)^x = e^{D_f}$. Therefore, the maximum network throughput, normalized to a given deadline $D_f$ is the same as the classic slotted-Aloha scheme [59], regardless of the value of $D_f$. This can be explained by the fact that each slot in the interval $[1, D_f]$ has its use disputed by an infinite amount of nodes, as in the case of the classic slotted-Aloha. On the other hand, note that

$$\begin{aligned}
\lim_{\lambda\to\infty} p_s\left(a, D_f, \lambda\right) &= \lim_{\lambda\to\infty} \left( \frac{4\lambda A - 1}{4\lambda A - 1 + D_f} \right)^{\frac{4\lambda A - 1}{D_f}} \frac{D_f}{4\lambda A - 1 + D_f} \\
&= \lim_{\lambda\to\infty} \left[ \frac{1}{\left(1 + \frac{D_f}{4\lambda A - 1}\right)^{4\lambda A - 1}} \right]^{\frac{1}{D_f}} \frac{D_f}{4\lambda A - 1 + D_f} \\
&= \frac{1}{e} \lim_{\lambda\to\infty} \frac{D_f}{4\lambda A - 1 + D_f} \\
&= 0. \qquad (4.18)
\end{aligned}$$

This means that the successful delivery probability goes to zero as the number of secondary users increases, although the maximum network throughput remains constant.

Note that the results Eq. (4.17) and Eq. (4.18) are obtained if, instead of taking $\lambda \to \infty$, one considers $R \to \infty$ (i.e., $A \to \infty$), that is, the network throughput and successful delivery probability

have limiting behavior independent of the the influence of hidden-terminals, since $N_R = \lambda A$ and $N_H = 3\lambda A$,

## 4.5 Numerical Results

In the following section, we carry out a performance analysis considering the transmission range $R = 1$ km, as proposed by the IEEE 802.11p [13]. Accordingly, $\lambda$ is shown in units of $nodes/km^2$. Fig. 4.4 illustrates the successful delivery probability $p_s$ as a function of $D_f$ for the case when PU is not present on the channel, following Bae [16] the number of nodes in the system are 10. The figure depicts the case when $N_R = \lambda A = 10$, which implies $N_H = 3\lambda A = 30$. Additionally, the figure contains a comparison with the case when there are no hidden terminals ($N_H = 0$, as treated in [16]). In addition, the behavior of the classic slotted-Aloha with and without hidden terminals is shown for comparison purposes, in which $a = \frac{1}{N_R+N_H} = \frac{1}{40}$, where $N_R + N_H$ is the amount of nodes inside the influence range ($2R$) of the tagged SU node. The curves show that the successful delivery probability is degraded considerably under the presence of hidden terminals, for a final deadline of $D_f = 100$ slots, there are a performance decay of 28.1% between the optimal cases, with and without the presence of hidden terminals, and of 15.2% in the value of a final deadline of $D_f = 500$ in both cases, if the final deadline $D_f$, for the transmission of the message, it is increase, there will be a bigger probability of success of delivery successfully the message to all receiver nodes, it indicates the deadline increases, $p_s$ tends to 1 as expected. On the other hand, the classic slotted-Aloha increases up to $\left(1 - \frac{1}{N_R+N_H}\right)^{N_R+N_H-1}$ with hidden terminals, and up to $\left(1 - \frac{1}{N_R}\right)^{N_R-1}$ for the case of no hidden terminals, when $D_f$ goes to infinity.

Fig. 4.5, illustrates the successful delivery probability for the case when the PU is present on the channel. In particular, we present some curves for different values of $\pi_1$ as the node density parameter $\lambda$ increase. The curves show that $p_s$ decreases with an increase of density of nodes, in the case of $\pi_1 = 0.5$ there is a loss of 30% with values of $\lambda$ of 10 and 40 which represents, following the relation $M = N_R + N_H = 4\lambda\pi R$, approximately 125 and 500 nodes. Also, $p_s$ decreases with a reduction in $\pi_1$, which is expected, since an increase in the percentage of time in the primary user is present on the channel leads to a decrease in the number of free slots for secondary users, for $\lambda = 10$ there is a loss of 33% in the probability of success $p_s$ between $\pi_1 = 1$ and $\pi_1 = 0.2$. Fig. 4.5 shows the impact of the percentage of the occupancy of the channel related to the final deadline $D_f$, where for $D_f = 500$ there are a gain of 19%, 29% and 35% for the cases of $\pi_1 = 0.5$, $\pi_1 = 0.8$ $\pi_1 = 1$ with respect to $\pi_1 = 0.2$ respectively.

## 4.6 Conclusions

This chapter considered the derivation of the optimal access probability $a$ for the successful delivery probability $p_s$ of a broadcast message under slotted-Aloha in a cognitive radio network with final deadline $D_f$ and hidden terminals. A Poisson bi-dimensional node distribution was proposed in order to carry out the analysis and the successful delivery probability was found to

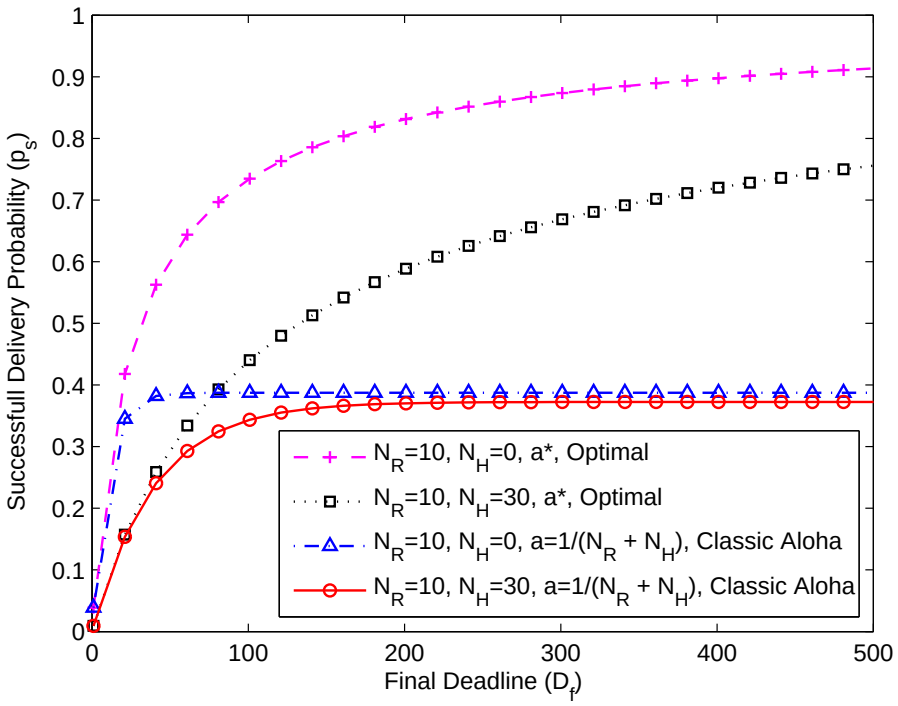



Figure 4.4: Successful delivery probability as a function of $D_f$, for $\pi_1 = 1$, i.e., when PUs are not present on the channel.

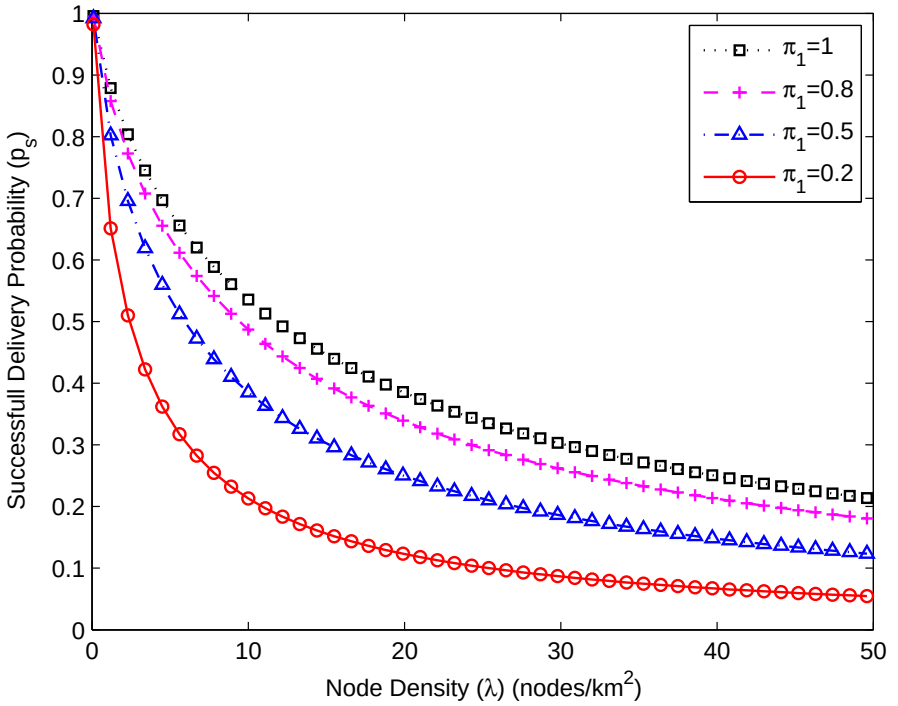



Figure 4.5: Successful delivery probability as a function of number of users with $D_f = 500$, for different values of $\pi_1$, considering the presence of hidden-terminals.

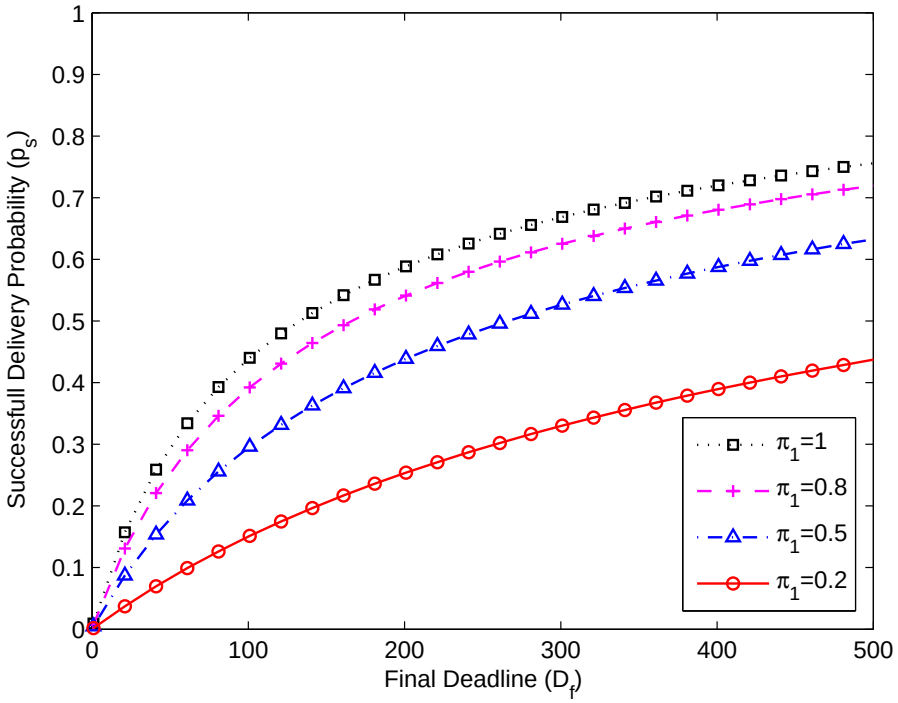



Figure 4.6: Successful delivery probability as a function of $D_f$, for different value of $\pi_1$, i.e., PUs are present on the channel and $\lambda = 10\ nodes/km^2$.

be substantially degraded by the presence of hidden terminals. In addition, successful delivery probability goes to zero with the increase of the number of secondary users, while another very important network performance measure, the limiting maximum network throughput, it was found to be a constant equal to $\frac{1}{e}$ as in the case of the classic slotted-Aloha scheme, independent of the value of the message deadline.

As we can see, this method of transmitting the message once, using the optimized access probability, improve the performance of the system, but it does not guarantee a probability of success $p_s > 99.9\%$. In the next chapters new methods for improving the probability of success, using periodic broadcast will be presented.

# Chapter 5

# Periodic Broadcast

## 5.1 Introduction

When a message is generated at the transmitter node, it must be delivered to all neighbors within a given strict deadline in order to accomplish its safety purpose. As a means to increase reliability and to improve the probability of successful delivery of safety messages, some works have proposed the use of repetitive broadcast, which means the repetitive transmission of a given broadcast message. Repetitive broadcast of safety messages in VANETs was first proposed in [51] and [61]. This technique has shown to provide an improvement in system performance. Such technique is not employed by IEEE 802.11p standard [13]. In that case safety messages are transmitted only once during a time frame, and the broadcast message is not re-transmitted nor acknowledged. In this chapter we develop our proposal to repeat the broadcast message in order to improve the probability of success $p_s$ and evaluate the possibility of get values of $p_s$ greater or equal than 99.9% within a deadline of 100 ms. The next sections will present the system model and the mathematical development. Finally, numerical results are presented with some conclusions at the end of the chapter.

## 5.2 Proposed Model

For our analysis we employ a variation of the synchronous p-persistent repetition SRP scheme, in which the transmitter node transmits the message in each time-slot with probability $a$. For our proposal we define two basic parameters, the Final Deadline $D_f$ and the Partial Deadlines $D_p$ as:

- $D_p$: It is the partial deadline. It defines the period of slots in which a broadcast message is going to be repeated.
- $D_f$: It is the final deadline, beyond which it is useless to send the safety message.

Therefore, there is a Final Deadline $D_f$ for the successful transmission of the safety message and in addition the message is re-transmitted during partial deadlines $D_p$ to ensure that all nodes receive

the message, as it can be seen in Fig. 5.1. Accordingly, there are $N = \frac{D_f}{D_p}$ transmission attempts, which characterize a periodic broadcast approach. In each $D_p$ there is only one transmission attempt. The transmitter node decides to transmit in a given slot with an access probability $a$. Once it is transmitted, it does not transmit anymore inside the time frame defined by a $D_p$. This transmission may or may not happen, depending on $a$. Once another time frame of $D_p$ size starts, another round of attempts initiates.

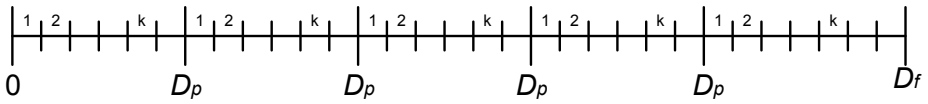



Figure 5.1: Slots diagram for broadcast message re-transmission.

In the next section it is developed the mathematical model for the case in which the message is sent once, i.e., $D_f$ is equal to $D_p$, as it was done in previous chapter, but now the term probability of failure $p_f$ is going to be incorporated in our analysis to indicate the probability of channel or reception failures.

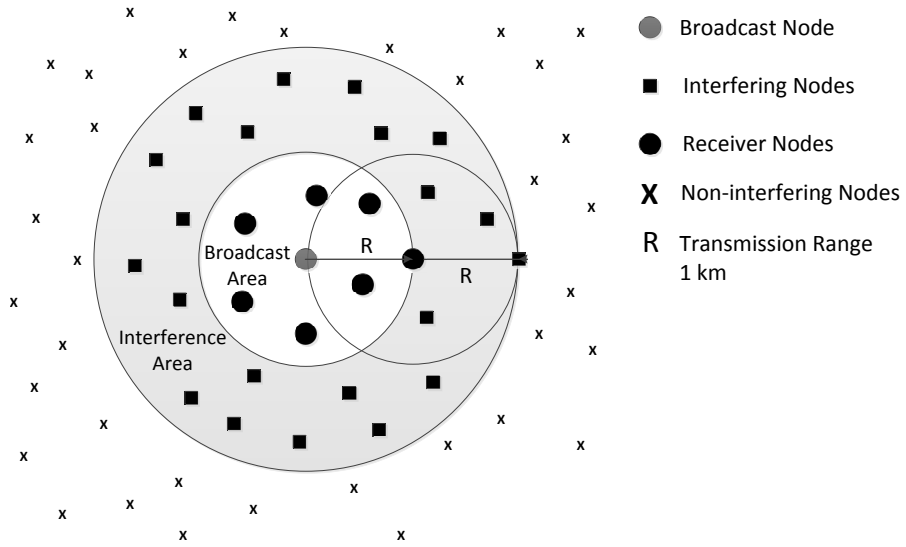



Figure 5.2: System model for analysis of periodic broadcast.

Fig. 5.2 depicts the network model used for the analysis. There are two main areas: the broadcast area, where it is located all nodes that should receive the broadcast message sent by the node in the center, and the interference area, where it is located all nodes that are hidden from the center node and may cause packet collisions.

## 5.3 The case $D_f = D_p$ with probability of failure $p_f$

In this section, we compute the optimal access probability, as well, as the successful delivery probability for the case $D_f = D_p$, taking into account the effect of hidden terminals and the probability $p_f$ of failed reception (due to channel errors). Following previous chapter, two cases are considered separately: the case $\pi_1 = 1$, i.e., the channel is unoccupied by PUs and it is

always available for use by the SUs, and the case $0 < \pi_1 < 1$. Similar to previous chapter, it is assumed that all SUs are saturated, and the analysis is performed by tagging an arbitrary SU and considering a packet in the head of the MAC queue (or head-of-line (HoL) packet), that is, the first packet to be transmitted. Note that, as $D_f = D_p$, there is only a single transmission of the message for the whole $D_f$.

### 5.3.1 Case 1: PU is not present in the channel ($\pi_1 = 1$)

Following previous analysis, the access probability (or probability of transmitting a packet in a given time slot) is $a$. A successful transmission of a tagged HoL packet happens in the $k^{th}$ slot if the packet has not been transmitted in any of the previous $k-1$ slots, and no other node transmits in the broadcast area as well as in the interference area in the $k^{th}$ slot. Therefore, if all events are assumed to be independent of each other, the probability of successful transmission of the HoL packet since its arrival at the head of the queue is $a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}(1-p_f)^{N_R-1}$, where $(1-a)^{N_R-1}$ means that only the transmitter node transmit inside his coverage area, $(1-a)^{N_H}$ implies that none of the nodes inside the hidden terminal area transmit, and $(1-p_f)^{N_R-1}$ means that all neighboring nodes received the broadcast message without errors. We define $M$ to be the total number of nodes in the system, i.e., $M = N_H + N_R$ and $D_f$ is the final deadline for the successful transmission. Therefore, the successful delivery probability $p_s(a, D_f, N_R, N_H, p_f)$ is obtained by noting that the successful transmission at each slot, up to the deadline $D_f$, are mutually exclusive events. By using again the law of total probability, we have that

$$p_s(a, D_f, N_R, N_H, p_f) = \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}\left(1-p_f\right)^{N_R-1}.$$

Defining $M = N_R + N_H$, Eq. (5.1) simplifies to

$$\begin{aligned} p_s(a, D_f, M, N_R, p_f) &= \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{M-1}\left(1-p_f\right)^{N_R-1} \\ &= (1-a)^{M-1}\left[1-(1-a)^{D_f}\right]\left(1-p_f\right)^{N_R-1}. \end{aligned} \tag{5.1}$$

Similar to previous chapter, we are interested in finding out the optimal value for the access probability $a$, i.e., the one that maximizes $p_s$. If we plot the values of $p_s$ for different values of $a$, we can note that there is a value of $a \in [0,1]$ that maximizes $p_s$ as it is shown in Fig. 5.3.

In fact, the value of the optimal access probability $a^*$ can be obtained by differentiating $p_s(a, D_p, M, N_R, p_f)$ with respect to $a$ and equating it to zero, i.e.,

$$\begin{aligned} \frac{d}{da}p_s(a, D_f, M, N_R, p_f) &= \left(1-p_f\right)^{N_R-1}\Big[-(M-1)(1-a)^{M-2}\Big[1-(1-a)^{D_p}\Big] \\ &\quad +D_p(1-a)^{M-1}(1-a)^{D_p-1}\Big] \\ &= \left(1-p_f\right)^{N_R-1}(1-a)^{M-2}\Big[(1-a)^{D_p}(M-1+D_p)-(M-1)\Big] \\ &= 0, \end{aligned} \tag{5.2}$$

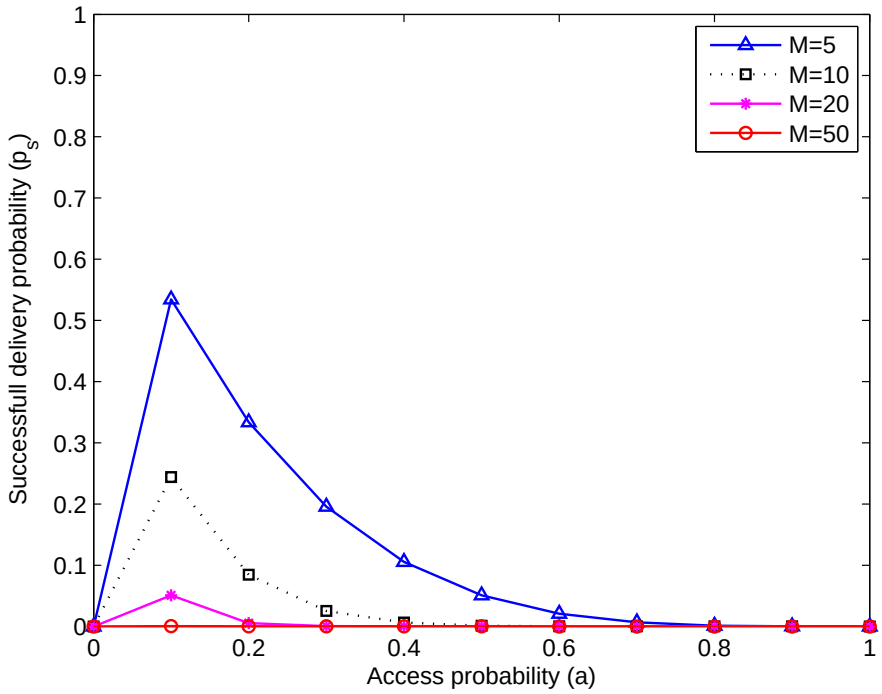



Figure 5.3: Successful delivery probability $p_s$ as a function of $a$, for $\pi_1 = 1$, $D_f = D_p = 500$ and $p_f = 0.1$.

which, by solving for $a$, it follows that

$$a^* = 1 - \left(\frac{M-1}{M-1+D_f}\right)^{\frac{1}{D_f}}. \tag{5.3}$$

It is possible to note that Eq. (5.3) does not depend on $p_f$ similarly to Eq. (4.12) in previous chapter. The successful delivery probability for the optimum value $a^*$ is obtained by substituting Eq. (5.3) into Eq. (5.1), resulting in

$$p_s(a^*, D_f, N_R, M, p_f) = \left(\frac{M-1}{M-1+D_f}\right)^{\frac{M-1}{D_f}} \frac{D_f}{M-1+D_f} (1-p_f)^{N_R-1}. \tag{5.4}$$

In this case, similar to previous chapter, note that $a^* \to 0$ and $p_s(a^*, D_f, M, N_R, p_f) \to 1$ as $D_f \to \infty$, which indicates that the successful delivery probability tends to 1 with an increase of $D_f$.

### 5.3.2 Case 2: PU is present in the channel $(0 < \pi_1 < 1)$

In this case, SUs can only use the channel when the PU is not present, which happens with probability $\pi_1 \in [0, 1]$ in any given slot. Analogous to Chapter 4, we observe that, in steady state, the number $N_f$ of free slots within $D_f$ follows a binomial distribution with parameters $D_f$ and $\pi_1$. Using the law of total probability, the successful delivery probability when interfering nodes are

present and packet errors may happen with probability of failure $p_f$ is given by

$$
\begin{aligned}
& p_s\left(a, D_f, M, N_R, p_f\right) \\
&= \sum_{d=1}^{D_f} P\left(N_f = d\right) p_s\left(a, d, M\right)\left(1-p_f\right)^{N_R-1} \\
&= \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} (1-a)^{M-1}\left[1-(1-a)^d\right]\left(1-p_f\right)^{N_R-1} \\
&= (1-a)^{M-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} \\
&\quad -(1-a)^{M-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1 - a\pi_1)^d (1-\pi_1)^{D_f-d}\left(1-p_f\right)^{N_R-1} \\
&= (1-a)^{M-1}\left[1-(1-\pi_1)^{D_f}\right] - (1-a)^{M-1}\left[(1-a\pi_1)^{D_f} - (1-\pi_1)^{D_f}\right]\left(1-p_f\right)^{N_R-1} \\
&= (1-a)^{M-1}\left[1-(1-a\pi_1)^{D_f}\right]\left(1-p_f\right)^{N_R-1}. \qquad (5.5)
\end{aligned}
$$

By differentiating Eq. (5.5) with respect to $a$ and equating it to zero, results that $p_s(a, D_f, M, N_R, p_f)$ is maximized at the value $a^*(D_f)$ that satisfies

$$
D_p \pi_1 (1-a)(1-a\pi_1)^{D_f-1} = (M-1)\left[1-(1-a\pi_1)^{D_f}\right], \qquad (5.6)
$$

which can be solved numerically for $a$.

### 5.3.3 Numerical Results

Fig. 5.4 shows the probability of success delivery $p_s$ versus the final deadline $D_f$, assuming $p_f = 0.05$. We observe how the system performance drops significantly comparing with Fig. 4.4, in previous chapter, due to the term $(1-p_f)^{N_R-1}$ in Eq. (5.4). There is a drop of 28.3% in the value of the successful delivery probability $p_s$ in all cases comparing with Fig. 4.4. Also, in Fig. 5.5 it can be seen that with the increase of the value of probability of failure $p_f$ the probability of success $p_s$ is severally affected. Possible collisions from hidden terminal nodes ($N_H$) and probability of failure ($p_f$) can happen in the receiver. The probability of success in delivering the message is only about 0.05 for $D_f = 500$ which represent a poor performance of $p_s$ that severally affect the reliability of the system. In this chapter, the value of $p_f$ is assumed to have a given value, however, in the next chapter $p_f$ will be computed for a typical VANET fading channel.

Fig. 5.6, illustrates the successful delivery probability as function of the number of nodes in the system. In this case there are primary users PUs in the system, and the figure show the performance of $p_s$ for different values of $\pi_1$. The curves show that $p_s$ decreases with an increase in the number of users. Also, $p_s$ decreases with the reduction of $\pi_1$, that is, once the presence of primary users in the channel increases, the number of free slots decreases.

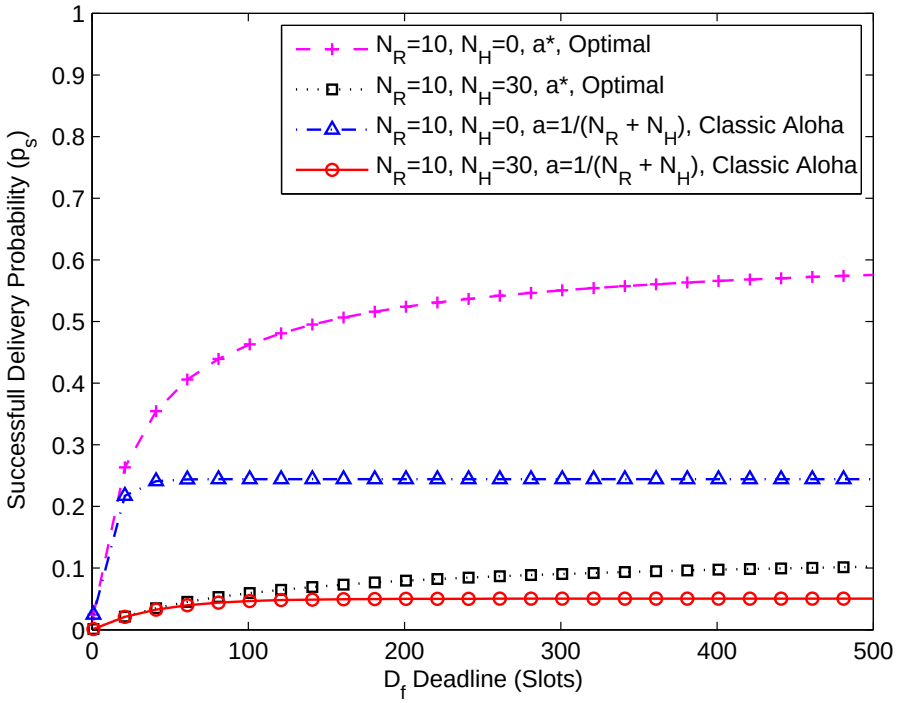



Figure 5.4: Successful delivery probability as a function of $D_f$, for $p_f = 0.05$ and $\pi_1 = 1$, i.e., channel unoccupied by primary users.

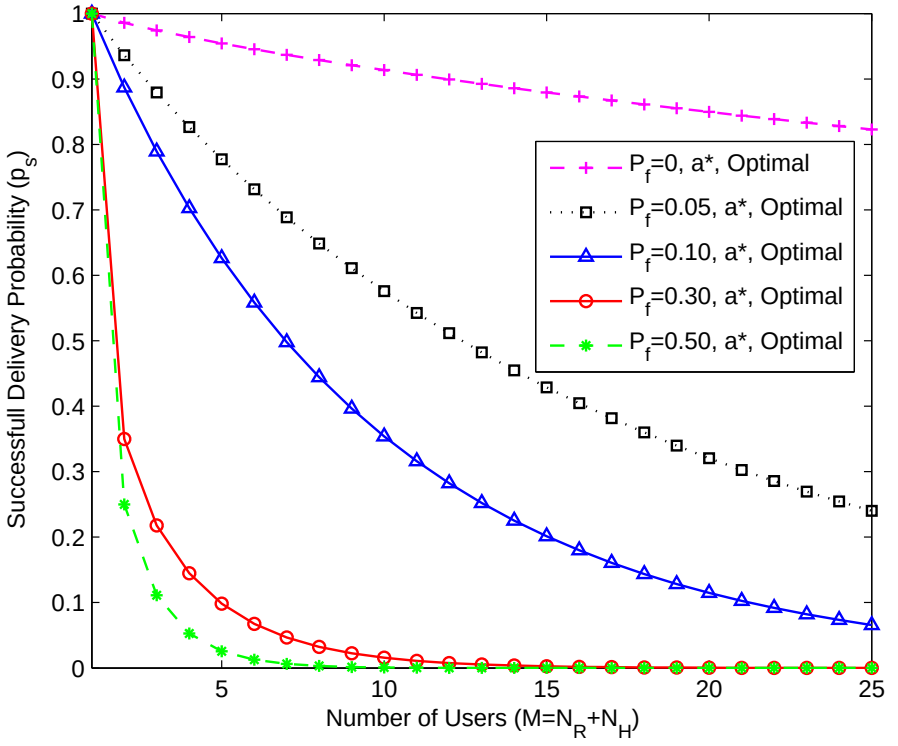



Figure 5.5: Successful delivery probability as a function of number of users $M = N_R + N_H$, varying $p_f$ and for $\pi_1 = 1$, i.e., channel unoccupied by primary users.

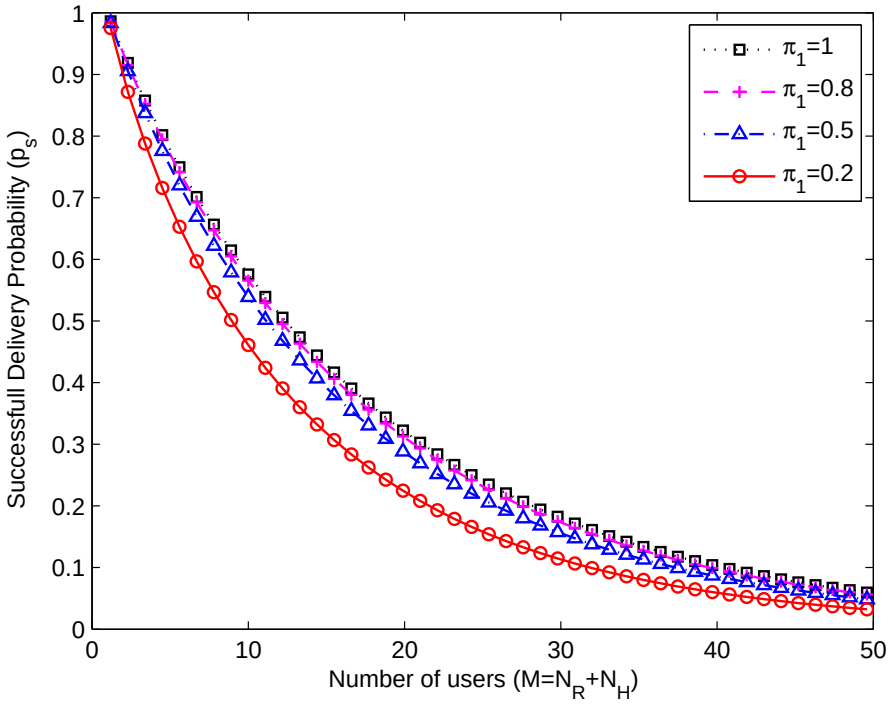



Figure 5.6: Successful delivery probability as a function of $M$, probability of failure $p_f = 0.05$ and diffent values of $\pi_1$, i.e., channel occupied by primary users.

## 5.4 The case $D_f > D_p$: All nodes receive the message at the same $D_p$ following a Geometric distribuion

This case models the periodic broadcast, i.e., the broadcast safety message will be re-transmitted several times to increase the probability of success $p_s$. As in previous chapter there is a final deadline $D_f$ to transmit the message, and it is divided in partial deadlines $D_p$. $D_f$ is a multiple number of $D_p$, and each $D_p$ consist of a certain number of slots. At each $D_p$, a node attempts to transmit the broadcast message. It only generates another one in the following time frame of size $D_p$. A broadcast message is considered successful only if all neighboring nodes receive the message within $D_f$. In each time frame of size $D_p$, a node transmit a broadcast message only once (determined by the access probability $a$ and availability of channel $\pi_1$). For modeling message re-transmission, in which all nodes must receive successfully the message, it will be used the Geometric Distribution that represents the probability of the first occurrence of success in $x$ number of independent trials, each with success probability $p_s$ where $1 < x < \frac{D_f}{D_p}$. If the probability of success on each trial period $D_p$ is $p_s$, then the probability that the $x^{th}$ trial is the first success is

$$P_r(X = x) = (1 - p_s)^{x-1} p_s. \tag{5.7}$$

In this case the message must be received for all nodes in one $D_p$, if one node does not receive the message, the transmission is considered failed. Finally, a failure packet reception probability $p_f$ is also considered. In the next section it is obtained the optimal access probability for the same

two scenarios: the case $\pi_1 = 1$, i.e., the channel is unoccupied by PUs and it is available for use by the SUs, and the case $0 < \pi_1 < 1$, i.e., there are primary users in the system.

### 5.4.1 Case 1: PU is not present on the channel ($\pi_1 = 1$)

For this section it will be used the result obtained in Section 5.3, for the probability of success in one period $Dp$, i.e.,

$$\begin{aligned} p_s(a, D_p, M, N_R, p_f) &= \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1}\left(1-p_f\right)^{N_R-1} \\ &= (1-a)^{M-1}\left[1-(1-a)^{D_p}\right]\left(1-p_f\right)^{N_R-1}. \end{aligned} \tag{5.8}$$

Now, that we have the probability of success in one partial deadline $D_p$ in Eq. (5.8), the message will be re-transmitted in others $D_p s$, according to the geometric distribution given in Eq. (5.8). The probability of success up to $\frac{D_f}{D_p}$ periodic broadcasting is obtained by

$$\begin{aligned} p_s(a, D_f, D_p, M, N_R, p_f) \;=\; & \sum_{x=1}^{Df/Dp}\left(1-\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}\left(1-p_f\right)^{N_R-1}\right)^{x-1} \\ & \left(\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}\left(1-p_f\right)^{N_R-1}\right), \end{aligned} \tag{5.9}$$

in which $\frac{D_f}{D_p}$ is assumed to be an integer. As $M = N_R + N_H$, Eq. (5.9) is rewritten by

$$\begin{aligned} p_s(a, D_f, D_p, M, N_R, p_f) \;=\; & \sum_{x=1}^{Df/Dp}\left(1-\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1}\left(1-p_f\right)^{N_R-1}\right)^{x-1} \times \\ & \left(\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1}\left(1-p_f\right)^{N_R-1}\right). \end{aligned} \tag{5.10}$$

Define $y$ as

$$\begin{aligned} y \;&=\; \left(\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1}\left(1-p_f\right)^{N_R-1}\right) \\ &=\; \left((1-a)^{M-1}\left[1-(1-a)^{D_p}\right]\left(1-p_f\right)^{N_R-1}\right). \end{aligned} \tag{5.11}$$

By replacing Eq. (5.11) into Eq. (5.10) we obtain

$$\begin{aligned} p_s(a, D_f, D_p, M, N_R, p_f) \;&=\; \sum_{x=1}^{Df/Dp}(1-y)^{x-1}\, y \\ &=\; y\sum_{x=1}^{Df/Dp}(1-y)^{x-1}. \end{aligned} \tag{5.12}$$

Since $y \in \{0,1\}$, we have that

$$\sum_{x=1}^{Df/Dp} (1-y)^{x-1} = \frac{1-(1-y)^{\frac{D_f}{D_p}}}{y}. \tag{5.13}$$

By replacing the result of Eq. (5.13) into Eq. (5.12) we obtain that

$$p_s(y, D_f, D_p) = 1 - (1-y)^{\frac{D_f}{D_p}}. \tag{5.14}$$

Now, using Eq. (5.14) into Eq. (5.11) we finally obtain that

$$p_s(a, D_f, D_p, M, N_R, p_f) = 1 - \left[1 - \left(1-(1-a)^{D_p}\right)(1-a)^{M-1}(1-p_f)^{N_R-1}\right]^{\frac{D_f}{D_p}}. \tag{5.15}$$

By defining $N = \frac{D_f}{D_p}$ we can write Eq. (5.15) as

$$p_s(a, N, M, N_R, p_f) = 1 - \left[1 - \left(1-(1-a)^{D_p}\right)(1-a)^{M-1}(1-p_f)^{N_R-1}\right]^{N}. \tag{5.16}$$

The optimum access probability $a^*$ is obtained by differentiating Eq. (5.16) with respect to $a$ and equating it to zero, i.e.,

$$\begin{aligned} \frac{d}{da}p_s(a, N, M, N_R, p_f) &= \frac{d}{da}\left(1 - \left[1 - \left(1-(1-a)^{D_p}\right)(1-a)^{M-1}(1-p_f)^{N_R-1}\right]^{N}\right) \\ &= 0, \end{aligned} \tag{5.17}$$

Appendix A1 contains the procedure to differentiate Eq. (5.17) with respect to $a$. The resulting expression is given by

$$\begin{aligned} &\frac{d}{da}p_s(a, N, M, N_R, p_f) \\ &= -\left(N(1-p_f)^{N_R-1}\left((M-1)\left(-\left((1-a)^{D_p}-1\right)\right)(1-a)^{M-2} - D_p(1-a)^{D_p+M-2}\right)\right. \\ &\quad \left.\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\right). \end{aligned} \tag{5.18}$$

Simplifying Eq. (5.18) the obtained expression is

$$\begin{aligned} &\frac{d}{da}p_s(a, N, M, N_R, p_f) \\ &= N(1-p_f)^{N_R-1}\left((M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2} + D_p(1-a)^{D_p+M-2}\right) \\ &\quad \left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}. \end{aligned} \tag{5.19}$$

By equating to zero Eq. (5.19), the value of $a$ that maximizes $p_s(a, D_f, D_p, M, N_R, p_f)$ can be obtained numerically, i.e.,

$$\begin{aligned} 0 &= N(1-p_f)^{N_R-1}\left((M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2} + D_p(1-a)^{D_p+M-2}\right) \\ &\quad \left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}. \end{aligned} \tag{5.20}$$

### 5.4.2 Case 2: PU is present in the channel ($0 < \pi_1 < 1$)

In this case, SUs can use the channel with probability $\pi_1 \in (0,1)$ at each slot, independently of each other. By observing that, in steady state, the number $N_f$ of free slots within $D_f$ follows a binomial distribution with parameters $D_p$ and $\pi_1$, and using the law of total probability, the successful delivery probability with hidden terminals is given by

$$\begin{aligned} & p_s\left(a, D_f, D_p, M, N_R, p_f\right) \\ & = \sum_{x=1}^{Df/Dp} \left(1 - \sum_{d=1}^{D_p} P\left(N_f = d\right) p_s\left(a, d, M\right) \left(1-p_f\right)^{N_R-1}\right)^{x-1} \times \\ & \left(\sum_{d=1}^{D_p} P\left(N = d\right) p_s\left(a, d, M\right) \left(1-p_f\right)^{N_R-1}\right). \end{aligned} \tag{5.21}$$

Using the expression for $p_s$ obtained in Eq. (5.5) it gives

$$\begin{aligned} & = \sum_{x=1}^{Df/Dp} \left(1 - (1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\left(1-p_f\right)^{N_R-1}\right)^{x-1} \times \\ & \left((1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\left(1-p_f\right)^{N_R-1}\right). \end{aligned}$$

Defining $y$ as

$$y = (1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\left(1-p_f\right)^{N_R-1}, \tag{5.22}$$

and replacing Eq. (5.22) into Eq. (5.22) we obtain

$$\begin{aligned} p_s(y, D_f, D_p, m) &= \sum_{x=1}^{Df/Dp} (1-y)^{x-1}\, y \\ &= y \sum_{x=1}^{Df/Dp} (1-y)^{x-1}. \end{aligned} \tag{5.23}$$

As before,

$$p_s(y, D_f, D_p) = 1 - (1-y)^{\frac{D_f}{D_p}}. \tag{5.24}$$

If we substitute Eq. (5.24) into Eq. (5.22) we obtain

$$p_s(a, D_f, D_p, M, N_R, p_f) = 1 - \left[1 - \left((1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\left(1-p_f\right)^{N_R-1}\right)\right]^{\frac{D_f}{D_p}}. \tag{5.25}$$

By defining $N = \frac{D_f}{D_p}$, we can write Eq. (5.25) as

$$p_s(a, D_f, D_p, M, N_R, p_f) = 1 - \left[1 - \left((1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\left(1-p_f\right)^{N_R-1}\right)\right]^{N}. \tag{5.26}$$

Appendix A2 contains the details for evaluation of the derivative of $p_s$ with respect to $a$. The final expression is given by

$$\begin{aligned}\frac{d}{da}p_s(a, D_f, D_p, M, N_R, p_f) \;=\; & -N\left[(M-1)(1-a)^{M-2}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right. \\ & \left.-D_p\pi_1(1-a)^{M-1}(1-p_f)^{N_R-1}(1-a\pi_1)^{D_p-1}\right] \\ & \left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}. \quad (5.27)\end{aligned}$$

The value of the access probability $a$ that maximizes $p_s$ is obtained by equating Eq. (5.27) to zero, as follows

$$\begin{aligned}0 \;=\; & -N\left[(M-1)(1-a)^{M-2}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right. \\ & \left.-D_p\pi_1(1-a)^{M-1}(1-p_f)^{N_R-1}(1-a\pi_1)^{D_p-1}\right] \\ & \left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}, \quad (5.28)\end{aligned}$$

which can be solved numerically.

## 5.5 The case $D_f > D_p$: All nodes not necessary receive the message at the same time $D_p$ following multinomial coefficients

In previous section, it is assumed that for a successful delivery of a broadcast message to happen, it is required that all neighboring nodes received the message at a given attempt. In reality, not all nodes need to receive the message at the same period $D_p$. In the first attempt of the transmission, some nodes can receive the message, in the second attempt, other ones may receive it and so on, until the message reaches all the nodes of interest in all attempts until the final deadline $D_f$.

Now, we need to count all possible cases for successful delivery of the message to $n$ nodes after a given number of $k$ period of $D_p$ slots. This is an special combinatorial problem, that can be stated in terms of distributing balls into boxes. In our case, the balls and boxes are distinguishable. The term 'distinguishable' refers to the fact that the nodes, or slots, are marked in some way or have some feature about them that makes each one distinguishable from the others. For example, they may be numbered, each with a different number, they may each have a different color, or they may each have a different size or shape. For our analysis, the terms balls and boxes are replaced by nodes and period of $D_p$ slots, respectively. Our problem is how to distribute $n$ distinguishable nodes in $D_p$ distinguishable period of slots. For the purpose of our discussion, when we speak of $n$ distinguishable nodes, we assume that they are numbered with consecutive integers $i$ through $n$, and when we speak of $k$ distinguishable period of slots $D_p$, we assume that they are numbered with consecutive integers $i$ through $k$. This problem is considered without exclusion, which means, that in a given slot more than one node can receive the message.

Table. 5.1 contains an example, in which we have only two neighbors and three slots, in which, the transmitter transmits the broadcast message. In this case there are 2 receiver nodes labeled $a$ and $b$ respectively, and $N = \frac{D_f}{D_p} = 3$ periods of $D_p$ slots $(1, 2, 3)$, indicating all the possible

cases to distribute 2 labeled nodes in 3 labeled $D_p$. In Appendix A.3 there are other examples in which Table A.1 shows the distribution of 3 nodes $a, b, c$ in 3 $D_p$ $(1, 2, 3)$, and Table A.2 shows the distribution of the same 3 nodes $(a, b, c)$ but for the case of 4 periods of $D_p$ slots $(1, 2, 3, 4)$.

Table 5.1: Possible combinations in which two labeled nodes $(a, b)$ can receive the message in three period of $D_p$ slots $(1, 2, 3)$.

| | **Slots** | | |
|---|---|---|---|
| **Attempts** | **1** | **2** | **3** |
| **1** | a,b | 0 | 0 |
| **2** | 0 | a,b | 0 |
| **3** | 0 | 0 | a,b |
| **4** | a | b | 0 |
| **5** | a | 0 | b |
| **6** | b | a | 0 |
| **7** | b | 0 | a |
| **8** | 0 | a | b |
| **9** | 0 | b | a |

Distributing $n$ distinguishable nodes into $k$ distinguishable periods of $D_p$ slots, without exclusion, corresponds to forming a permutation of size $n$, with unrestricted repetitions, taken from a set of size $k$. Therefore, there are $k^n$ different ways to distribute $k$ distinguishable periods of $D_p$ slots into $n$ distinguishable nodes, without exclusion. Applying this rule to the example of distributing two nodes in three periods of $D_p$ slots (Table. 5.1) there are 9 possible ways of doing that.

The multinomial coefficients have a direct combinatorial interpretation, as the number of ordered arrangements of $n$ objects, in which there are $n_1$ objects of type 1, $n_2$ objects of type 2,..., and $n_k$ objects of type $k$ where $n_1 + n_2 + ... + n_k = n$, depositing the $n$ distinct objects into $k$ distinct bins, with $n_1$ objects in the first bin, $n_2$ objects in the second bin, and so on. We are specially interested in describe all the possible cases, and to represent them, we use the multinomial coefficient

$$\binom{n}{n_1, n_2, ..., n_k} = \frac{n!}{n_1! n_2! ... n_k!}. \tag{5.29}$$

To express all the possible permutations we compute Eq. (5.29) as

$$\sum_{n_1+n_2+...+n_k} \binom{n}{n_1, n_2, ..., n_k} = \sum_{n_1+n_2+...+n_k} \frac{n!}{n_1! n_2! ... n_k!}. \tag{5.30}$$

The sum is taken over all combinations of non negative integer indices $n_1$ through $n_k$, such the sum of all $n_i$ is $n$ which gives immediately that

$$\sum_{n_n+n_2+...+n_k=n} \binom{n}{n_1, n_2, ..., n_k} = \sum_{n_1+n_2+...+n_k=n} \frac{n!}{n_1! n_2! ... n_k!} = k^n. \tag{5.31}$$

Using Eq. (5.31) we can study all possible cases in which $n$ distinguishable nodes are distributed into $k$ distinguishable periods of $D_p$ slots. Hence, it is possible to build a matrix with all possible cases in which the message is successfully received by neighbors, as presented in Table 5.2, where rows indicate all the possible ways to distribute $n$ distinguishable nodes are distributed into $k$ distinguishable periods of $D_p$ slots and columns indicate the period of $D_p$ slots in which the message is (or not) successfully received, and the elements $n_{i,j}$ indicate the number of labeled nodes that successfully received the broadcast message at the slot.

Table 5.2: List of possible combinations in which $n$ labeled nodes can receive the message in $k$ slots.

| | **Slots** $D_p s$ | | | |
|---|---|---|---|---|
| | $k_1$ | $k_2$ | .... | $k_j$ |
| $n_1$ | $n_{1,1}$ | $n_{1,2}$ | .... | $n_{1,j}$ |
| $n_2$ | $n_{2,1}$ | $n_{2,2}$ | .... | $n_{2,j}$ |
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |
| $n_i$ | $a_{i,1}$ | $n_{i,2}$ | .... | $n_{i,j}$ |

In the next section we present the derivation of the successful delivery probability for the case when it is relaxed the assumption that all nodes need to receive the broadcast message in the same partial deadline $D_p$. We do so by analyzing the tools just described.

### 5.5.1 Case 1: PU is not present in the channel ($\pi_1 = 1$)

In this section it will be modeled the probability of success $p_s$ using the multinomial coefficient approach presented in the previous section. It is important to note that in this case there are slots, time periods of $D_p$ slots and, a set of $N$ time periods of $D_p$ slots, equal to $D_f$. Given that the packet access probability in a given slot is $a$, a successful transmission of a tagged HoL packet happens in the $k^{th}$ slot if the packet is not transmitted in any of the previous $k-1$ slots, and no other node transmits in the broadcast area as well as in the hidden-terminal area in the $k^{th}$ slot. The quantity of $N = \frac{D_f}{D_p}$ defines the number of attempts to transmit the message and the probability of reception failure for each node is $p_f$. As we see in previous section, we must study all possible cases in which all the nodes receive the broadcast message in a period of $D_p$ slots, to do that, we evaluate all the elements $n_{i,j}$ as in matrix $A$, similarly to Table 5.2,

$$A = \begin{pmatrix} n_{1,1} & n_{1,2} & ... & n_{1,j} \\ n_{2,1} & n_{2,2} & ... & n_{2,j} \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ n_{i,1} & n_{i,2} & ... & n_{i,j} \end{pmatrix}. \tag{5.32}$$

Then we develop the expression to evaluate the possible cases inside $A$, related to the probability of failure $p_f$, i.e.,

$$\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right], \tag{5.33}$$

where the term $(1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}}$ means that, in that specific period of $D_p$ slots, just the nodes $n_{i,j}$ successfully received the message, while the others $N_R - 1 - n_{i,j}$ did not.

Accordingly, the probability of successful transmission of the HoL packet since its arrival at the head of the queue is $a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}$ as in previous sections, and incorporating the term (5.33) we have

$$p_s(a,N,M,N_R,p_f) = \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right]. \tag{5.34}$$

In order to simplify the term of transmission in one $D_p$, Eq. (5.34) can also be written as

$$\begin{aligned} p_s(a,N,M,N_R,p_f) &= \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1} \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right] \\ &= (1-a)^{M-1} \left[ 1-(1-a)^{D_p} \right] \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right]. \end{aligned} \tag{5.35}$$

The optimum access probability $a^*$ is obtained by differentiating $p_s(a,N,M,N_R,p_f)$ with respect to $a$ and equating it to zero, i.e.,

$$\begin{aligned} &\frac{d}{da} p_s(a,N,M,N_R,p_f) \\ &= \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right] \Big[ -(M-1)(1-a)^{M-2} \left[ 1-(1-a)^{D_p} \right] \\ &\quad + D_p (1-a)^{M-1}(1-a)^{D_p-1} \Big] \\ &= \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right] (1-a)^{M-2} \left[ (1-a)^{D_p} (M-1+D_p) - (M-1) \right] \\ &= 0, \end{aligned} \tag{5.36}$$

which solving for $a$, it follows that

$$a^* = 1 - \left( \frac{M-1}{M-1+D_p} \right)^{\frac{1}{D_p}}. \tag{5.37}$$

The successful delivery probability for the optimum value $a^*$ is obtained by substituting Eq. (5.37) into Eq. (5.35), resulting in

$$\begin{aligned} &p_s(a,N,M,N_R,p_f) \\ &= \left( \frac{M-1}{M-1+D_f} \right)^{\frac{M-1}{D_p}} \frac{D_f}{M-1+D_f} \left\{ \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[ (1-p_f)^{n_{i,j}} (p_f)^{N_R-1-n_{i,j}} \right] \right\}. \end{aligned} \tag{5.38}$$

### 5.5.2 Case 2: PU is present in the channel ($0 < \pi_1 < 1$)

In this case, PUs are present on a given time slot with probability $\pi_1 \in (0,1)$. Similar to previous section, in this case there are slots, time periods of $D_p$ slots and, a set of $N$ time periods of $D_p$ slots, called $D_f$. By observing the presence of PUs in the system, in steady state, the number $N_f$ of free slots in $D_p$ slots follows a binomial distribution with parameters $D_p$ and $\pi_1$. The quantity of $N = \frac{D_f}{D_p}$ defines the number of attempts to transmit the message and the probability of reception failure for each node $p_f$. As we see in previous section, we must to study all possible cases in which all the nodes receive the broadcast message in a period of $D_p$ slots, to do that, we evaluate all the elements $n_{i,j}$ as in matrix $A$, similarly to Table 5.2. Using the law of total probability, the successful delivery probability with hidden terminals is given by

$$
\begin{aligned}
&p_s\left(a, N, D_f, M, N_R, p_f\right) \\
&= \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \sum_{d=1}^{D_p} P\left(N_f = d\right) p_s\left(a, d, M\right) \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right] \\
&= \sum_{d=1}^{D_p} P\left(N_f = d\right) p_s\left(a, d, M\right) \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right] \\
&= \sum_{d=1}^{D_p} \binom{D_p}{d} \left(\pi_1\right)^d (1-\pi_1)^{D_p-d} (1-a)^{M-1} \left[1-(1-a)^d\right] \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right]\right] \\
&= (1-a)^{M-1} \sum_{d=1}^{D_p} \binom{D_p}{d} \left(\pi_1\right)^d (1-\pi_1)^{D_p-d} \\
&\quad -(1-a)^{M-1} \sum_{d=1}^{D_p} \binom{D_p}{d} \left(\pi_1 - a\pi_1\right)^d (1-\pi_1)^{D_p-d} \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right]\right] \\
&= (1-a)^{M-1} \left[1-(1-\pi_1)^{D_p}\right] - (1-a)^{M-1} \\
&\quad \left[(1-a\pi_1)^{D_p} - (1-\pi_1)^{D_p}\right] \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right]\right] \\
&= (1-a)^{M-1} \left[1-(1-a\pi_1)^{D_p}\right] \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_f\right)^{n_{i,j}} \left(p_f\right)^{N_R-1-n_{i,j}}\right]\right]. \qquad (5.39)
\end{aligned}
$$

Differentiating $p_s(a, N, D_f, M, N_R, p_f)$ with respect to $a$ and equating it to zero, it results that $p_s(a, N, D_f, M, N_R, p_f)$ is maximized at the value $a^*(D_p)$ that satisfies

$$
D_p \pi_1 \left(1-a\right) \left(1-a\pi_1\right)^{D_p-1} = (M-1) \left[1-(1-a\pi_1)^{D_p}\right], \qquad (5.40)
$$

which can be solved numerically for $a$.

## 5.6 Numerical Results

In this section we show some important results related to the successful delivery probability $p_s$ in function of number of the nodes $M = N_R + N_H$ and final deadline $D_f$. The main idea is to present the improvement on the performance using re-transmission of the broadcast message. For the simulations there are 10 nodes randomly distributed inside the broadcast area, and 10 nodes inside the hidden terminal area, chosen based in previous works. For the analysis we consider 4 cases to compare the performance of our proposed scheme. The cases are:

- Non-periodic case: There is no periodic transmission of the message, i.e., $D_f = D_p$. Moreover, the packet failure probability is null ($p_f = 0$) and the access probability $a$ is optimal.
- Non-periodic case with probability of failure: As in previous item, there is no periodic transmission of the message, and $D_f = D_p$. The access probability is $a$ optimal. A constant value for the probability of packet failure is included in this model to represent reception errors.
- Geometric case: this case was presented in Section 5.4. The message is re-transmitted periodically, with $D_f$ defined as a multiple $N$ of time period $D_p$, i.e., $D_f = ND_p$. In the analysis, the successful delivery probability was modeled using the geometric distribution. A constant value for the probability of packet failure is included in this model to represent reception errors.
- Multinomial coefficient case: this case was presented in Section 5.5. In this case, the message is transmitted periodically, with $D_f$ defined as a multiple $N$ of time periods of $D_p$ slots, i.e. $D_f = ND_p$. In this analysis, the successful delivery probability is modeled using the multinomial coefficients. A constant value for the probability of packet failure is included in this model to represent reception errors.

The results for each case will be presented to compare and show the improvement and the benefits in transmitting the message several times. The observed advantage has a price to be paid, which is the reduction of the size of the packet to be equal to the amount of times the message is repeated.

Figs. 5.7 and 5.8 present the successful delivery probability $p_s$ as a function of the total number of nodes $M = N_R + N_H$ for the Geometric and Multinomial case, respectively. A constant value for the probability of packet failure of 0.1 is included and $D_f = 500$. It is possible to observe that the proposed scheme of re-transmit the broadcast message increased the successful delivery probability $p_s$. For 20 nodes, $p_s$ increase its value 64% and 79% for the geometric and the multinomial cases respectively, when the message is re-transmitted 100 times ($N = 100$) compared with the non-periodic scheme ($N = 1$). For $N = 10$ attempts, it is possible to obtain values greater than or equal to 99.9% for the successful delivery probability $p_s$ for 7 users in the geometric case and 10 users in the multinomial one, which indicates that the multinomial model has a better performance in terms of $p_s$, due to not assume that all nodes must receive in the same $D_p$. It is also important to note, that if $M$ goes to infinity the successful delivery probability it seems to converge to 0, what

makes sense. If there are infinite users in the system there will be a few probability of access to the channel. The proposed mechanisms works well for a small number of nodes, around $M = 20$, in which it can be obtained a successful probability greater or equal than 99.9% repeating the message.

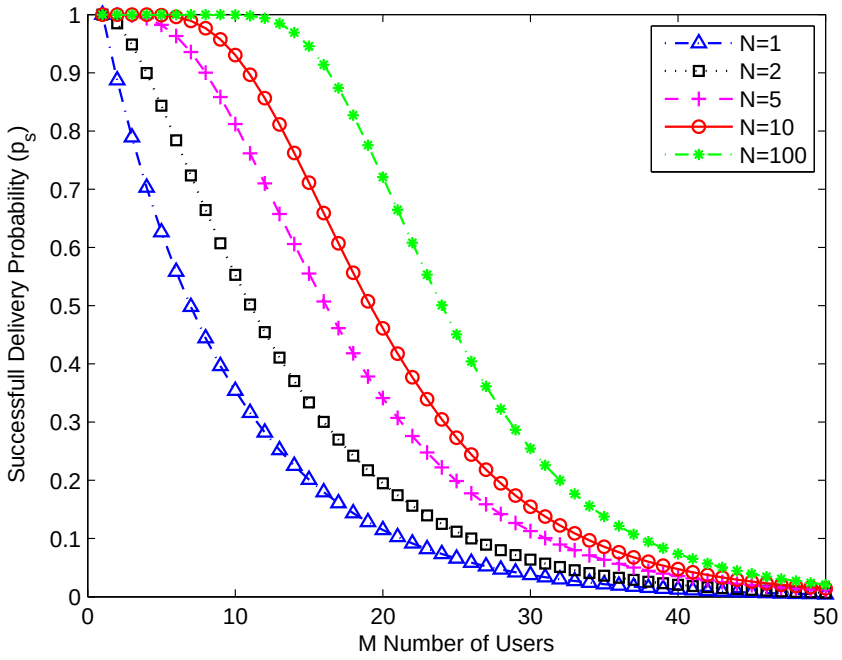



Figure 5.7: Successful delivery probability as a function of the total number of nodes $M = N_R + N_H$, probability of failure $p_f = 0.1$ and $\pi_1 = 1$, varing the number of transmission attempts $N$ for Geometric case, with $D_f = 500$.

Fig. 5.9 presents the successful delivery probability $p_s$ as a function of the final deadline $D_f$ for the 4 cases discussed before: the non-periodic with and without fail, and the geometric and multinomial cases. A constant value for the probability of packet failure of $p_f = 0.1$ is included and the total number of nodes $M = N_R + N_H = 20$ is used. In the geometric and multinomial cases, the message is re-transmitted 10 times, i.e., $N = \frac{D_f}{D_p} = 10$. There is an important reduction of 53.4% in the successful delivery probability $p_s$ between the non-periodic cases, with and with out probability of failure $p_f$. Observing the three models in which the term probability of failure is included, for $D_f = 500$, there are gains of 52.1% and 60.3% for the geometric and multinomial cases, compared with the non-periodic one with $p_f = 0.1$.

Fig. 5.10 illustrates the success probability as a function of total number of nodes $M = N_R + N_H$ in the network. A value for the probability of packet failure of $p_f = 0.1$ is included and the final deadline is $D_f = 500$ slots. In the geometric and multinomial cases, the message is re-transmitted 10 times, i.e., $N = \frac{D_f}{D_p} = 10$. For $M = 20$ there are gains of 52.1% and 60.3% for the geometric and multinomial model, as it is also seen in Fig. 5.9 compared with the non-periodic case for $p_f = 0.1$. In all cases analyzed in this figure it is not possible to obtain a successful delivery probability $p_s$ greater than 99.9%. To obtain such value of probability we must re-transmit the

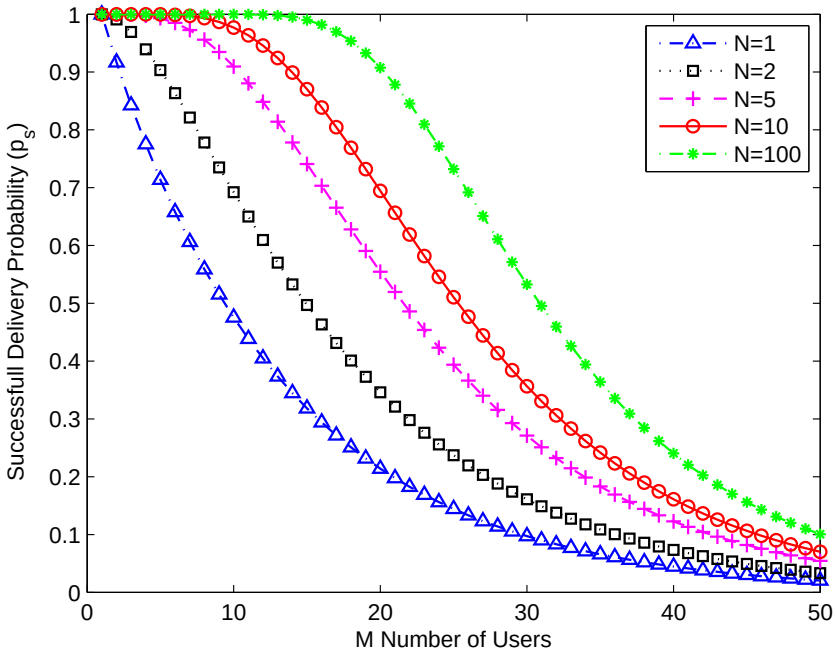



Figure 5.8: Successful delivery probability as a function of the total number of nodes $M = N_R + N_H$, probability of failure $p_f = 0.1$ and $\pi_1 = 1$, varing the number of transmission attempts $N$ for Multinomial case, with $D_f = 500$..

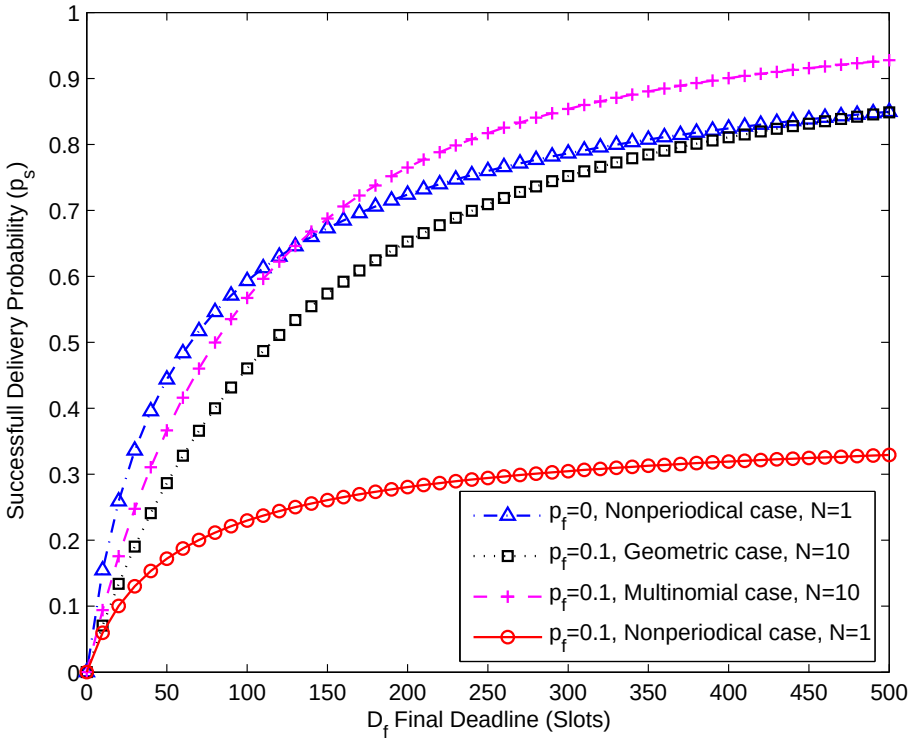



Figure 5.9: Successful delivery probability as a function of $D_f$, $N_R = 10$, $N_H = 10$, $\pi_1 = 1$, i.e., channel unoccupied by primary users.

message more times. As we can see in Fig. 5.11, with parameters $p_f = 0.1$, $D_f = 500$ and $M = 20$ the message must be re-transmitted 16 times and 31 times, for the geometric and the multinomial cases respectively, to get values of $p_s$ greater than 99.9%, but the size of the message must be reduced and it is related to the amount of times the message is repeated. It can be concluded from Fig. 5.10 that the number of nodes greatly impacts the successful delivery probability $p_s$, what shows that the scheme developed has good performance for few nodes. Also it can be seen in these two Figs. 5.10 and 5.11 that the multinomial case shows gain in performance, which decrease if the number of nodes $M$ increase, and it goes to zero if the number of nodes tend to infinity. If the number of users $M$ goes to infinity, the probability of success goes to 0, what makes sense because there will be a lot of users disputing the channel with the Slotted Aloha protocol.

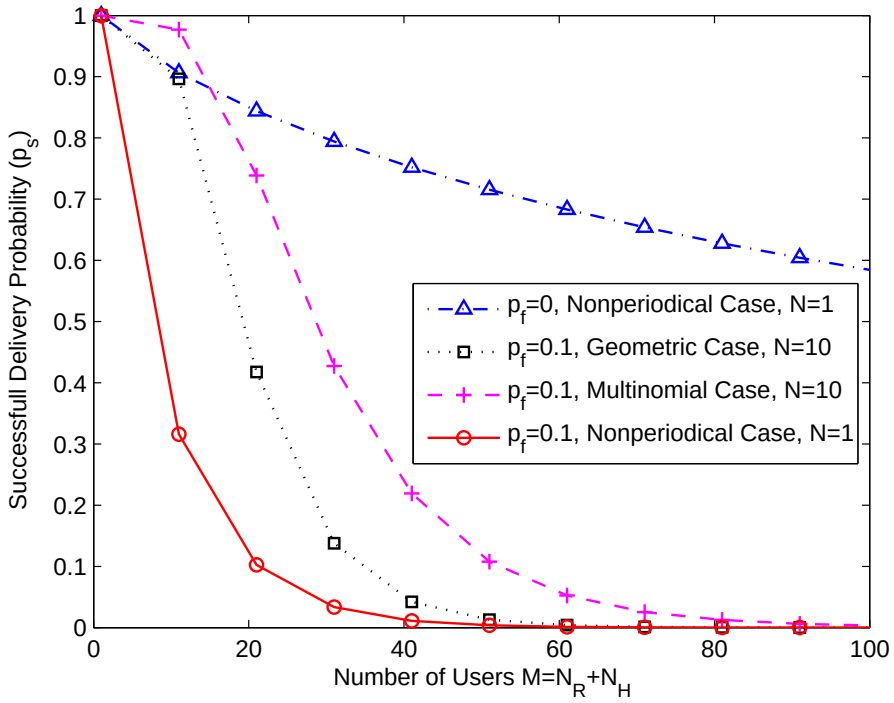



Figure 5.10: Successful delivery probability as a function of $M$, probability of failure $p_f = 0.1$, $D_f = 500$ and $\pi_1 = 1$, i.e., channel unoccupied by primary users.

Figs. 5.12 and 5.13 present the successful delivery probability $p_s$ as a function of the final deadline $D_f$ for the geometric and the multinomial cases respectively. In this case there are PUs present occupying the channel. Similarly to the previous figures a value for the probability of packet failure of $p_f = 0.1$ is employed and the number of nodes $M = 20$. In the geometric and multinomial cases the message is re-transmitted 10 times, i.e., $N = \frac{D_f}{D_p} = 10$. In the geometric case, there are reductions of 25.3%, 21.2% and 11.4% in the successful delivery probability $p_s$ for $\pi_1 = 0.2$, $\pi_1 = 0.5$ and $\pi_1 = 0.8$, respectively, compared with the case $\pi_1 = 1$. For the multinomial case there are reductions of of 29.4%, 26.3% and 15.3% in the successful delivery probability $p_s$ for $\pi_1 = 0.2$, $\pi_1 = 0.5$ and $\pi_1 = 0.8$ respectively, compared with the case $\pi_1 = 1$. These values confirm the better performance of the multinomial case compared with the geometric one.

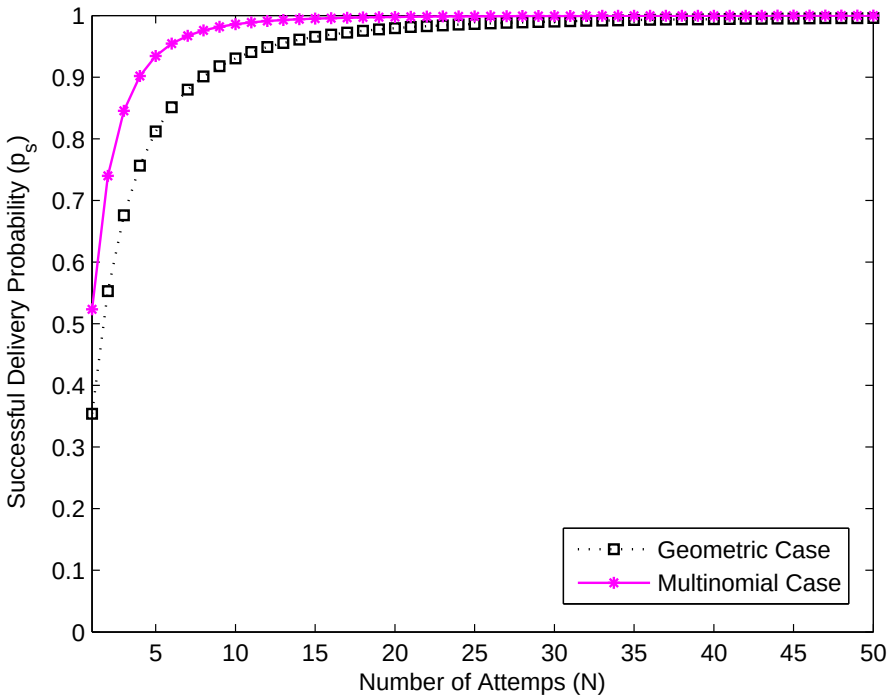



Figure 5.11: Successful delivery probability as a function of $N$, $N_R = 10$, $N_H = 10$, $\pi_1 = 1$, $D_f = 500$ and $p_f = 0.1$.

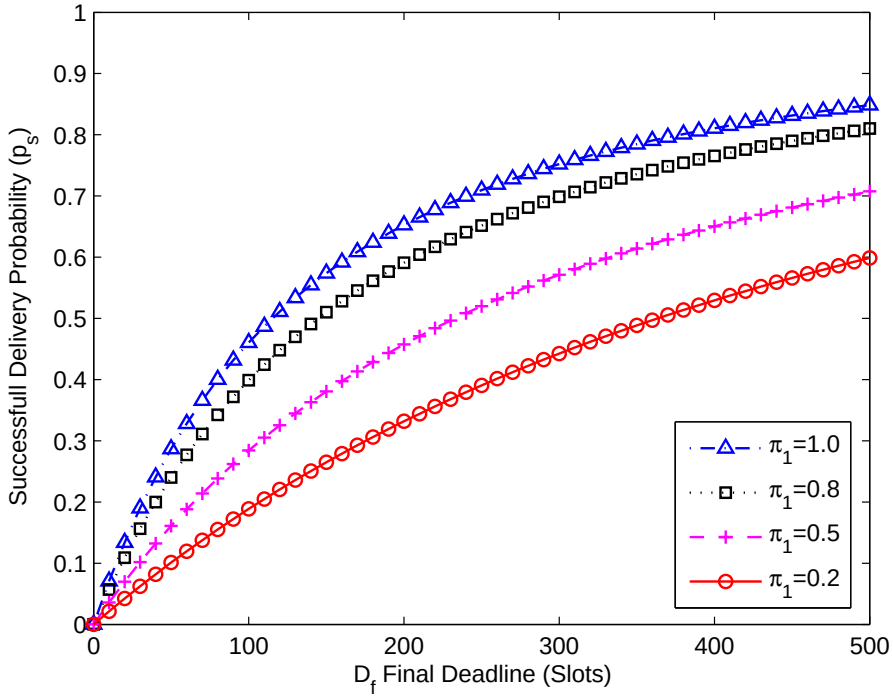



Figure 5.12: Successful delivery probability for Geometric case, as a function of $D_f$, $p_f = 0.1$ and diffent values of $\pi_1$, i.e., channel occupied by primary users.

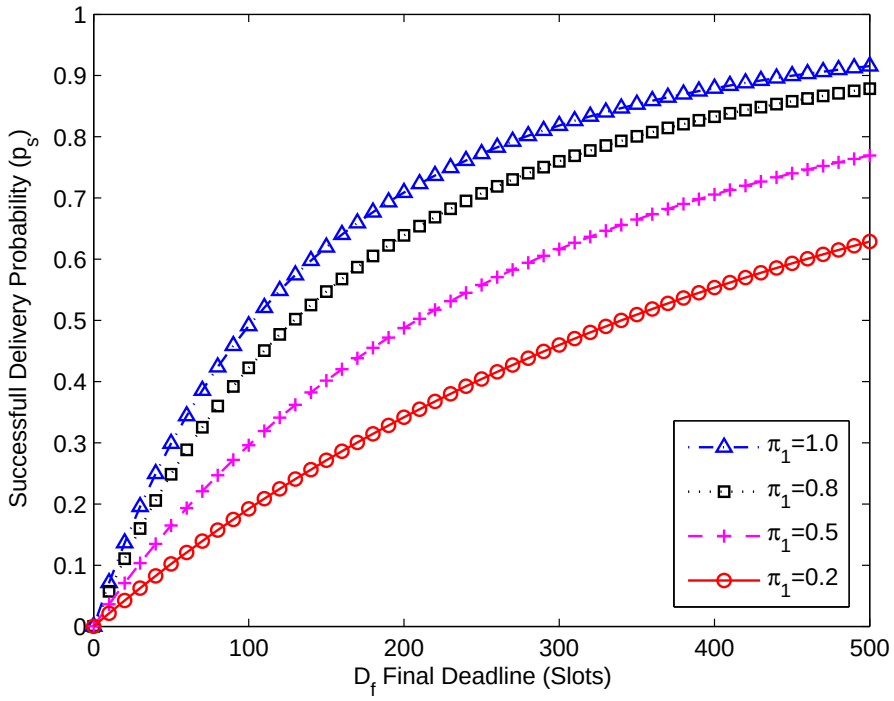



Figure 5.13: Successful delivery probability for Multinomial case, as a function of $D_f$, $p_f = 0.1$ and diffent values of $\pi_1$, i.e., channel occupied by primary users.

Fig. 5.14 presents the successful delivery probability $p_s$ as function of the number of nodes $M = N_R + N_H$, using the same parameters as in Figs. 5.12 and 5.13, $p_f = 0.1$, $D_f = 500$ and $N = \frac{D_f}{D_p} = 10$. It can be seen that for $M = 40$ there are reductions in the value of successful delivery probability $p_s$ of 6.1%, 9.2% and 19.1% for $\pi_1 = 0.2$, $\pi_1 = 0.5$ and $\pi_1 = 0.8$ respectively, compared with occupancy of the channel $\pi_1 = 1$, due to the presence of PUs in the system which hinder the access to the channel. Similarly to Fig. 5.10, if the number of users $M$ goes to infinity, the probability of success tends to 0, because there will be infinite users disputing the channel due to the Slotted Aloha protocol.

Fig. 5.15 illustrates the successful delivery probability $p_s$ as function of the packet failure probability $p_f$, for $D_f = 500$ and $M = 20$. In the geometric and multinomial cases the message is re-transmitted 10 times, i.e., $N = \frac{D_f}{D_p} = 10$. In this figure it is possible to observe the degradation of $p_s$ with respect to the probability of failure $p_f$. For a probability of failure $p_f = 0.2$ there are differences of 66.1% and 46% between the multinomial and the geometric model, respectively, compared with the non-periodic case. In order analyze to the impact that $p_f$ causes in the successful delivery probability we decide to study this parameter and its relation with fading to obtain a more realistic value of $p_f$, which will be done in the next chapter.

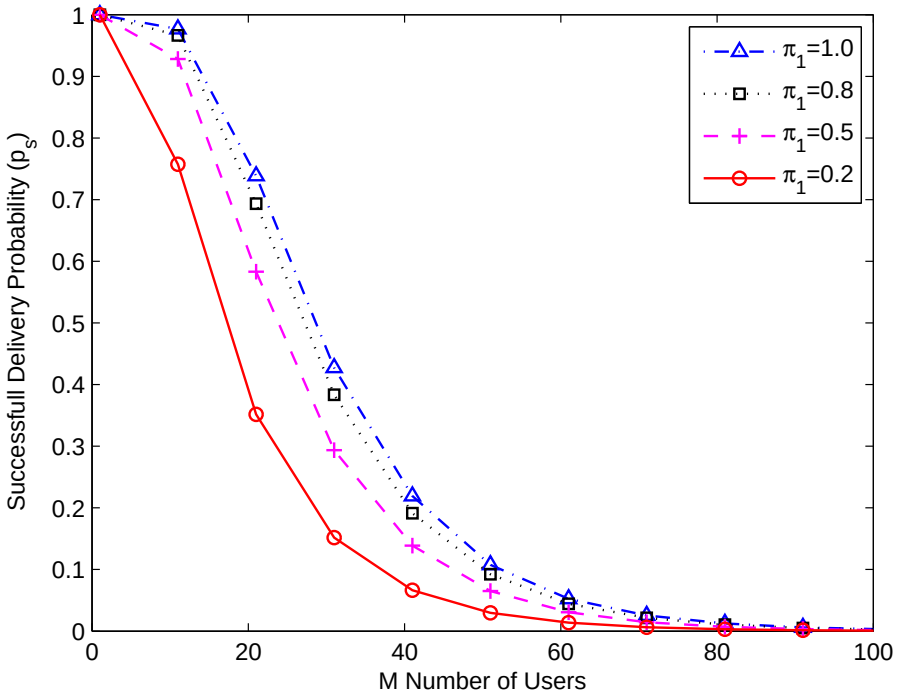



Figure 5.14: Successful delivery probability for Multinomial Case, as a function of $M$, probability of failure $p_f = 0.1$ and diffent values of $\pi_1$, i.e., channel occupied by primary users.

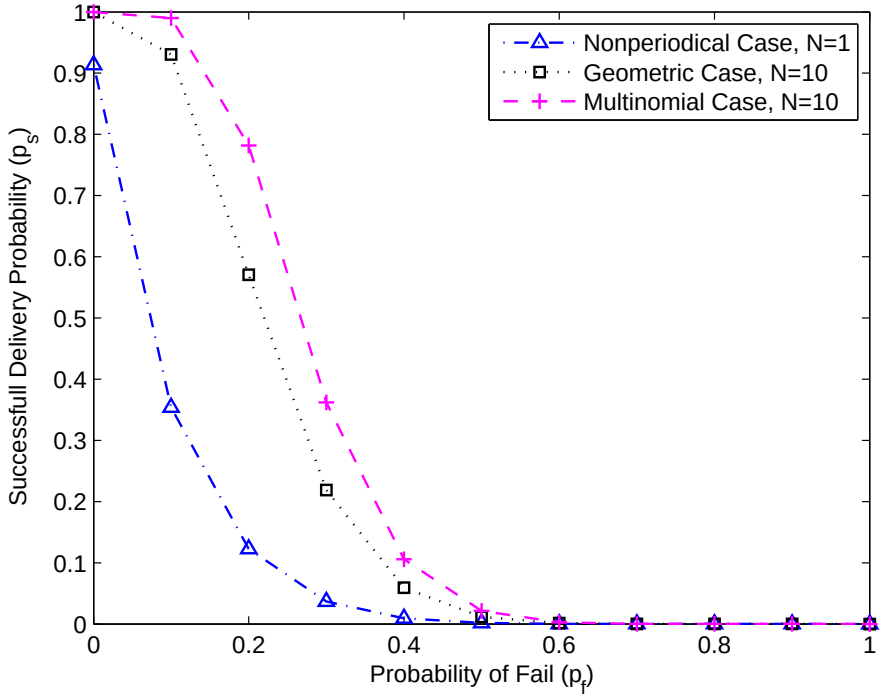



Figure 5.15: Successful delivery probability for Multinomial Case, as a function of $p_f$, number of users $M = 10$, $D_f = 500$ and $\pi_1 = 1$, i.e., channel unoccupied by primary users..

## 5.7 Conclusion

This chapter presented two approaches for modeling periodic broadcast transmission in order to increase the probability of success of safety broadcast messages. Two models were developed, the first one, assuming that all nodes must receive the message successfully at the same period of slots $D_p$, called Geometric case, because it is used a geometric distribution to model it. The second model assumes that no all nodes must receive the message in one specific $D_p$, called the Multinomial Case, because it uses multinomial coefficients to express all possible cases with success. The multinomial case shows a better performance, and the proposed scheme to repeat the message several times show an improvement in the successful delivery probability $p_s$. In the next chapter, it will be studied the probability of failure $p_f$ associated to fading channel in VANETS, and it will be used the parameters proposed by IEEE 1609 [58] and the IEEE 802.11p [13] to evaluate the reliability of the proposed scheme.

# Chapter 6

# Impact of Fading Channel and Reliability in VANETs

## 6.1 Introduction

Vehicular communications present scenarios with unfavorable characteristics to develop wireless communications, i.e., multiple reflecting objects able to degrade the strength and quality of the received signal. Additionally, fading effects resulting from the mobility of the surrounding objects and/or the sender and receivers themselves have to be taken into account. While there are many factors that can affect the bit error rate (BER) communication performance, which finally impact the reliability in the delivery of the broadcast safety message.

Reliability in the context of VANET broadcast services is defined as the probability that all the intended mobile nodes receive the broadcast message within the specified operation duration. Safety systems can be designed based on a high speed wireless communication network to improve the safety on the road. Once an emergency situation occurs, it is critical to inform the surrounding vehicles about the situation as soon as possible. Because driver reaction time (the duration between when an event is observed and when the driver actually applies the brakes) to warn traffic signals, such as the brake light, which can be in the order of 700 ms or longer, the update interval of safety message should be less than 100 ms (we refer to it as the lifetime of a safety message). According to the requirements in [7], the probability of the message delivery failure in a vehicular network should be less than 0.01 (or packet delivery ratio greater than 0.99). Accordingly, as stated in [22], safety applications require at most a 100 ms mean delay and a 99.9% probability of the successful transmission in order to be effective.

In this chapter, the concepts of fading channel and reliability in VANETS will be included in our analysis, in order to obtain a realistic performance of the system. The requirements for safety applications are shown, and the parameters of IEEE 1609 and IEEE 802.11p are used to obtain numerical results and show that it is possible to improve the probability of success $p_s$, in a final deadline $D_f$. Finally, we concluded that it is possible to obtain successful delivery probability and delay which guarantee reliability in vehicular networks using some parameters values in the

proposed scheme.

## 6.2 Probability of failure

In previous analysis, it was not considered physical layer aspects neither the fading aspects that degrade the strength and quality of the received signal. A value of failure probability $p_f$, usually of 10% were assumed, but it does not necessarily represent the real impact of the physical layer. In order to present a realistic model of the system, we include the term bit error probability $p_{BER}$ inside the probability of packet failure $p_f$, assuming that bit errors occur independently on the packet,

$$p_f = 1 - (1 - p_{BER})^T, \tag{6.1}$$

where, $T$ is the length of the packet and $p_{BER}$ is the fixed bit error rate (BER) probability that will be numerically evaluated for a Nakagami-m fading channel for each node. To evaluate the $p_{BER}$, it is necessary define the modulation scheme to be used. In IEEE 802.11p [13], there are 5 types of modulations that can be used: BPSK, QPSK, 16QAM and 64QAM. For our analysis we use the BPSK modulation, because it is simple and offer small error rates. The expression for the error bit of binary PSK $p_{BER}$, as a function of the received SNR is given by [53]

$$p_{BER}(\gamma) = Q\left(\sqrt{2\gamma}\right), \tag{6.2}$$

where $\bar{\gamma} = \alpha\frac{E_b}{N_0}$, $\alpha$ is the attenuation parameter, $E_b$ is the energy per bit and $N_0$ is the noise power. To obtain the error probability, when the attenuation parameter ($\alpha$) is characterized by the Nakagami-m distribution, we must average the probability of error evaluating the integral

$$p_{BER}(\gamma) = \int_0^\infty Q\left(\sqrt{2\gamma}\right) f_\gamma(\gamma) d\gamma, \tag{6.3}$$

where $Q\left(\sqrt{2\bar{\gamma}}\right)$ is the tail probability of the standard normal distribution, and $f_{\bar{\gamma}}(\bar{\gamma})$ represents the probability density function (PDF) of the Nakagami-m distribution,

$$f_\gamma(\gamma) \quad = \quad \frac{m^m}{\Gamma(m)\bar{\gamma}^m}\gamma^{m-1}e^{\frac{-m\gamma}{\bar{\gamma}}}, \tag{6.4}$$

in which $\bar{\gamma} = E(\alpha)\frac{E_b}{N_0}$ and $m$ is the fading figure, as it was mentioned in Chapter 3. It has been estimated based on empirical measurements for a vehicle-to-vehicle link with values of

$$m = \begin{cases} 1.75 & \text{if } d < 80\,m; \\ 0.75 & \text{if } d > 80\,m. \end{cases} \tag{6.5}$$

In order to obtain a more realistic value of the packet failure probability Eq. (6.3) is numerically evaluated to compute the value of $p_{BER}$. Given that, the value of $p_f$ can be computed according in Eq. (6.1). In the next sections this new definition of $p_f$ will be inserted in the analysis of all cases, the non periodic, the geometric and the multinomial cases.

## 6.3 Non-periodic Case with Nakagami-m Fading

In Section 5.3 it was computed the successful delivery probability $p_s$ for the case of non-periodic broadcast, i.e., $D_f = D_p$. A probability of packet failure $p_f$ was inserted in the model to represent channel and reception fails. Now a new definition of probability of failure $p_f$, shown in Eq.(6.1) will be incorporated to our analysis to represent a more realistic model in a VANET scenario. Similarly to Section 5.3, two cases are analyzed: with and without PU present in the channel.

### 6.3.1 Case 1: PU is not present in the channel ($\pi_1 = 1$)

Following previous analysis, if all events are assumed to be independent of each other, the probability of successful transmission of the HoL packet since its arrival at the head of the queue is $a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]$, where $(1-a)^{N_R-1}$ means that only the transmitter node transmit inside his coverage area, $(1-a)^{N_H}$ implies that none of the nodes inside the interference area transmit, and based in Eq. (6.1) we introduced the term $\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]$ to indicate that there is not failure in the reception of the entire message in every node from 1 to $N_R-1$, excluding the transmitter node. The successful delivery probability $p_s(a, D_f, M, N_R, p_{BERi})$ is obtained by noting that the successful transmission at each slot, up to the deadline $D_f$, are mutually exclusive events, then

$$\begin{aligned} p_s(a, D_f, M, N_R, p_{BERi}) &= \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{M-1}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] \\ &= (1-a)^{M-1}\left[1-(1-a)^{D_f}\right](1-p_f)^{N_R-1}. \end{aligned} \tag{6.6}$$

In fact, the value of the optimal access probability $a^*$ can be obtained by differentiating $p_s(a, D_f, M, N_R, p_{BERi})$ with respect to $a$ and equating it to zero, i.e.,

$$\begin{aligned} \frac{d}{da}p_s(a, D_f, M, N_R, p_{BERi}) &= \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\Big[-(M-1)(1-a)^{M-2}\left[1-(1-a)^{D_p}\right] \\ &\quad +D_p(1-a)^{M-1}(1-a)^{D_p-1}\Big] \\ &= \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right](1-a)^{M-2}\Big[(1-a)^{D_p}(M-1+D_p) \\ &\quad -(M-1)\Big] \\ &= 0, \end{aligned} \tag{6.7}$$

which, by solving for $a$, it follows that

$$a^* = 1-\left(\frac{M-1}{M-1+D_f}\right)^{\frac{1}{D_f}}. \tag{6.8}$$

It is possible to note that Eq. (6.8) do not depend on $p_f$ similarly to Eq. (4.12) in previous chapter, because $p_f$ is a constant value independent of $a$. The successful delivery probability for

the optimum value $a^*$ is obtained by substituting Eq. (6.8) into Eq. (6.6), resulting in

$$p_s(a, D_f, M, N_R, p_{BERi}, T) = \left(\frac{M-1}{M-1+D_f}\right)^{\frac{M-1}{D_f}} \frac{D_f}{M-1+D_f} \prod_{i=1}^{N_R-1} \left[1-(1-p_{BERi})^T\right]. \quad (6.9)$$

### 6.3.2 Case 2: PU present on the channel ($0 < \pi_1 < 1$ :)

In this case, SUs can only use the channel when the PU is not present, which happens with probability $\pi_1 \in [0,1]$ in any given slot. Analogous to what it was done in Chapter 5 we observe that, in steady state, the number $N_f$ of free slots within $D_f$ follows a binomial distribution with parameters $D_f$ and $\pi_1$. Using the law of total probability, the successful delivery probability when interfering nodes are present and introducing the term $\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]$ to indicate that there is no failure in the reception of the entire message we have

$$\begin{aligned}
&p_s\left(a, D_f, M, N_R, p_{BERi}, T\right) \\
&= \sum_{d=1}^{D_f} P\left(N_f = d\right) p_s\left(a, d, M\right) \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] \\
&= \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} (1-a)^{M-1}\left[1-(1-a)^d\right] \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] \\
&= (1-a)^{M-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1)^d (1-\pi_1)^{D_f-d} \\
&\quad -(1-a)^{M-1} \sum_{d=1}^{D_f} \binom{D_f}{d} (\pi_1 - a\pi_1)^d (1-\pi_1)^{D_f-d} \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] \\
&= (1-a)^{M-1}\left[1-(1-\pi_1)^{D_f}\right] - (1-a)^{M-1} \\
&\quad \left[(1-a\pi_1)^{D_f} - (1-\pi_1)^{D_f}\right] \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] \\
&= (1-a)^{M-1}\left[1-(1-a\pi_1)^{D_f}\right] \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]. \quad (6.10)
\end{aligned}$$

By differentiating Eq. (6.10) with respect to $a$ and equating it to zero, it results that $p_s$ is maximized at the value $a^*(D_f)$ that satisfies

$$D_p \pi_1 (1-a)(1-a\pi_1)^{D_F-1} = (M-1)\left[1-(1-a\pi_1)^{D_f}\right], \quad (6.11)$$

which it can be solved numerically for $a$.

## 6.4 Geometric Case with Nakagami-m Fading

In Section 5.4, it was computed the successful delivery probability $p_s$ for periodic broadcast ($D_f > D_p$), using the geometric distribution approach. The probability of packet failure $p_f$ was

inserted in the model to represent channel and reception failures. A new definition of the term probability of failure $p_f$, from Eq. (6.1) will be incorporated to our analysis to represent a more realistic model in VANETs scenario. Similar to Section 5.4 two cases are analyzed: with and without PUs present in the channel.

### 6.4.1 Case 1: PU is not present in the channel ($\pi_1 = 1$)

In the Subsection 5.4.1 we obtained the probability of success in the case $\pi_1 = 1$, applying the concept of the geometric distribution. Now, based on Eq. (6.1), we introduce the term $\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]$ to indicate that there is no failure in the reception of the entire message in every node from 1 to $N_R - 1$. Therefore, the successful delivery probability is

$$\begin{aligned} & p_s(a, D_f, D_p, N_R, N_H, p_{BER}, T) \\ &= \sum_{x=1}^{Df/Dp} \left(1 - \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H} \prod_{i=1}^{N_R-1}\left[(1-p_{BERi})^T\right]\right)^{x-1} \\ & \left(\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H} \prod_{i=1}^{N_R-1}\left[(1-p_{BERi})^T\right]\right). \end{aligned} \tag{6.12}$$

Defining $M = N_R + N_H$, Eq. (6.12) becomes

$$\begin{aligned} & p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\ &= \sum_{x=1}^{Df/Dp} \left(1 - \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1} \prod_{i=1}^{N_R-1}\left[(1-p_{BERi})^T\right]\right)^{x-1} \\ & \left(\sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1} \prod_{i=1}^{N_R-1}\left[(1-p_{BERi})^T\right]\right). \end{aligned} \tag{6.13}$$

Using the same procedure applied in Section 5.4, we obtain

$$\begin{aligned} & p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\ &= 1 - \left[1 - \left((1-a)^{D_p} - 1\right)(1-a)^{M-1} \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\right]^{\frac{D_f}{D_p}}. \end{aligned} \tag{6.14}$$

Differentiating Eq. (6.14), defining $N = \frac{D_f}{D_p}$ and equating it to zero, we obtain

$$\begin{aligned} 0 \;=\; & \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\left((M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2} + D_p(1-a)^{D_p+M-2}\right) \\ & \left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1} \prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right] + 1\right)^{N-1}, \end{aligned} \tag{6.15}$$

which could be solve numerically for $a$.

### 6.4.2 Case 2: PU present on the channel ($0 < \pi_1 < 1$ :)

In the Subsection 5.4.2, we obtained the probability of success in the case $0 < \pi_1 < 1$, with probability of failure $p_f$. In this part, we introduced the term $\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]$ to indicate that there is not fail in the transmission of the entire message in every node from 1 to $N_R$ as in Eq. (6.1). Then the successful delivery probability $p_s(a, D_f, D_p, M, N_R, p_{BER}, T)$ is represented by

$$\begin{aligned} & p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\ = \; & 1-\left[1-\left((1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\right)\right]^{\frac{D_f}{D_p}}. \end{aligned} \tag{6.16}$$

Defining $N = \frac{D_f}{D_p}$, we can write Eq. (6.16) as

$$\begin{aligned} & p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\ = \; & 1-\left[1-\left((1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right]\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\right)\right]^{N}. \end{aligned} \tag{6.17}$$

The procedure for derivative of $p_s$ with respect to $a$ is presented in Appendix A.2. The final expression obtain is

$$\begin{aligned} & \frac{d}{da}p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\ = \; & -N\left[(M-1)(1-a)^{M-2}(1-p_f)^{M-1}\left(1-(1-a\pi_1)^{D_p}\right)\right. \\ & \left.-D_p\pi_1(1-a)^{M-1}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right](1-a\pi_1)^{D_p-1}\right] \\ & \left(1-(1-a)^{M-1}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}. \end{aligned} \tag{6.18}$$

Equating Eq. (6.18) to zero, it results that $p_s(a, D_f, D_p, M, N_R, p_{BER}, T)$ is maximized at the value $a^*$. That expression can be solved numerically for $a$ in order to obtain the maximum value for $p_s$, i.e., solve for $a$ the expression

$$\begin{aligned} 0 \; = \; & -N\left[(M-1)(1-a)^{M-2}(1-p_f)^{M-1}\left(1-(1-a\pi_1)^{D_p}\right)\right. \\ & \left.-D_p\pi_1(1-a)^{M-1}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right](1-a\pi_1)^{D_p-1}\right] \\ & \left(1-(1-a)^{M-1}\prod_{i=1}^{N_R-1}\left[1-(1-p_{BERi})^T\right]\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}. \end{aligned} \tag{6.19}$$

## 6.5 Multinomial Case with Nakagami-m Fading

In Section 5.5, it was computed the successful delivery probability $p_s$ for periodic broadcast and $D_f > D_p$, using the multinomial coefficients approach. A probability of packet failure $p_f$ was

inserted in the model to represent channel and reception fails. Now a new term of probability of failure $p_f$, presented in Eq.(6.1) will be incorporated to our analysis, to represent a more realistic model in a VANET scenario. In this case, we have several $D_p s$ in a $D_f$, with a defined quantity of nodes intended to receive the broadcast message in one specific $D_p$. Eq.(6.1) should be adapted in order to evaluate all the cases in the matrix $A$. Then we define the success as, all nodes in that entry of the matrix $(i, j)$ which receive the message successfully, represented by

$$\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}, \tag{6.20}$$

where $\left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}}$ means that, in that specific period of $D_p$ slots, the nodes $n_{(i,j)}$ successfully received the message, while the others $N_R - 1 - n_{i,j}$, did not. Similar to Section 5.5, two cases are analyzed: with and without PU present in the channel.

### 6.5.1 Case 1: PU is not present in the channel ($\pi_1 = 1$)

Similar to Subsection 5.5.1 and incorporating the term in (6.20), the packet transmission probability in a given slot is $a$, a successful transmission of a tagged HoL packet happens in the $k^{th}$ slot if the packet is not transmitted in any of the previous $k-1$ slots, and no other node transmits in the broadcast area as well as in the hidden-terminal area in the $k^{th}$ slot. Accordingly, the probability of successful transmission of the HoL packet since its arrival at the head of the queue is represented by

$$\begin{aligned}
&p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\
&= \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1} \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}} \\
&= (1-a)^{M-1}\left[1-(1-a)^{D_p}\right] \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}
\end{aligned} \tag{6.21}$$

The optimum access probability $a^*$ is obtained by differentiating $p_s(a, D_f, D_p, M, N_R, p_{BER}, T)$ whit respect to $a$ and equating it to zero, i.e.,

$$\begin{aligned}
&\frac{d}{da} p_s(a, D_f, D_p, M, N_R, p_{BER}, T) \\
&= \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}} \Big[-(M-1)(1-a)^{M-2} \\
&\quad \left[1-(1-a)^{D_p}\right] + D_p(1-a)^{M-1}(1-a)^{D_p-1}\Big] \\
&= \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}} (1-a)^{M-2} \\
&\quad - \left[(1-a)^{D_p}(M-1+D_p)(M-1)\right] \\
&= 0,
\end{aligned} \tag{6.22}$$

which, by solving for $a$, it follows that

$$a^* = 1 - \left(\frac{M-1}{M-1+D_p}\right)^{\frac{1}{D_p}}. \tag{6.23}$$

### 6.5.2 Case 2: PU present on the channel ($0 < \pi_1 < 1$)

In the Subsection 5.5.2, we obtained the probability of success in the case $0 < \pi_1 < 1$, with probability of failure $p_f$. Following the same analysis done in Subsection 5.5.2, and inserting the term (6.20) for probability of failure, the probability of success $p_s$ can be computed as

$$\begin{aligned}
&p_s\left(a, D_f, D_p, M, N_R, p_{BER}, T\right) \\
&= \sum_{d=1}^{D_p} P\left(N=d\right) p_s\left(a, d, M\right) \sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}} \\
&= \sum_{d=1}^{D_p} \binom{D_p}{d} (\pi_1)^d (1-\pi_1)^{D_p-d} (1-a)^{M-1}\left[1-(1-a)^d\right] \\
&\quad \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}\right] \\
&= (1-a)^{M-1} \sum_{d=1}^{D_p} \binom{D_p}{d} (\pi_1)^d (1-\pi_1)^{D_p-d} \\
&\quad -(1-a)^{M-1} \sum_{d=1}^{D_p} \binom{D_p}{d} (\pi_1 - a\pi_1)^d (1-\pi_1)^{D_p-d} \\
&\quad \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}\right] \\
&= (1-a)^{M-1}\left[1-(1-\pi_1)^{D_p}\right] - (1-a)^{M-1} \\
&\quad \left[(1-a\pi_1)^{D_p} - (1-\pi_1)^{D_p}\right] \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}\right] \\
&= (1-a)^{M-1}\left[1-(1-a\pi_1)^{D_p}\right] \\
&\times \left[\sum_{i=1}^{(N_R-1)^N} \prod_{j=1}^{N} \left[\left(1-p_{BER_{i,j}}\right)^T\right]^{n_{i,j}} \left[\left(p_{BER_{i,j}}\right)^T\right]^{N_R-1-n_{i,j}}\right].
\end{aligned} \tag{6.24}$$

Differentiating $p_s(a, D_f, D_p, M, N_R, p_{BER}, T)$ with respect to $a$ and equating it to zero, it results that $p_s$ is maximized at the value $a^*(D_p)$ which satisfies

$$D_p \pi_1 \left(1-a\right)\left(1-a\pi_1\right)^{D_p-1} = (M-1)\left[1-(1-a\pi_1)^{D_p}\right], \tag{6.25}$$

which can be solved numerically for $a$.

## 6.6 Simulation scenario

The network model used in this case is shown in Fig. 6.1. As in previous chapters, there is a broadcast area, where it is located the nodes that must receive the safety message to be transmitted and, they are located within a transmission range of 300 m, according to Table 6.1. There is an additional area called interference area, where are the nodes that could cause interference to any of the target nodes located inside the broadcast area, and it has a transmission range of 1.3 km. This is because all nodes have transmission range of 1 km and a node located within that limit can transmit at the same time as the broadcast node which cause collisions.

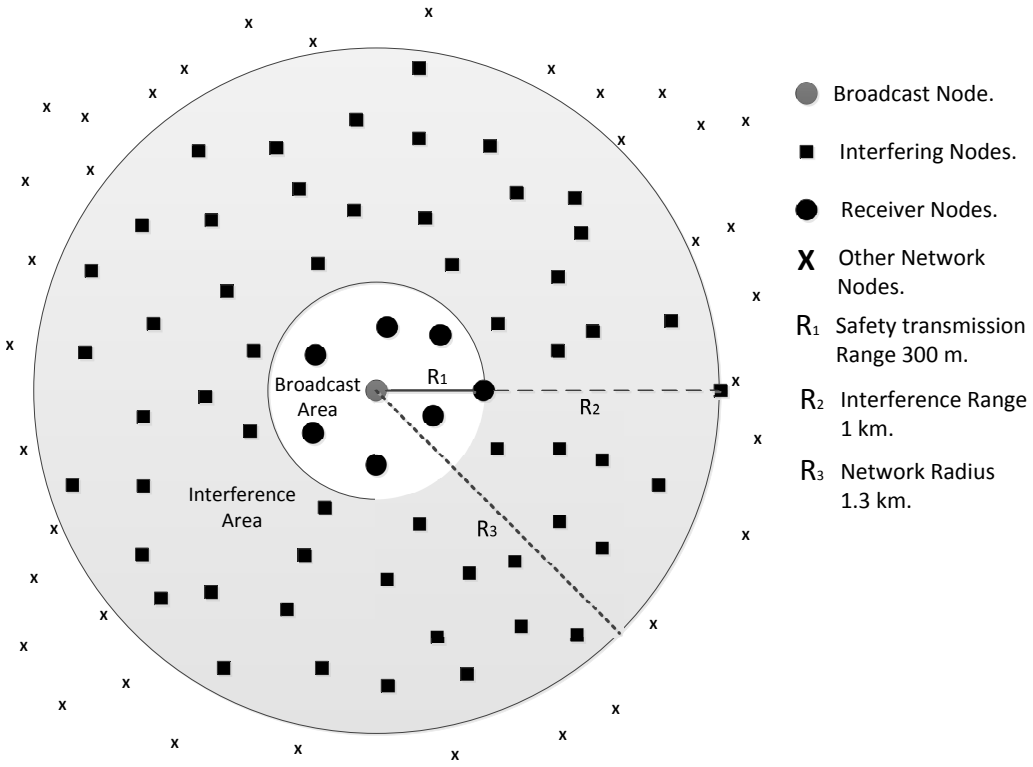



Figure 6.1: Simulation scenario for broadcast safety message transmission.

The main goal of Vehicular *ad hoc* Networks VANETS is to improve the safety of future transportation systems. VANETs provide a variety of safety applications and non-safety applications for more driving efficiency, comfort and safety. Safety applications have strict requirements on communication reliability and delay, whereas non safety applications are more throughput sensitive instead of delay sensitive. The requirements for different applications are shown in Table. 6.1.

Table 6.2 contains the parameters for physical and MAC layer used in the standard IEEE 1609 WAVE Wireless Access for Vehicular Environments, that are used for transmission of safety message. We adopt these parameters in order to make our numerical analysis based on some realistic scenarios.

We use the simplified path loss model, shown in Section 3.10, assuming a path loss exponent of 4 for our evaluations, which it is the worst case, for the calculation of the bit error probability $p_{BER}$. In [62], the Nakagami parameter $m$ has been estimated based on empirical measurements

Table 6.1: VANETs Safety Requirements [5],[6] and [7].

| **Applications** | **Latency (ms)** | **Application Range (m)** | **Priority** |
|---|---|---|---|
| Intersection Collision Warning | 100 | 300 | Safety of Life |
| Cooperation Collision Warning | 100 | 50 - 300 | Safety of Life |
| Intersection Collision Avoidance | 100 | 300 | Safety of Life |
| Work Zone Warning | 1000 | 300 | Safety |
| Transit Vehicle Signal Priority | 1000 | 300 - 1000 | Safety |
| Service Announcements | 500 | 0 - 90 | Non-safety |
| Movie Download | N.A. | 0 - 1000 | Non-safety |

Table 6.2: PHY and MAC parameters for the Wave Short Message (WSM) in IEEE 802.11p [13].

| **Physical and MAC layer parameters: 802.11p** | |
|---|---|
| Data Rate $R_{T_x}$ | 3 - 6 Mbps |
| Message Size | 50 - 200 Bytes |
| Transmit Power | 33 dBm |
| Minimum Rx Threshold | -85 dBm |
| Transmission Range | 300 m |
| Maximum Delay | 100 ms |
| Frequency | 5.9 Ghz |
| Band | 10 Mhz |
| Antenna Gain | 4 dBi |
| Modulation | BPSK |

for a vehicle-to-vehicle link in a highway as it was mentioned in Chapter 3, and the values in Eq. (6.5). Fig. 6.2 shows how the nodes were distributed in uniformly on the streets, first using a map from *Google Maps*. Similar to previous chapter, there are two areas: the broadcast area, with $R_1 = 300$ m where it is located the target receiver nodes and the interference area with $R_3 = 1.3$ km where all the interference nodes are.

### 6.6.1 Numerical results

In this part of the work, some important results are presented in order to evaluate the performance of the proposed model. The parameters used are the proposed by IEEE 802.11p [13] and IEEE 1609 [58] for emergency safety messages. The performance of our model is evaluated with the successful delivery probability $p_s$ as a function of the final deadline $D_f$ and total number of users presents in the system $M = N_R + N_H$. Other important parameters as message size $T$ and signal noise ration SNR are also presented as function of $p_s$. The main idea is to evaluate that the two criteria of $p_s > 99.9\%$ in a final deadline $D_f$ of 100 ms will be accomplished. The four cases analyzed in Chapter 5, Non-periodic with and without fading, Geometric and Multinomial cases are also presented here to compare between the different proposed schemes. The nodes are uniformly distributed, because of this, the simulations were done 10 times varying topology, and

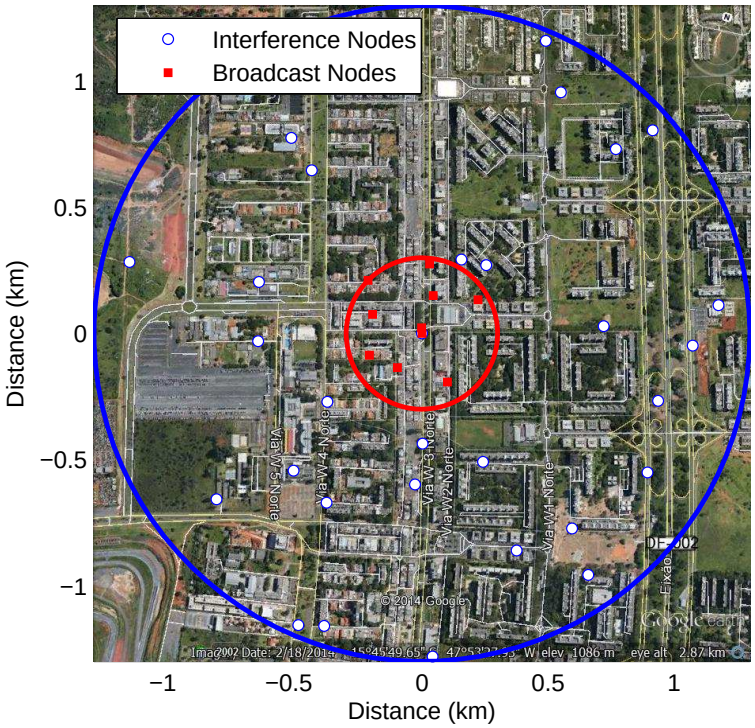



Figure 6.2: Nodes Distribution - Broadcast Nodes $N_R = 10$ and Inteference Nodes $N_H = 30$.

the mean value were used for the graphics.

Fig. 6.3 illustrates the reception power in dBm for one node, at different distances up to 300 m. The power falls quickly with distance in the first 50 meters, however, it can be seen that it does not reach the limit of reception threshold set by the IEEE 802.11p of -85dBm. This is mainly because the transmission power is high and the antenna gain has also a significant value, in addition to the fact that the further distance is only 300 m, which makes the reception power to not fall significantly, and as we shall see in the next figures, the combination of high power and low noise makes the probability of failure to not be a big value. It is important to note that Fig. 6.3 shows just the model for signal propagation without fading channel, with that, the received power may be lower.

Fig. 6.4 illustrates the successful delivery probability $p_s$ as function of the final deadline $D_f$. We consider 40 nodes in the system, where 10 nodes are inside the broadcast area and 30 nodes in the interference area. The size of the message $T = 50$ bytes and a transmission rate of 3 Mbps were assumed. Also there are not PUs present in the channel. The difference among the non-periodic case with and without fading, at the value of $D_f = 100$ there is a difference of 0.008 of $p_s$, what indicate, for the parameters used, that the probability of failure $p_f$ is lower than 0.1 that was assumed in previous chapter. Another important thing to note, it is that there is a difference between the geometric and the multinomial case, as in previous section, since the multinomial case shows a better performance than the geometric one, in terms of $p_s$, due to not assume that all nodes must receive the message in the same $D_p$. It is possible to observe that for the multinomial

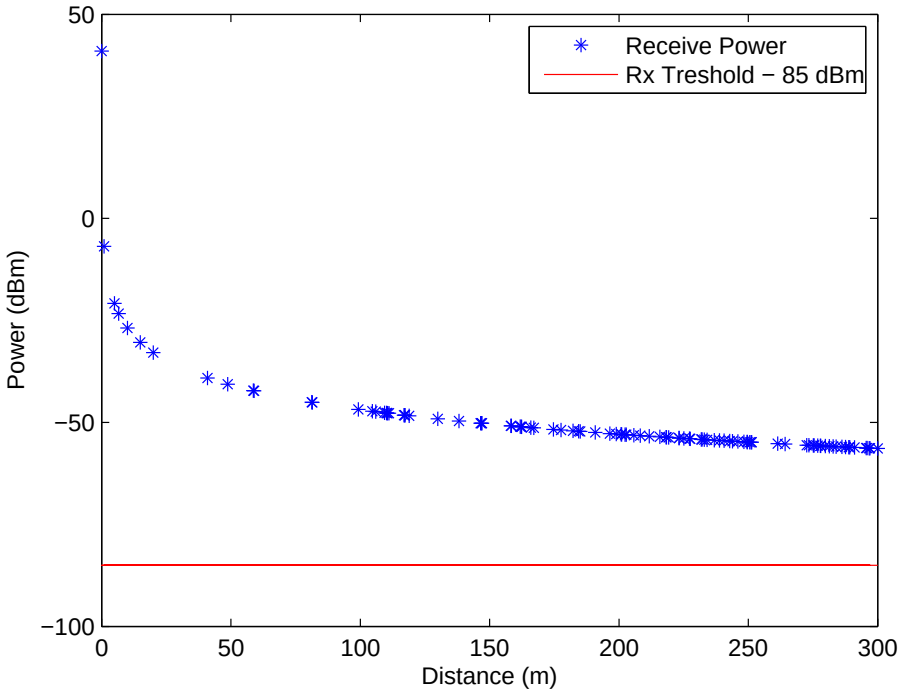



Figure 6.3: Power (dBm) as function of distance $d$.

and geometric cases it is possible to get a value of successful delivery probability $p_s$ greater than 99.9 % in 100 ms, which meets the requirements established for a reliable transmission in broadcast safety messages. Fig. 6.5 uses the same parameters as Fig. 6.4, except for the size of the message, that in this case is 200 bytes. In this figure it is possible to see the impact of the message size $T$; with an increase of it, there is a reduction in the successful delivery probability $p_s$ of 18.1%, in $D_f = 100$, with respect to the observed in Fig. 6.4. In this case it is not possible to reach the $p_s$ greater than 99.9 % in 100 ms. To obtain that value we need to increment the final deadline $D_f$, which does not satisfy the safety message requirements.

Fig. 6.6 presents the successful delivery probability $p_s$ as function of final deadline $D_f$; in this case we increment the transmission rate from 3 to 6 Mbps. There are 40 nodes in the system, as in previous figures and following recent literature [16], [30], [20], [63], [15] and the message size is 50 bytes. It is possible to see how, for geometric and multinomial cases, is possible to reach a successful delivery probability $p_s$ with values greater than 99.9% in 100 ms. In fact, for the geometric case $p_s = 99.9\%$ is reached in 70.6 ms and for the multinomial case in 46.7 ms, this because if we increment the transmission rate we are making available more slots in 100 ms; therefore, there is an increment in successful delivery probability $p_s$. Fig. 6.7 maintained the same parameters as in Fig. 6.6, but the message size is incremented from 50 to 100 bytes. In this case, the multinomial scheme can accomplish values of $p_s$ greater than 99.9% while the geometric case is near with $p_s = 99.3\%$ in 100 ms. Finally in Fig. 6.8 a message size of 200 bytes is used in the simulation, and in any case were not attained the value of $p_s$ required by the regulations. Comparing Figs. 6.6, 6.7 and 6.8, with Figs. 6.4 and 6.5 there is an improvement of the performance of the successful

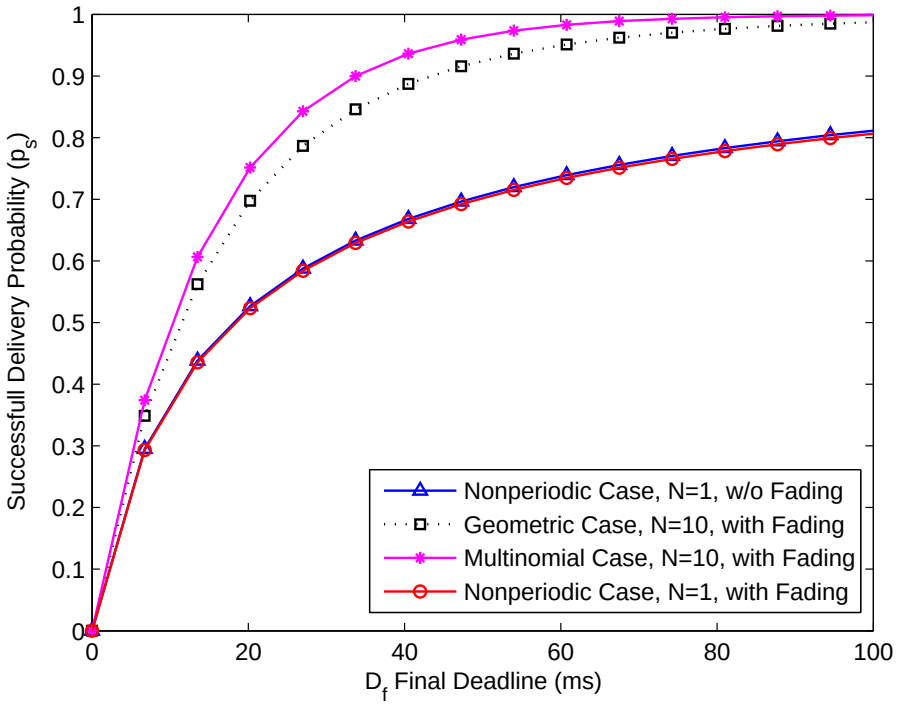



Figure 6.4: Successful delivery probability as a function of $D_f$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, $R_{T_x} = 3$ Mbps.

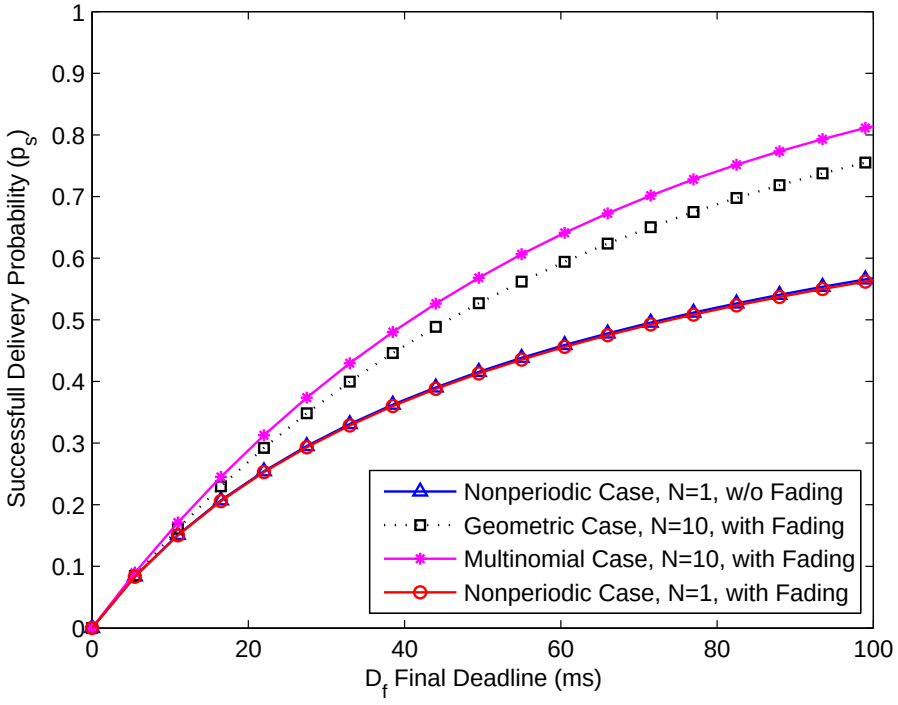



Figure 6.5: Successful delivery probability as a function of $D_f$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=200 Bytes, $R_{T_x} = 3$ Mbps.

deliver probability $p_s$ when the transmission rate is increased, in which $R_{T_x} = 6$ Mbps presents better results although the error rate could be higher.

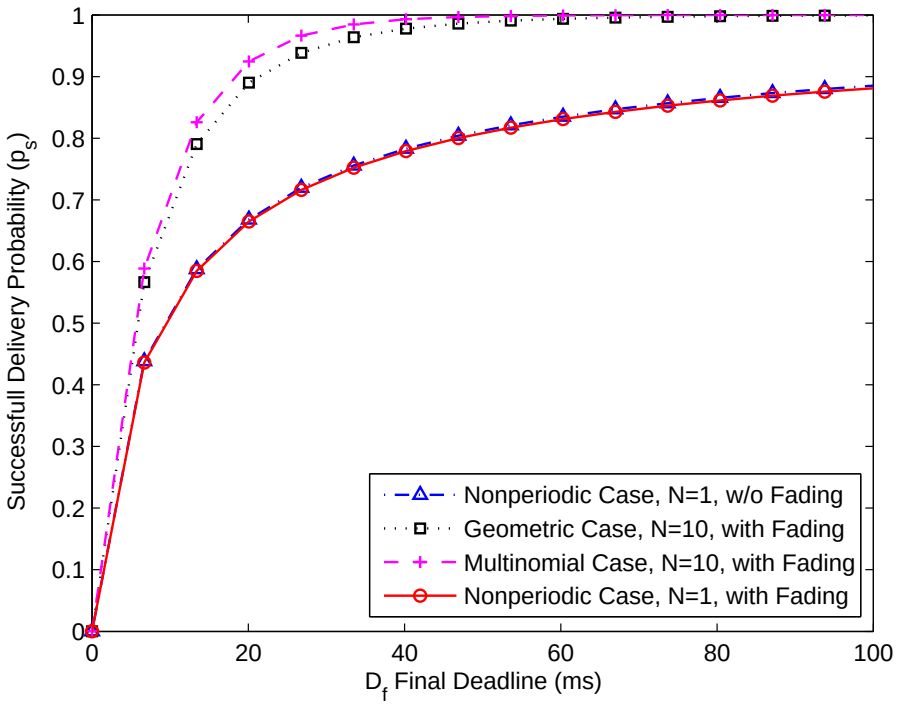



Figure 6.6: Successful delivery probability as a function of $D_f$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, $R_{T_x} = 6$ Mbps.

Fig. 6.9 illustrates the successful delivery probability $p_s$ as function of the number users $M$. In this case, a final deadline $D_f$ of 100 ms, a message size $T$ of 50 bytes and a transmission rate $R_{T_x}$ of 6 Mbps is used as parameters for the simulation. In this figure it is possible to see how the proposed model works well for few numbers of users, for 41 and 48 users for geometric and multinomial case respectively, it is possible to obtain a successful delivery probability $p_s$ of 99.9% in 100 ms. In this case just 10 attempts to send the message were employed. One thing that could be done to improve the probability of success with a higher quantity of nodes is to rebroadcast more times or increment the final deadline $D_f$. Also it is possible to see that for case where there is no repetition of the message, the non-periodic cases, it is not possible to get values of $p_s$ greater than 99.9% in 100 ms, what confirms that the repetition model improve significantly the performance of the system.

Fig. 6.10 shows the successful delivery probability $p_s$ as function of the total number of users $M = N_R + N_H$. This figure is done for the multinomial case, which has proven to be the best case for transmission of safety message. In this simulation there is primary user PU occupying the channel with probability $\pi_1$, a message size $T$ of 50 bytes, a final deadline $D_f$=100 ms and a transmission rate $R_{T_x}$ of 3 Mbps was assumed. In this case, there are $M$ equal to 5, 12, 18 and 23 nodes which can receive successfully in $D_f$=100 ms with $p_s$ greater than 99.9%, for $\pi_1$=0.2, $\pi_1$=0.5, $\pi_1$=0.8 and $\pi_1$=1, respectively. Fig. 6.11 has the same parameter as Fig. 6.10, but the

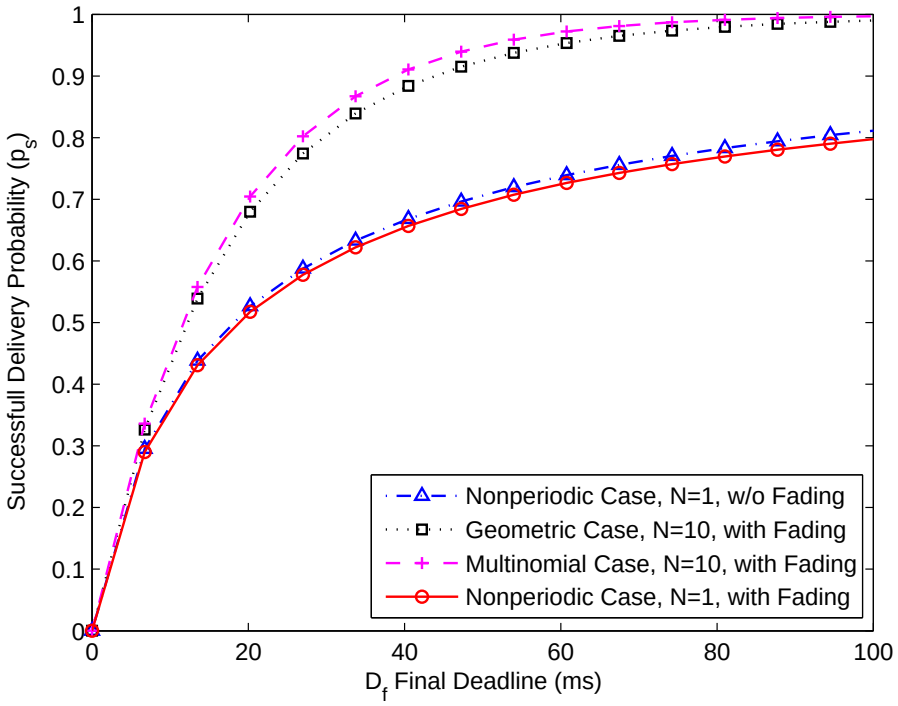



Figure 6.7: Successful delivery probability as a function of $D_f$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=100 Bytes, $R_{T_x} = 6$ Mbps.

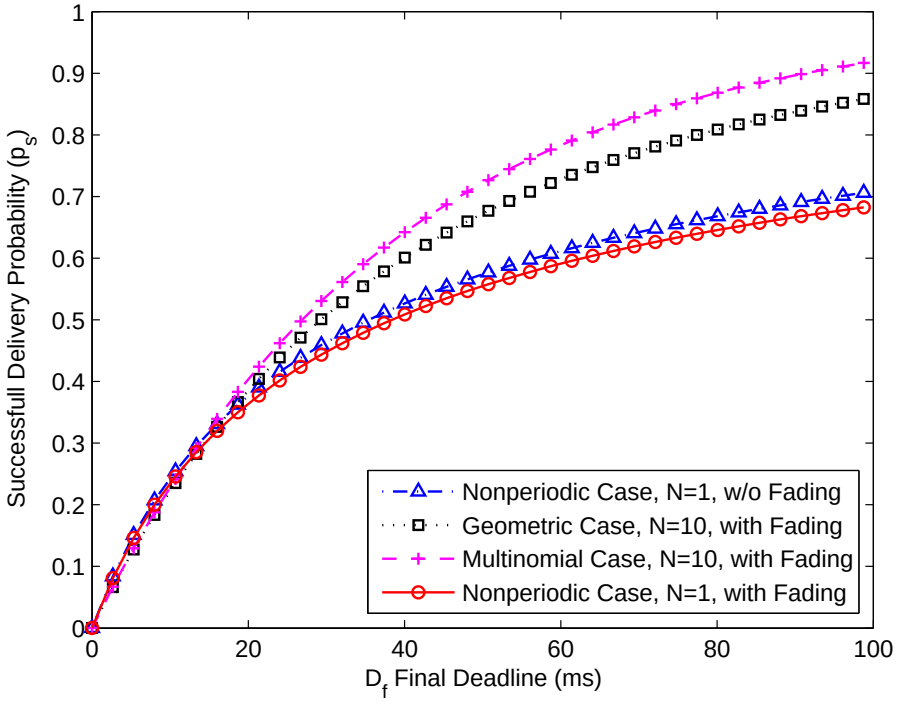



Figure 6.8: Successful delivery probability as a function of $D_f$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=200 Bytes, $R_{T_x} = 6$ Mbps.

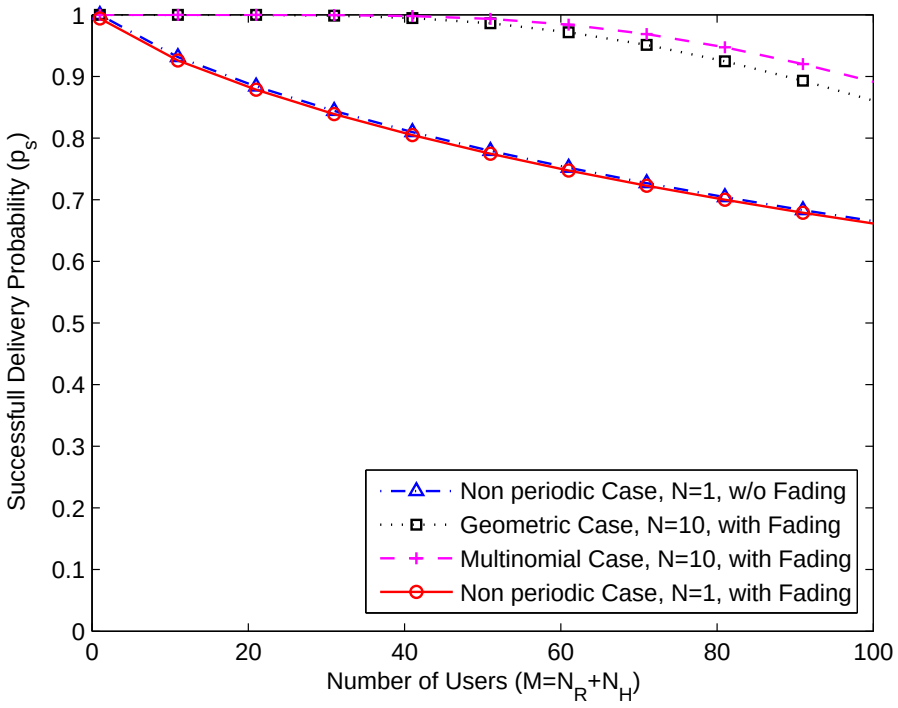



Figure 6.9: Successful delivery probability as a function of $M$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes.

transmission rate is modified from 3 to 6 Mbps. It is possible to observe that there is an increment of the number of nodes that successfully received the message. For $M$ equal to 10, 23, 33 and 40 nodes for $D_f$=100 ms $p_s$ is greater than 99.9%. Comparing the Figs. 6.10 and 6.10 we can concluded that by using the proposed scheme, it is possible to obtain values of successful delivery probability $p_s$ greater than 99.9% for a final deadline $D_f$ of 100 ms, meeting the requirements of safety message in VANETs, even though PUs are present in the system.

Figs. 6.12 and 6.13 illustrate the probability of success $p_s$ as function of distance for multinomial case. The number of nodes $M$ are 40 and the final deadline $D_f$ is 100 ms. Fig. 6.12 showS the performance of the successful delivery probability in the case the message size $T$ is 200 bytes.

The distance between vehicles is a very important parameter for safety message in VANETS. There is a range of 300 m, from the transmitter node, in which all the vehicles must receive the message. In Figs. 6.12 and 6.13 it can be seen the probability of success $p_s$ as a function of distance. In Fig. 6.12 a message size of 50 bytes, and a transmission rate of 3 Mbps are considered, while in Fig. 6.13 it is assumed a transmission rate of 6 Mbps. It is possible to see how $p_s$ decrease with distance $d$ and increase with the number of attempts $N$. In Fig. 6.12 it is possible to see that just in the case of $N$=10 attempts it is possible to observe probability of success greater than 99.9% until 98 m. After that distances, $p_s$ decreases to values not acceptable for safety message transmission.

Te message size is another important parameter in our model, depending of it, the probability

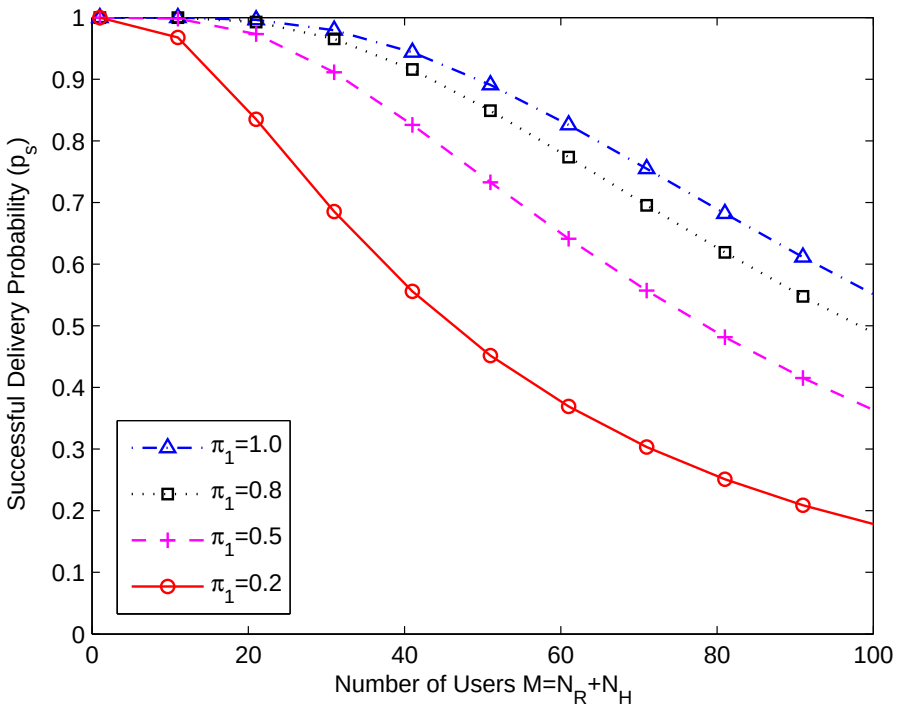



Figure 6.10: Successful delivery probability as a function of $M$, with fading, $0 < \pi_1 < 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, transmission rate $R_{T_x} = 3$ Mbps, multinomial case.

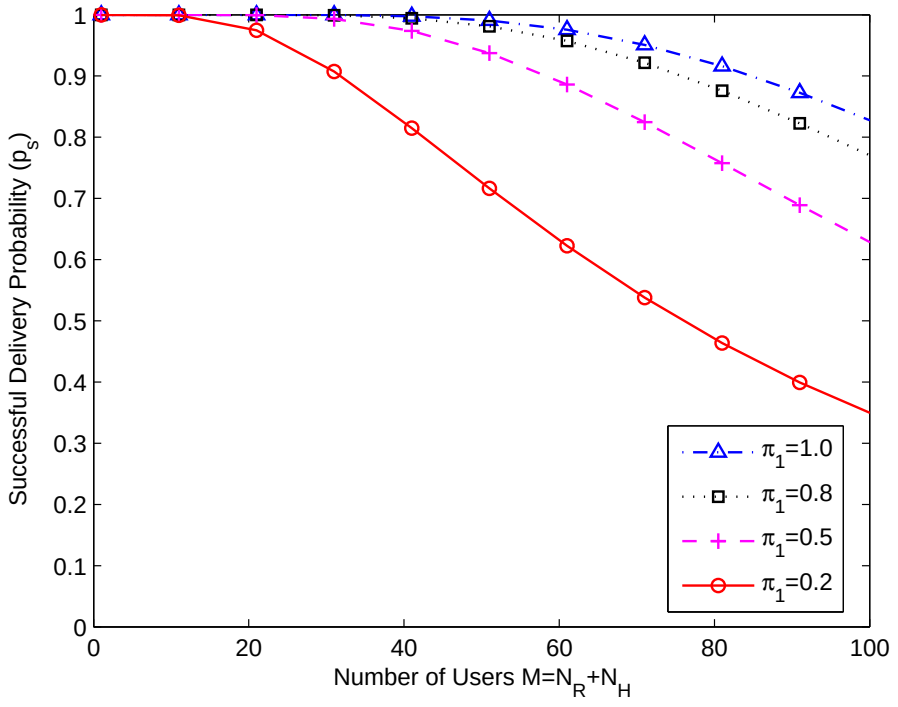



Figure 6.11: Successful delivery probability as a function of $M$, with fading, $0 < \pi_1 < 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, transmission rate $R_{T_x} = 3$ Mbps, multinomial case.

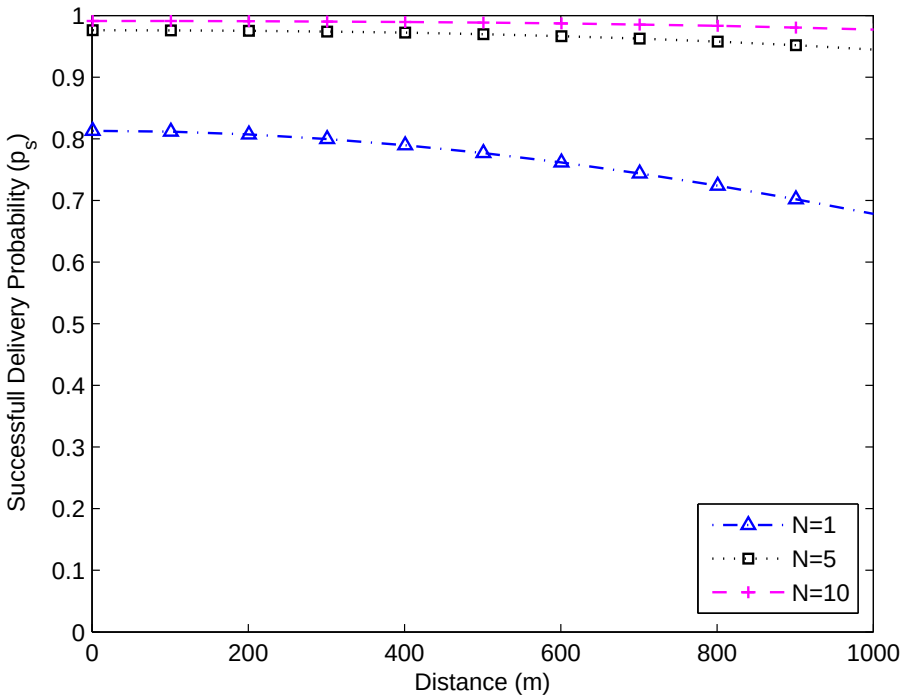



Figure 6.12: Successful delivery probability as a function of distance $d$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, $D_f = 100$ ms, $R_{T_x} = 3$ Mbps , multinomial case.

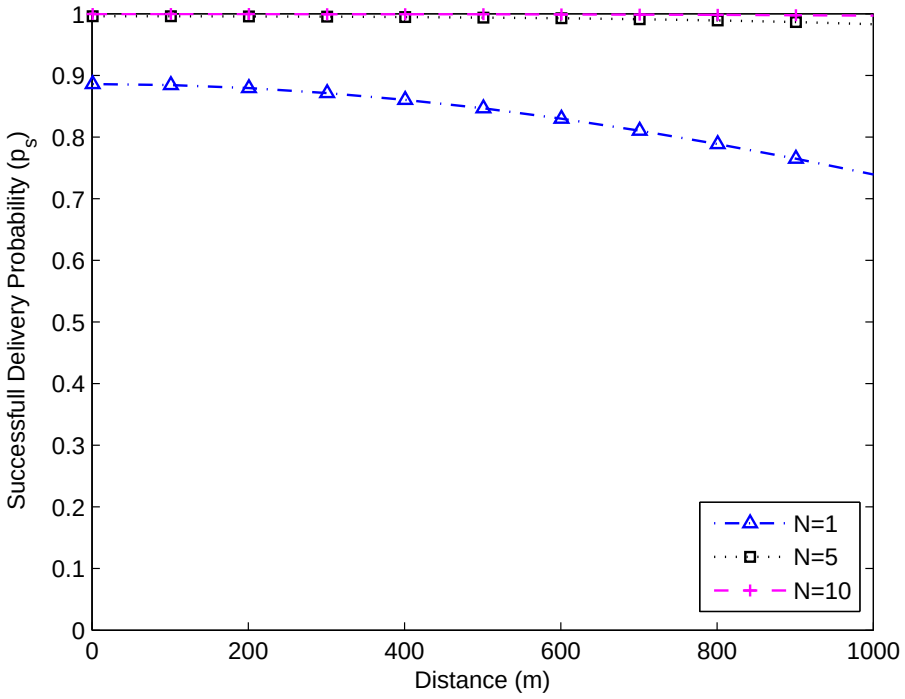



Figure 6.13: Successful delivery probability as a function of distance $d$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 30$, $T$=50 Bytes, $D_f = 100$ ms, $R_{T_x} = 6$ Mbps, multinomial case.

of success can reach values greater than 99.9% in 100 ms. Fig. 6.14 presents the probability of success $p_s$ as function of the message size $T$ for the multinomial case. The final deadline $D_f$ is 100 ms, there are 40 nodes presents in the system, and the transmission rate is 6 Mbps. Here we can see that for $N = 10$ i.e., 10 attempts, it is possible to obtain a probability of success of 99.9% for message size lower than 220 bytes in 100 ms. For 5 attempts that number is reduced to 60 bytes. This figure also shows that the proposed model with re-transmission of the broadcast message improves the successful delivery probability $p_s$; although, if the message is transmitted more times, the size of it must be reduced.

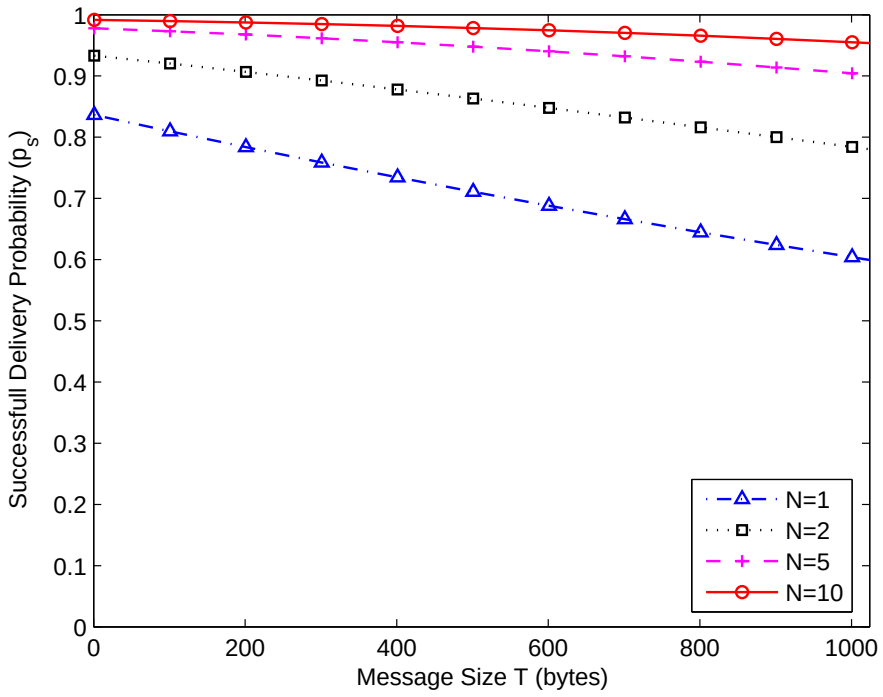



Figure 6.14: Successful delivery probability as a function of message size $T$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 40$ and $D_f = 100$ ms.

Finally, Fig. 6.15 shows the probability of failure as function of the Signal to Noise ratio (SNR), it can be seen that with the increase of the SNR there is a decrease in probability of failure $p_f$, that is because there is a rise of the transmission power and a decrease of the noise. It is also important to note that with the increase of the message size $T$, there is a increase of the probability of failure as indicated in Eq. (6.1). With the values of SNR calculated from the IEEE 801.11p the probability of failure does not reach large values and that is why we have small values of $p_f$.

## 6.7 Conclusion

In this chapter, it is shown the analysis of the scheme proposed using the parameters of the IEEE 1609 and 802.11p, incorporating to the probability term the fading channel impact, in a Nakagami-m fading channel. The protocol is evaluated to study if the parameters of reliability

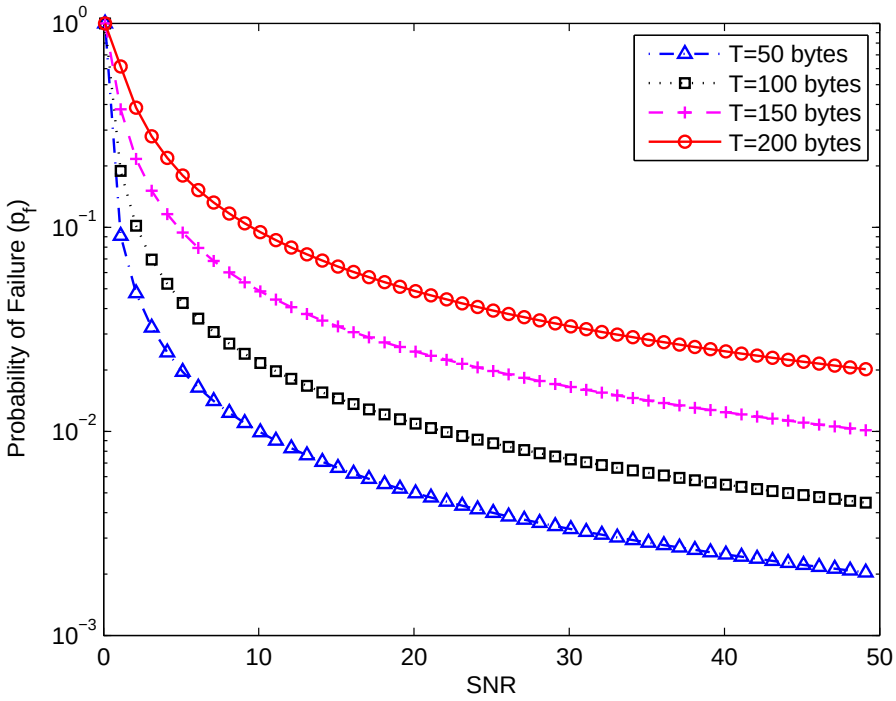



Figure 6.15: Probability of failure as a function of SNR, varying the message size $T$, with fading, $\pi_1 = 1$, $N_R = 10$, $N_H = 40$ and $D_f = 100$ ms.

proposed by regulations for probability of success of 99.9% and final deadline of 100 ms could be fulfilled. It is shown that our proposal works properly until an acceptable number of nodes, and varying the parameters, it is possible to meet the reliability requirements. It is also shown that the probability of success decrease with the increase of the size of the message $T$ and with the increase of the distance $d$ of the receiver nodes with respect to the transmitter node. Finally, our idea of repeat the broadcast message, using the optimized access probability $a$, shows a better performance and it is possible to call it a reliable approach.

# Chapter 7

# Conclusions and Future Work

## 7.1 Conclusions

Development of schemes to guarantee reliability and an acceptable latency for collision avoidance systems, as well as other applications, requires an excellent designed mechanism of delivery with success, part of this in the medium access control MAC layer. Reliable data dissemination in vehicular networks has some limitations, mainly due to the characteristics of the wireless medium and the lack of synchronization, in which nodes typically move in a wide area surrounded of obstacles like buildings, mountains and other things that affect the propagation of the message. In this dissertation, our idea was to present an scheme to transmit broadcast messages in a reliable way in a vehicular environment, considering two issues: hidden terminals and fading channel.

A mathematical analysis has been developed to model the probability of success $p_s$ as a function of the number of the nodes in the network $M$, the final deadline $D_f$ and the probability of failure $p_f$ in a cognitive network. The optimal probability $a$ of message transmission was found and used to achieve high reliability. This work presents two schemes for rebroadcasting safety message in VANETs, in order to increase the successful delivery probability. The first one, assumed that all nodes must receive the message at the same partial deadline $D_p$, which was called geometric case, and the other one, with nodes receiving the message in different partial deadlines $D_p$, called multinomial case. The multinomial case has shown better performance in all simulations due the assumptions mentioned before, besides it is a more realistic approach because not all nodes should receive the message at the same attempt, but it does in others attempts, until the end of the final deadline $D_f$ to be considered successful.

The number of nodes is an important variable that should be taken into account in the proposed model, because it impacts directly the probability of success. Our approach show a good performance for a few quantity of nodes, less than 50. If there are a lot of nodes competing for the channel, the probability of success drops significantly because the protocol use is the Slotted-Aloha. It is important to note that the quantity of nodes also impacts the probability of failure $p_f$, the greater the number of nodes, the higher the probability of failure will be.

In Chapter 4 the term probability of failure $p_f$ was introduced to our analysis to represent

channel and receptions failures, that value was chosen arbitrarily. In Chapter 5, it was used the Nakagami channel model for the vehicle-to-vehicle communication link to represent channel failures. The simulations follow a realistic Nakagami channel model with parameters chosen from the IEEE 802.11p standard. Due to the high transmission power of the antennas used in vehicles, the SNR (Signal to noise ratio) is very high, which gives small failure probabilities, favoring the proposed model for transmission of emergency messages.

A model for a cognitive radio scheme using a Markov chain was used to represent the occupancy of the channel. Although a cognitive scheme is not so appropriated for a emergency message transmission, due to the time required to scan the channel and use it for transmission, which impacts directly the final deadline established by regulations, it was important to test our model. It was shown that with 50% of channel occupation by primary user it possible to obtain successful delivery probabilities $p_s$ higher than 99.9% in 100 ms, what makes it possible to use in safety message transmission.

The analysis presented in this work takes on a general approach and not only is applicable to safety broadcast message in VANETs, also it can be used for any repetition based broadcast protocol in which the probability of success is an important metric. The results shown in this work, analytically and numerically, reveal that a repetition approach can provide significant performance improvements over non-repetition broadcast schemes at cost of reduction in the size of the message. Numerical results presented in this work shown that our proposal of re-broadcasting, using Slotted Aloha, it is able to transmit safety messages under practical conditions. The propose model here shows promising performance and provides features required in a vehicular medium access control protocol.

The core of our design is to repeat the broadcast message and use the optimal probability of access to transmit the message which improves reliability for small safety messages. We studied how the safety message rebroadcasting can be used. If we variate some parameters, allowed by regulations, as message size or transmission rate, we can increase significantly the performance and reach a reliability of 99.9% and latency of 100 ms.

## 7.2 Future Work

The effects of mobility of the vehicles on the proposed protocol remain to be studied. There are some traces or mobility models especially for VANETS that are interesting to incorporate to the analysis. The use of acknowledgments was not considered. It would be very important to know if the message arrive to all destinations and to obtain a feedback from the receiver nodes to improve the repetition scheme. In this work, we use the Slotted-Aloha protocol. The use of another more efficient protocol as CSMA/CA, that is proposed by IEEE 1609, may be an interesting approach to improve reliability.

Several transmissions gives an opportunity for implementing network coding in a repetition based broadcast. In this scenario, messages from different users can be combined in each transmission to help to disseminate messages and can also provide path diversity for nodes whose line

of sight is blocked. Network coding in a vehicular network may offer increased reliability and efficiency but requires further study.

One important future work is to test the proposed model in network simulators, like NS-2, and real environments to test its performance. Other important thing to do in the future is to develop a multihop protocol to reach nodes outside the transmission range of the transmitter. Also to create a mechanism of communication among vehicles and roadside units to extend coverage and reliability is also an important future issue.

# Bibliography


[1] X. Ma, X. Yin, and K. S. Trivedi, "On the reliability of safety applications in VANETs," *International Journal of Performability Engineering*, vol. 8, no. 2, p. 115, 2012.

[2] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "DART: Dynamic address routing for scalable ad hoc and mesh networks," *Networking, IEEE/ACM Transactions on*, vol. 15, no. 1, pp. 119–132, Feb 2007.

[3] N. H. T. S. Administration *et al.*, "US department of transportation," *Traffic safety facts*, vol. 2, 1999.

[4] E. Zaloshnja and T. R. Miller, "Costs of crashes in the united states," *Accident Analysis & Prevention*, vol. 36, no. 5, pp. 801–808, 2004.

[5] J. Zhang, "A survey on trust management for VANETs," *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, pp. 105–112, 2011.

[6] C. Perkins, E. Royer, S. Das, and M. Marina, "Performance comparison of two on demand routing protocols for ad hoc networks," *Personal Communications, IEEE*, vol. 8, no. 1, pp. 16–28, Feb 2001.

[7] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless networks*, vol. 8, no. 5, pp. 481–494, 2002.

[8] E.-S. Jung and N. H. Vaidya, "A power control MAC protocol for ad hoc networks," *Proceedings of the 8th annual international conference on Mobile computing and networking*, pp. 36–47, 2002.

[9] M. Xiaomin, Y. Xiaoyan, and K. S. Trivedi, "Performance of VANET safety message broadcast at rural intersections," in *Proc. of IWCMC*, June 2013.

[10] M. Khabazian, S. Aissa, and M. M. Ali, "Performance modeling of safety messages broadcast in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 380–387, 2013.

[11] M. Xiaomin, J. Zhang, Y. X. Yin, and K. S. Trivedi, "Design and analysis of a robust broadcast scheme for VANET safety related services," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 46–61, 2012.

[12] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, 2007.

[13] *IEEE P802.11p/D9.0*, 2009, draft standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements: Wireless access in vehicular environments.

[14] C. Campolo, A. Vinel, A. Molinaro, and Y. Koucheryavy, "Modeling broadcasting in IEEE 802.11p/WAVE vehicular networks," *IEEE Communications Letters*, vol. 15, no. 2, pp. 199–201, 2011.

[15] H. Cheng and Y. Yamao, "Reliable inter vehicle broadcast communication with sectorized roadside relay station," in *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*, June 2013, pp. 1–5.

[16] Y. H. Bae, "Analysis of optimal random access for broadcasting with deadline in cognitive radio networks," *IEEE Communications Letters*, vol. 17, no. 3, pp. 573–575, 2013.

[17] B. Xu, A. Ouksel, and O. Wolfson, "Opportunistic resource exchange in inter vehicle ad hoc networks," in *Mobile Data Management, 2004. Proceedings. 2004 IEEE International Conference on.* IEEE, 2004, pp. 4–12.

[18] Y. P. Fallah, C. L. Huang, R. Sengupta, and H. Krishnan, "Analysis of information dissemination in vehicular ad hoc networks with application to cooperative vehicle safety systems," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 1, pp. 233–247, 2011.

[19] J. C. Montealegre, M. M. Carvalho, and R. M. de Moraes, "Deadline-constrained optimal broadcasting under hidden terminals in cognitive networks," in *Proceedings of the Latin America Networking Conference on LANC 2014.* ACM, 2014, p. 13.

[20] B. Hassanabadi and S. Valaee, "Reliable periodic safety message broadcasting in VANETs using network coding," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 3, pp. 1284–1297, March 2014.

[21] S. Hassanabadi, B Valaee, "Reliable periodic safety message broadcasting in VANETs using network coding," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 3, pp. 1284–1297, March 2014.

[22] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *Vehicular Technology Magazine, IEEE*, vol. 2, no. 2, pp. 12–22, 2007.

[23] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 3, pp. 74–88, 2008.

[24] S. Sibecas, C. A. Corral, S. Emami, and G. Stratis, "On the suitability of 802.11 for high mobility DSRC," in *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, vol. 1. IEEE, 2002, pp. 229–234.

[25] ASTM, "E2213 03, standard specification for telecommunications and information exchange between roadside and vehicle systems 5 ghz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications."

[26] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 584–616, 2011.

[27] S. Tsugawa, M. Aoki, A. Hosaka, and K. Seki, "A survey of present IVHS activities in Japan," *Control Engineering Practice*, vol. 5, no. 11, pp. 1591–1597, 1997.

[28] S. Grafling, P. Mahonen, and J. Riihijarvi, "Performance evaluation of IEEE 1609 wave and IEEE 802.11 p for vehicular communications," in *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on.* IEEE, 2010, pp. 344–348.

[29] B. Katrin, U. Elisabeth, S. Erik G, B. Urban *et al.*, "On the ability of the 802.11 p MAC method and STDMA to support real time vehicle to vehicle communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[30] A. J. Ghandour, M. Di Felice, H. Artail, and L. Bononi, "Dissemination of safety messages in IEEE 802.11 p/wave vehicular network: analytical study and protocol enhancements," *Pervasive and Mobile Computing*, vol. 11, pp. 3–18, 2014.

[31] J. P. Thompson and C. D. Wang, "Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real time adaptive probabilistic neural network," 1997, US Patent 5,613,039.

[32] P. L. Olson and M. Sivak, "Perception response time to unexpected roadway hazards," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 28, no. 1, pp. 91–96, 1986.

[33] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle to vehicle wireless communication protocols for enhancing highway traffic safety," *Communications Magazine, IEEE*, vol. 44, no. 1, pp. 74–82, 2006.

[34] Department of Transportation USA, "Crash facts," accessed: 11-11-2014. [Online]. Available: http://safety.fhwa.dot.gov/intersection/

[35] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 3, pp. 74–88, 2008.

[36] A. S. Tanenbaum, *Computer Networks,* $4^{th}$ *Edition.* Prentice Hall, 2003.

[37] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11 based vehicular ad hoc networks," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.* ACM, 2004, pp. 10–18.

[38] M. Xiaomin, C. Xianbo, R. Hazem H *et al.*, "Performance and reliability of DSRC vehicular safety communication: a formal analysis," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[39] C. V. S. C. Consortium *et al.*, "Vehicle safety communications project task 3 final report, mar. 2005," *VANETs Magazine, CAMP*, vol. 02, no. 1, 2012.

[40] S. Oyama, "Vehicle safety communications: progresses in japan," in *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on.* IEEE, 2008, pp. 241–241.

[41] M. Green, "How long does it take to stop? methodological analysis of driver perception brake times," *Transportation human factors*, vol. 2, no. 3, pp. 195–216, 2000.

[42] K. Na Nakorn and K. Rojviboonchai, "Comparison of reliable broadcasting protocols for vehicular ad hoc networks," *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pp. 1168–1171, 2010.

[43] M. Torrent Moreno, S. Corroy, F. Schmidt-Eisenlohr, and H. Hartenstein, "IEEE 802.11 based one hop broadcast communications: understanding transmission success and failure under different radio propagation environments," in *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems.* ACM, 2006, pp. 68–77.

[44] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance evaluation of safety applications over DSRC vehicular ad hoc networks," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.* ACM, 2004, pp. 1–9.

[45] J. He, Z. Tang, T. O'Farrell, and T. M. Chen, "Performance analysis of DSRC priority mechanism for road safety applications in vehicular networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 980–990, 2011.

[46] K. Tang and M. Gerla, "MAC layer broadcast support in 802.11 wireless networks," in *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 1. IEEE, 2000, pp. 544–548.

[47] M. Gerla and K. Tang, "MAC reliable broadcast in ad hoc networks," in *Military Communications Conference, 2001. MILCOM 2001. Communications for Network Centric Operations: Creating the Information Force. IEEE*, vol. 2. IEEE, 2001, pp. 1008–1013.

[48] M. t. Sun, L. Huang, S. Wang, A. Arora, and T.-H. Lai, "Reliable MAC layer multicast in IEEE 802.11 wireless networks," *Wireless Communications and Mobile Computing*, vol. 3, no. 4, pp. 439–453, 2003.

[49] M.-T. Sun, W.-C. Feng, T.-H. Lai, K. Yamada, H. Okada, and K. Fujimura, "Gps based message broadcast for adaptive intervehicle communications," in *Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd*, vol. 6. IEEE, 2000, pp. 2685–2692.

[50] G. Korkmaz, E. Ekici, and F. Ozguner, "Black burst based multihop broadcast protocols for vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 5, pp. 3159–3167, 2007.

[51] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle to vehicle safety messaging in DSRC," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.* ACM, 2004, pp. 19–28.

[52] A. Goldsmith, *Wireless communications.* Cambridge university press, 2005.

[53] S. M. Proakis John G., *Digital communications.* McGraw-Hill, 2007.

[54] J. Yin, G. Holland, T. Elbatt, F. Bai, and H. Krishnan, "DSRC channel fading analysis from empirical measurement," *Communications and Networking in China, 2006. ChinaCom'06. First International Conference on*, pp. 1–5, 2006.

[55] M. Nakagami, "The m distribution a general formula of intensity distribution of rapid fading," *Statistical Method of Radio Propagation*, 1960.

[56] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta, "Empirical determination of channel characteristics for DSRC vehicle to vehicle communication," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks.* ACM, 2004, pp. 88–88.

[57] A. F. Molisch, F. Tufvesson, J. Karedal, and C. F. Mecklenbrauker, "A survey on vehicle to vehicle propagation channels," *Wireless Communications, IEEE*, vol. 16, no. 6, pp. 12–22, 2009.

[58] *IEEE 1609 WAVE Wireless Access for Vehicular Enviroments*, 2012.

[59] L. G. Roberts, "ALOHA packet system with and without slots and capture," *ACM SIGCOMM Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975.

[60] Z. Qing, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 589–600, 2007.

[61] B. Hassanabadi, L. Zhang, and S. Valaee, "Index coded repetition based MAC in vehicular ad hoc networks," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE.* IEEE, 2009, pp. 1–6.

[62] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in ns 2," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems.* ACM, 2007, pp. 159–168.

[63] D. N. M. Dang, H. N. Dang, V. Nguyen, Z. Htike, and C. S. Hong, "HERMAC A Hybrid Efficient and Reliable MAC for Vehicular Ad Hoc Networks," *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, pp. 186–193, May 2014.

# Appendix A

# Mathematical Expressions

## A.1 Differentiation with respect to $a$ Geometric Case 1

From Eq. (5.16), differentiate by $a$, we have that

$$\frac{dp_s}{da} = \frac{d}{da}\left(1 - \left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^N\right) \tag{A.1}$$

$$= \frac{d}{da} - \frac{d}{da}\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^N$$

$$= -\frac{d}{da}\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^N$$

$$= -\frac{d}{da}N\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)$$
$$\left(\left((1-a)^{D} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^{N-1}$$

$$= \frac{d}{da}N(1-p_f)^{N_R-1}\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}\right)$$
$$\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^{N-1} - \frac{d}{da}$$

$$= -N(1-p_f)^{N_R-1}\frac{d}{da}\left(\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}\right)\right)$$
$$\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1} + 1\right)^{N-1}$$

$$= \frac{d}{da}N\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}\left(\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}\right. \tag{A.2}$$
$$\left.(1-p_f)^{N_R-1} + 1\right)^{N-1} - \frac{d}{da}\left((1-a)^{D_p} - 1\right)(1-a)^{M-1}$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(\frac{d}{da}(1-a)^{D_p}(1-a)^{M-1}+\frac{d}{da}\left((1-a)^{D_p}-1\right)\left(d(1-a)^{M-1}\right)-\frac{d}{da}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(\frac{d}{da}(1-a)^{M-1}\left((1-a)^{D_p}\right)+\left((1-a)^{D_p}-1\right)\left(\frac{d}{da}(1-a)^{M-1}\right)\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left((1-a)\frac{d}{da}D_p(1-a)^{D_p-1}(1-a)^{M-1}+\left((1-a)^{D_p}-1\right)\left(\frac{d}{da}(1-a)^{M-1}\right)\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(D_p((1-a)\frac{d}{da})(1-a)^{D_p+M-2}+\left((1-a)^{D_p}-1\right)\left(\frac{d}{da}(1-a)^{M-1}\right)\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(-\frac{a}{da}dD_p(1-a)^{D_p+M-2}+\left((1-a)^{D_p}-1\right)\left(\frac{d}{da}(1-a)^{M-1}\right)+\frac{d}{da}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(\left((1-a)^{D_p}-1\right)\left(\frac{d}{da}(1-a)^{M-1}\right)-D_pa\frac{d}{da}(1-a)^{D_p+M-2}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left((1-a)\frac{d}{da}(M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2}-D_pa\frac{d}{da}(1-a)^{D_p+M-2}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Bigg(N(1-p_f)^{N_R-1}\left(-a\frac{d}{da}(M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2}-D_pa\frac{d}{da}(1-a)^{D_p+M-2}+\frac{d}{da}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Bigg)$$

$$= -\Big(N(1-p_f)^{N_R-1}\Big(-(M-1)a\frac{d}{da}\left((1-a)^{D_p}-1\right)(1-a)^{M-2} - D_p a\frac{d}{da}(1-a)^{D_p+M-2}\Big)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Big)$$

Finally the derivative of $p_s$ with respect to $a$ is

$$\frac{d}{da}p_s(a,D_p,M) = -\big(N(1-p_f)^{N_R-1}\left((M-1)\left(-\left((1-a)^{D_p}-1\right)\right)(1-a)^{M-2} - D_p(1-a)^{D_p+M-2}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}\Big) \tag{A.3}$$

Rearranging the expression we obtain that

$$\frac{d}{da}p_s(a,D_p,M,N_R,p_f) = (1-p_f)^{N_R-1}\left((M-1)\left((1-a)^{D_p}-1\right)(1-a)^{M-2} + D_p(1-a)^{D_p+M-2}\right)$$
$$\left(\left((1-a)^{D_p}-1\right)(1-a)^{M-1}(1-p_f)^{N_R-1}+1\right)^{N-1}. \tag{A.4}$$

## A.2 Differentiation with respect to $a$ Geometric Case 2

From Eq. (5.26), differentiate by $a$, we have that

$$\frac{d}{da}p_s(a,D_p,M) = \frac{d}{da} - \frac{d}{da}\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^N \tag{A.5}$$

$$= -\frac{d}{da}(1-(1-a)^{(-1+M)}(1-p)^{(-1+M)}(1-(1-a\pi_1)^{D_p}))^N$$

$$= -\frac{d}{da}N\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)$$
$$\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= -\frac{d}{da} - \frac{d}{da}N(1-p_f)^{N_R-1}\left((1-a)^{M-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)$$
$$\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\frac{d}{da}\left(\left((1-a)^{M-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= \frac{d}{da}N(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}+\frac{d}{da}(1-a)^{M-1}\left(1-(1-a\pi_1)^{D_p}\right)$$

$$= N(1-p_f)^{N_R-1}\left((1-a)^{M-1}\left(\frac{d}{da}\left(1-(1-a\pi_1)^{D_p}\right)\right)+(1-a)\frac{d}{da}(M-1)(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left(-a\frac{d}{da}(M-1)(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)+(1-a)^{M-1}\left(\frac{d}{da}\left(1-(1-a\pi_1)^{D_p}\right)\right)+\frac{d}{da}\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left((1-a)^{M-1}\left(\frac{d}{da}\left(1-(1-a\pi_1)^{D_p}\right)\right)-(M-1)a\frac{d}{da}(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left(-\frac{d}{da}(1-a)^{M-1}(1-a\pi_1)^{D_p}-(M-1)(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)+\frac{d}{da}\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left(-(1-a)^{M-1}\left(\frac{d}{da}(1-a\pi_1)^{D_p}\right)-(M-1)(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left(-\frac{d}{da}D_p(1-a)^{M-1}(1-a\pi_1)(1-a\pi_1)^{D_p-1}-(M-1)(1-a)^{M-2}\left(1-(1-a\pi_1)^{D_p}\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

$$= N(1-p_f)^{N_R-1}\left(-a\frac{d}{da}D_p\pi_1(1-a)^{M-1}(1-a\pi_1)^{D_p-1} - (M-1)(1-a)^{M-2}\right.$$
$$\left.\left(1-(1-a\pi_1)^{D_p}\right) - \frac{d}{da}\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1}$$

Finally the derivative of $p_s$ with respect to $a$ is

$$\frac{d}{da}p_s(a,D_p,M,N_R,p_f) = N(1-p_f)^{N_R-1}\left(D_p\pi_1(1-a)^{M-1}(1-a\pi_1)^{D_p-1} - (M-1)(1-a)^{M-2}\right.$$
$$\left.\left(1-(1-a\pi_1)^{D_p}\right)\right)\left(1-(1-a)^{M-1}(1-p_f)^{N_R-1}\left(1-(1-a\pi_1)^{D_p}\right)\right)^{N-1} \quad (A.6).$$

## A.3 Multinomial Cases

Table A.1: Distribution for 3 nodes $(a, b, c)$ and 3 slots $(1, 2, 3)$.

| | **Slots** | | |
|---|---|---|---|
| **Attempts** | **1** | **2** | **3** |
| **1** | a,b,c | 0 | 0 |
| **2** | 0 | a,b,c | 0 |
| **3** | 0 | 0 | a,b,c |
| **4** | a | b,c | 0 |
| **5** | a | 0 | b,c |
| **6** | 0 | b,c | a |
| **7** | 0 | a | b,c |
| **8** | b,c | 0 | a |
| **9** | b,c | a | 0 |
| **10** | b | 0 | c,a |
| **11** | b | c,a | b |
| **12** | 0 | b | c,a |
| **13** | 0 | c,a | 0 |
| **14** | c,a | 0 | b |
| **15** | c,a | b | 0 |
| **16** | c | 0 | b,a |
| **17** | c | b,a | 0 |
| **18** | 0 | c | b,a |
| **19** | 0 | b,a | c |
| **20** | b,a | 0 | c |
| **21** | b,a | c | 0 |
| **22** | a | b | c |
| **23** | a | c | b |
| **24** | b | a | c |
| **25** | b | c | a |
| **26** | c | a | b |
| **27** | c | b | a |

Table A.2: Distribution for 3 nodes $(a, b, c)$ and 4 slots $(1, 2, 3, 4)$.

| | **Slots** | | | |
|---|---|---|---|---|
| **Attempts** | 1 | 2 | 3 | 4 |
| 1 | 0 | 0 | 0 | a,b,c |
| 2 | 0 | 0 | a,b,c | 0 |
| 3 | 0 | a,b,c | 0 | 0 |
| 4 | a,b,c | 0 | 0 | 0 |
| 5 | 0 | 0 | a | b,c |
| 6 | 0 | 0 | b,c | a |
| 7 | 0 | a | 0 | b,c |
| 8 | 0 | a | b,c | 0 |
| 9 | 0 | b,c | a | 0 |
| 10 | 0 | b,c | 0 | a |
| 11 | a | 0 | 0 | b,c |
| 12 | a | 0 | b,c | 0 |
| 13 | a | b,c | 0 | 0 |
| 14 | b,c | 0 | 0 | a |
| 15 | b,c | 0 | a | 0 |
| 16 | b,c | a | 0 | 0 |
| 17 | 0 | 0 | b | a,c |
| 18 | 0 | 0 | a,c | b |
| 19 | 0 | b | 0 | a,c |
| 20 | 0 | b | a,c | 0 |
| 21 | 0 | c,a | 0 | b |
| 22 | 0 | c,a | b | 0 |
| 23 | b | 0 | 0 | c,a |
| 24 | b | 0 | c,a | 0 |
| 25 | b | c,a | 0 | 0 |
| 26 | c,a | 0 | 0 | b |
| 27 | c,a | 0 | b | 0 |
| 28 | c,a | b | 0 | 0 |
| 29 | 0 | 0 | c | a,b |
| 30 | 0 | 0 | a,b | c |
| 31 | 0 | c | 0 | a,b |
| 32 | 0 | c | a,b | 0 |
| 33 | 0 | a,b | 0 | c |
| 34 | 0 | a,b | c | 0 |
| 35 | c | 0 | 0 | a,b |
| 36 | c | 0 | a,b | 0 |
| 37 | c | a,b | 0 | 0 |
| 38 | a,b | 0 | 0 | c |

| | | | | |
|---|---|---|---|---|
| 39 | a,b | 0 | c | 0 |
| 40 | a,b | c | 0 | 0 |
| 41 | 0 | a | b | c |
| 42 | 0 | a | c | b |
| 43 | 0 | b | a | c |
| 44 | 0 | b | c | a |
| 45 | 0 | c | a | b |
| 46 | 0 | c | b | a |
| 47 | a | 0 | b | c |
| 48 | a | 0 | c | b |
| 49 | b | 0 | a | c |
| 50 | b | 0 | c | a |
| 51 | c | 0 | a | b |
| 52 | c | 0 | b | a |
| 53 | a | b | 0 | c |
| 54 | a | c | 0 | b |
| 55 | b | a | 0 | c |
| 56 | b | c | 0 | a |
| 57 | c | a | 0 | b |
| 58 | c | b | 0 | a |
| 59 | a | b | c | 0 |
| 60 | a | c | b | 0 |
| 61 | b | a | c | 0 |
| 62 | b | c | a | 0 |
| 63 | c | a | b | 0 |
| 64 | c | b | a | 0 |