Effect of Retransmission on the Performance of the IEEE 802.11 MAC Protocol for DSRC

by

Md. Imrul Hassan

Submitted in total fulfilment of the requirements for the degree of

Doctor of Philosophy

Centre for Advanced Internet Architectures
Swinburne University of Technology
Australia

2013
Abstract

Effect of Retransmission on the Performance of the IEEE 802.11 MAC Protocol for DSRC

by Md. Imrul Hassan

Dedicated Short Range Communication (DSRC) has the potential to improve road traffic safety and to significantly reduce accidents by enabling a broadcasting of critical safety information. One of the major sources causing unreliable safety message propagation is the so-called "hidden terminal problem" where transmissions from two vehicles out of the range of each other overlap in the receiver resulting in a packet loss. The problem is further aggravated due to the lack of acknowledgement for a successful reception of the broadcasting message in a medium access control (MAC) protocol.

In this thesis, we evaluate and improve the performance of the MAC protocol for safety applications in a single hop broadcast DSRC-based vehicle-to-vehicle (V2V) network.

Our first contribution is to develop a comprehensive yet flexible analytical model to study the IEEE 802.11 distributed coordination function (DCF) MAC protocol that has been adopted by the IEEE 802.11p standard for DSRC. This is one of the first models to capture the detrimental effect of hidden terminals in DSRC environment with various retransmission based MAC protocols. Furthermore, explicit expressions are derived for the mean and standard deviation of the packet delay, as well as for the packet delivery ratio (PDR) at the MAC layer in an unsaturated network formed by moving vehicles on a highway. The proposed model is validated using extensive simulations and its superior accuracy compared to that of other
existing models is demonstrated.

Our second contribution is to use the model to evaluate our proposed retransmission based MAC protocols, namely, blind sequential scheme, out-of-band signalling based NACK sequential scheme, piggybacked feedback based sequential scheme, and batch scheme. In the blind sequential scheme and the batch scheme every safety message is retransmitted fixed number of times without feedback, where as in the NACK sequential scheme and piggybacked sequential scheme feedback is provided through out-of-band busy tone and piggybacked with later packets respectively. We show that the NACK scheme can support the safety applications reliability requirement for up to twice the traffic load. We also demonstrate that prioritization of event safety messages by retransmission can improve the PDR by up to 17% compared to single transmission case for sequential schemes. The batch scheme, however, does not perform as good as the sequential schemes due to negative effect of multiple collisions per packet. For all of the schemes, we utilize our model to show the effect of various parameters on the performance such as maximum number of vehicle density, retransmission attempts, fraction of prioritized event safety messages, and in case of piggybacked sequential scheme the number of bits per packet ID. Finally, we optimize such parameters using our model and also predict which scheme perform best in particular scenario.
Acknowledgments

I would like to express my gratitude to my supervisors Prof. Hai L. Vu, A/Prof. Lachlan L.H. Andrew, and Dr. Philip Branch for their supervision and support during my PhD duration. It is their careful guidance and constant encouragement that help me get through the difficult period when I could not see the finish line. The knowledge that I have gained and the lessons that I have learned from them will be very useful for my future career.

I would also like to acknowledge active supervision by Dr. Taka Sakurai during first few years and for his continued cooperation and support with my PhD research. During my short visits to City University of Hong Kong and Michigan State University I have received full support and cooperation from Prof. Moshe Zukerman and Prof. Subir Biswas respectively. It was a great experience for me to work in their respective research laboratories and broaden my research skills.

I greatly appreciate the generous support of Prof. Grenville Amitage for me in the Centre of Advanced Internet Architecture (CAIA). I would like to thank the entire CAIA lab for the great environment and the fun time. I am grateful to all my friends, specially, Dr. Suong Nguyen and Dr. Kewin Stoeckigt for all their supports, valuable inputs, and countless conversations. I take the opportunity to convey my heartiest thanks to them for such nice friendship, affection and cooperation.

Finally, this thesis would not have been possible without the strong support, encouragement, and love of my parents and my sisters. I want to express my profound love, respect and gratefulness by dedicating this thesis to them.
This thesis is dedicated to my parents for their endless love, support, and encouragement.
Declarations

This is to certify that

(i) the thesis comprises only my original work,

(ii) due acknowledgement has been made in the text to all other material used,

(iii) the thesis is less than 100,000 words in length, exclusive of table, maps, bibliographies, appendices and footnotes.

Signature________________________________

Date______________________________________
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Abstract</strong></td>
<td>ii</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Motivation</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Research Challenges</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Contributions</td>
<td>6</td>
</tr>
<tr>
<td>1.4 Publications</td>
<td>7</td>
</tr>
<tr>
<td><strong>2 Related Work</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 Vehicular Adhoc Networks</td>
<td>9</td>
</tr>
<tr>
<td>2.2 Existing MAC Protocols</td>
<td>12</td>
</tr>
<tr>
<td>2.2.1 CSMA-based MAC Protocols</td>
<td>14</td>
</tr>
<tr>
<td>2.2.2 Singlehop broadcast protocols</td>
<td>16</td>
</tr>
<tr>
<td>2.2.3 Multihop broadcast protocols</td>
<td>19</td>
</tr>
<tr>
<td>2.3 Reliability</td>
<td>22</td>
</tr>
<tr>
<td>2.4 Existing Analytical Models</td>
<td>26</td>
</tr>
<tr>
<td>2.4.1 Models for unicast communication</td>
<td>26</td>
</tr>
<tr>
<td>2.4.2 Models for Broadcast communication</td>
<td>28</td>
</tr>
<tr>
<td><strong>3 Analytical Model For Delay And Reliability for Safety Message</strong></td>
<td>31</td>
</tr>
<tr>
<td>3.1 System Model</td>
<td>32</td>
</tr>
<tr>
<td>3.2 Direct Collision</td>
<td>35</td>
</tr>
<tr>
<td>3.3 Hidden Terminals</td>
<td>38</td>
</tr>
<tr>
<td>3.4 Delay Calculation</td>
<td>40</td>
</tr>
<tr>
<td>3.4.1 Mean and Standard Deviation</td>
<td>43</td>
</tr>
</tbody>
</table>
4 Retransmission Based MAC Protocol Extensions

4.1 Extensions

4.1.1 NACK Sequential Scheme

4.1.2 Blind Sequential Scheme

4.2 Analytical Model for NACK Sequential Scheme

4.3 Analytical Model for Blind Sequential Scheme

4.4 Simulations

4.5 Conclusion

5 Safety Message Prioritization Using Retransmissions

5.1 Extensions

5.1.1 Blind Sequential Retransmission

5.1.2 Batch Retransmission

5.1.3 Piggybacked Sequential Retransmission

5.2 Analysis of Packet Deliver Ratio

5.2.1 Direct collision

5.2.2 Hidden terminal

5.2.3 Packet delivery ratios

5.3 Delay Calculation

5.3.1 Distribution of service time

5.3.2 Mean and Variance of Delay

5.4 Simulations

5.5 Conclusion

6 Protocol Enhancement

6.1 Extensions

6.1.1 Sequential Retransmission
### 6.1 Batch Retransmission

- **6.1.2 Batch Retransmission**...

### 6.2 Sequential Retransmission

- **6.2.1 Hidden Collision**...
- **6.2.2 Number of Affected Nodes**...
- **6.2.3 Delay**...
- **6.2.4 Packet Delivery Ratio**...
- **6.2.5 Simulation Results**...

### 6.3 Batch Retransmission

- **6.3.1 Routine Packets**...
- **6.3.2 Event Packets**...
- **6.3.3 Simulation Results**...

### 6.4 Conclusion

- **6.4 Conclusion**...

### 7 Conclusion

- **7.1 Contributions**...
- **7.2 Future Work**...
- **7.3 Final Remarks**...
List of Figures

2.1 IEEE 802.11 DCF basic access [43] ................................. 16

3.1 Summary of the equations involved in the fixed point system .... 46

3.2 Total delay for direct collision using the following parameter set:
(data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes]) 48

3.3 Standard deviation of delay for direct collision using the following
parameter set: (data rate [Mbps], packet arrival rate [packets/sec],
packet size [bytes]) .................................................... 49

3.4 Packet Delivery Ratio for direct collision using the following param-
eter set: (data rate [Mbps], packet arrival rate [packets/sec], packet
size [bytes]) ............................................................. 50

3.5 Packet Delivery Ratio in network with hidden terminals using the
following parameter set: (data rate [Mbps], packet arrival rate [pack-
ets/sec], packet size [bytes]) ........................................ 51

3.6 Comparison of packet delay with Chen et al.’s model [22] using the
following parameter set: (data rate [Mbps], packet arrival rate [pack-
ets/sec], packet size [bytes]) ........................................ 52

3.7 Comparison of Packet Delivery Ratio with Chen et al.’s model in
network with hidden terminals [22] using the following parameter set:
(data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes]) 53

4.1 Total delay for NACK sequential scheme with three transmission at-
tempts using the following parameter set: (data rate [Mbps], packet
arrival rate [packets/sec], packet size [bytes]) ....................... 68
5.6 Relative improvement of the PDR for the blind sequential and batch transmission schemes with $\beta = 0.01$ ............................................ 102
5.7 Relative improvement of the PDR for the blind sequential and batch transmission schemes with $\beta = 0.05$ ............................................ 102
5.8 The PDR for the blind sequential scheme with optimal $m \in [1, 5]$ and $\alpha = 0.5$ ............................................................. 104
5.9 PDR for the blind sequential scheme with varying contention window, $W$ for $\beta = 0.05$ and $\alpha = 0.1$ ............................................ 104

6.1 PDR for sequential and piggybacked schemes, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 2$ ........................................ 118
6.2 PDR for sequential schemes, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 3$. ........................................ 119
6.3 PDR for sequential schemes, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 2$. ........................................ 120
6.4 PDR for sequential schemes, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 3$. ........................................ 121
6.5 PDR for piggybacked scheme with varying ID bits for $m = 2$. ........................................ 122
6.6 Values of $\alpha$ above which piggybacked scheme performs better than sequential, for $\lambda = 20$ [packets/sec], $m = 3$, and 16 [bits] packet ID. ........................................ 123
6.7 Karnaugh Map to simplify the expression ($(RE_1$ or $RE_{12}$) and ($RE_{12}$ or $RE_{23}$) or ($RE_{23}$ or $RE_3$)) to calculate the loss probability of event packets using batch scheme with 3 subpackets ........................................ 129
6.8 Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 2$. ........................................ 132
6.9 Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 2$. ........................................ 132
6.10 Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 3$. ........................................ 134
6.11 Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 3$. . . . 134

6.12 PDR (numerical) for different schemes with varying fraction of event packets for $m = 2$ and $\beta = 50$. . . . . . . . . . . . . . . . . . . . . . . 135

6.13 PDR (numerical) for different schemes with varying fraction of event packets for $m = 3$ and $\beta = 50$. . . . . . . . . . . . . . . . . . . . . . . 135
## List of Tables

3.1 DSRC System Parameters for Single Transmission Scheme . . . . . 48
3.2 Packet Delay for DSRC Safety Messages . . . . . . . . . . . . . . . . 54

4.1 PDR with reduced transmission range using 24 [Mbps] data rate and 10 [packets/sec] arrival rate . . . . . . . . . . . . . . . . . . . . . . . 71

5.1 DSRC System Parameters for Retransmission Based Schemes . . . . 96
6.1 DSRC System Parameters for Retransmission Based Schemes . . . . 117
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS</td>
<td>Intelligent Transportation System</td>
</tr>
<tr>
<td>VANET</td>
<td>Vehicular Ad-Hoc Network</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communication</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access in Vehicular Environment</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communication Commission</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle-to-Vehicle</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle-to-Infrastructure</td>
</tr>
<tr>
<td>CCA</td>
<td>Cooperative Collision Avoidance</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>NACK</td>
<td>Negative Acknowledgement</td>
</tr>
<tr>
<td>PACK</td>
<td>Piggybacked Acknowledgement</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Multiple Access</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>WiFi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>DCF</td>
<td>Distributed Coordination Function</td>
</tr>
<tr>
<td>EDCA</td>
<td>Enhanced Distributed Channel Access</td>
</tr>
<tr>
<td>RTS</td>
<td>Request-to-send</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear-to-send</td>
</tr>
<tr>
<td>CW</td>
<td>Contention Window</td>
</tr>
<tr>
<td>TXOP</td>
<td>Transmission Opportunity</td>
</tr>
<tr>
<td>SIFS</td>
<td>Short Inter-Frame Space</td>
</tr>
<tr>
<td>DIFS</td>
<td>Distributed Inter-Frame Space</td>
</tr>
<tr>
<td>EIFS</td>
<td>Extended Inter-Frame Space</td>
</tr>
<tr>
<td>r.v.</td>
<td>random variable</td>
</tr>
<tr>
<td>PDR</td>
<td>Packet Delivery Ratio</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>SDMA</td>
<td>Space Division Multiple Access</td>
</tr>
</tbody>
</table>
## List of Notations

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma$</td>
<td>the duration of one idle slot.</td>
</tr>
<tr>
<td>$\tau$</td>
<td>the transmission attempt probability.</td>
</tr>
<tr>
<td>$W$</td>
<td>the contention window size.</td>
</tr>
<tr>
<td>$W'$</td>
<td>the increased contention window size for the successive attempts in NACK sequential scheme</td>
</tr>
<tr>
<td>$\bar{W}$</td>
<td>the average number of backoff slots during contention period.</td>
</tr>
<tr>
<td>$\rho$</td>
<td>the queue utilization factor.</td>
</tr>
<tr>
<td>$i$</td>
<td>a superscript denoting a particular scheme ($i \in {\emptyset, n, s, b, p}$).</td>
</tr>
<tr>
<td>$k$</td>
<td>a subscript denoting a particular safety message type ($k \in {\emptyset, r, e}$).</td>
</tr>
<tr>
<td>$l$</td>
<td>a subscript denoting $l^{th}$ transmission attempt.</td>
</tr>
<tr>
<td>$g$</td>
<td>a subscript denoting a particular group of nodes ($g \in {\emptyset, L, R}$).</td>
</tr>
<tr>
<td>$m$</td>
<td>the maximum number of transmission attempts per packet.</td>
</tr>
<tr>
<td>Notations</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>$M_g$</td>
<td>the actual number of transmission attempts per packet in group $g$.</td>
</tr>
<tr>
<td>$b^i$</td>
<td>the channel busy probability for scheme $i$.</td>
</tr>
<tr>
<td>$N_n, N_h$</td>
<td>the number of nodes other than the tagged node within transmission/interference range of the tagged node.</td>
</tr>
<tr>
<td>$d^i_{k,l}$</td>
<td>the event that the $l^{th}$ retransmission of the safety message type $k$ for NACK and blind sequential schemes and $1st$ transmission of type $k$ for single and batch schemes does not experience direct collision for the scheme $i$.</td>
</tr>
<tr>
<td>$c^i_{k,l}$</td>
<td>the event that the $l^{th}$ retransmission of the safety message type $k$ for NACK and blind sequential schemes and $1st$ transmission of type $k$ for single and batch schemes does not experience any collision for the scheme is $i$.</td>
</tr>
<tr>
<td>$\overline{d}^*_e$</td>
<td>the average direct collision probability over all the transmission attempts for event packet in NACK and blind sequential scheme $i$.</td>
</tr>
<tr>
<td>$H^i_{k,l,g}$</td>
<td>the event that no hidden node in group $g$ is in the state $V^{j \in {a,b}}$ when the tagged node started its transmission of $l^{th}$ attempt of packet of type $k$ with scheme $i$.</td>
</tr>
<tr>
<td>$V^*_{c^\ast,c}$</td>
<td>the period after($j = a$) or before($j = b$) the tagged node starts transmitting a class $c^\ast$ packet during which it is vulnerable to transmissions of class $c$.</td>
</tr>
<tr>
<td>Notations</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>$T^i$</td>
<td>the complete transmission time of a batch of subpackets including <em>DIFS</em> period with scheme $i$.</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>the rate of packets per second.</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>the rate of batch transmission per second.</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>the fraction of the packets that are event safety packets.</td>
</tr>
<tr>
<td>$D^i$</td>
<td>the delay until packet is received by all intended recipients with scheme $i$.</td>
</tr>
<tr>
<td>$S^i$</td>
<td>the service time until sender stops sending packet with scheme $i$.</td>
</tr>
<tr>
<td>$A^i_{k,l}$</td>
<td>the access delay for scheme $i$ and packet type of $k$ until $l^{th}$ attempt.</td>
</tr>
<tr>
<td>$Q^i$</td>
<td>the queueing delay for scheme $i$.</td>
</tr>
<tr>
<td>$B$</td>
<td>the backoff delay for each transmission attempt.</td>
</tr>
<tr>
<td>$B'$</td>
<td>the backoff delay for successive transmission attempt for NACK sequential scheme with larger contention window.</td>
</tr>
<tr>
<td>$T_{Res}$</td>
<td>the residual time until the current packet transmission finishes.</td>
</tr>
<tr>
<td>$Y$</td>
<td>the duration of the virtual slot.</td>
</tr>
<tr>
<td>$p_{scv}$</td>
<td>the successive collision probability.</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Motivation

Vehicular transport is a daily part of our life whether going back and forth to work, school, recreation or other activities. It also has a huge economic effect as a mean of connecting businesses to markets and bringing items from suppliers. According to the Australian Bureau of Statistics, 227 billion kilometers were traveled on Australian roads in 2010 [8]. So, safe and efficient transport systems can contribute to economic prosperity as well as the betterment of people’s everyday life.

This comes from the fact that billions of dollars are lost each year due to traffic congestion and accidents. Although accurate cost valuation of road crashes is difficult specially for a fatal crash where human life needs to be evaluated, [20] presents some estimates of the cost of road crashes for 2006 in Australia. According to this report, the social cost of road crashes in 2006 accounted for 1.7% of GDP, an estimated 17.85 billion dollars. More than a million vehicles were involved in an estimated 653,853 road crashes and as many as 1,600 people died whereas 31,200 people were injured and hospitalized.

Due to the severity of the issue, the government invests substantial amounts of money on identifying the problems, and working towards improving road safety. Australian Transportation Council has laid down a plan for the current decade in [9] on reducing fatal and serious injury crashes on Australian roads. Subsequently, the goal of improving road safety funds and drives researches in this field. Traditionally, the focus of research was to investigate effectiveness of passive safety systems such
as airbags and seat belts in protecting passengers during a crash. However, recently the focus has shifted towards active safety systems such as active braking systems, electronic stability controls and collision avoidance systems. These systems collect data from sensors fitted in the car and activate emergency responses when a hazard situations arise. In contrast to isolated sensing and reacting, another approach is to communicate and cooperate among vehicles. Communication enabled cooperative applications can leverage the information shared among vehicles.

Research in Vehicular Ad-Hoc Networks (VANETs) cooperative safety application has gained momentum after Federal Communications Commission (FCC) assigned dedicated bandwidth for DSRC use. The term DSRC has been coined for short range wireless communications between vehicles in VANET with the primary focus on cooperative safety applications. Various wireless technologies were considered for DSRC communication before WiFi IEEE 802.11p \[44\] was agreed upon. WiFi has been very popular and successful for the last decade in providing service to private home as well as campus wide and city wide coverage. Still, the highly mobile and dynamic V2V network poses many challenges for a reliable and efficient communication channel based on WiFi for safety applications.

As such, performance evaluation of DSRC communication for the use of safety applications is required before such applications are deployed. In this thesis, we study the performance of DSRC communication in single hop V2V network which is relevant for safety applications. Explicit expressions are derived and validated using extensive simulations for the mean and standard deviation of the packet delay, as well as for the PDR at the MAC layer. To improve performance, we propose and evaluate extensions to existing DSRC protocol.

1.2 Research Challenges

In this section, we highlight some of the research challenges on safety applications in DSRC environment. At first, we present challenges related to the reliability of
DSRC communication protocol which is the focus of this thesis. Afterwards, we provide a short summary of other research challenges despite being out of scope for our work.

Reliable and timely safety message dissemination in V2V network is essential for safety applications. However, as many vehicles contend for the shared channel access, safety packets can be lost due to packet collisions. The number of vehicles in a road strip can vary significantly depending on the time of day, location and other factors. So, the MAC plays a significant role in the efficient use of the channel. Vehicles contend for and acquire access of the channel through the MAC layer before broadcasting a safety message to all nearby vehicles. Broadcast communication in contrast to unicast communication is appropriate for safety messages as these are intended for all vehicles. However, the current broadcast mechanism in the WiFi MAC protocol does not incorporate acknowledgement (ACK) of successful packet reception. Although some work suggested acknowledgement based extensions, suitability of those in DSRC environment is not well tested. As such, performance of DSRC communication for the use of safety applications need to be evaluated and analyzed. Although, network simulators can be used for performance evaluation, analytical modeling may provide better insights of the system. In this thesis, we develop an analytical model which is simple enough to gain insights while being reasonably accurate.

Packet collision can also occur between vehicles which are out of their range, but can affect packet reception. These vehicles are called “hidden terminals” and this phenomenon is know as “hidden terminal problem”. The hidden terminal problem is significant in WiFi networks as well. WiFi includes a channel reservation extension based on an RTS/CTS mechanism. However, for reasons similar to the difficulty of broadcast acknowledgment, it can not be implemented for broadcast communication in its current form. As such, the hidden terminal problem is one of the major concerns for unreliability of safety message propagation. Also, most analytical models that capture hidden terminal problem are for RTS/CTS based MAC protocols. This
is not the case for DSRC communication, as such, in the thesis we model hidden terminals without considering any channel reservation mechanism.

Once we evaluate the performance of DSRC protocol for safety applications, we need to improve the performance as well to meet quality of service (QoS) requirement. In this thesis, we propose a number of extensions to standard WiFi MAC protocol based on retransmissions to improve reliability. We extend the analytical model for standard MAC protocol to evaluate and compare their performance. As the proposed protocol extensions vary in their operation, we have additional challenges in modeling them. For batch retransmission scheme, which retransmits packets back-to-back without any gap as a long batch of packets, the challenge is to capture multiple collision effect in the model. By multiple collision effect for batch scheme, we mean loss of a complete batch due to more than one packet collisions. In the thesis, we model packet loss for batch retransmission scheme considering up to three collisions in a single batch.

Now, we highlight some challenges for safety applications which are not considered in this thesis. Safety applications primarily can act in two different ways upon detecting a hazard condition. Firstly, through actuators it can initiate an emergency response such as hard braking when there is an imminent collision. Secondly, it can inform the driver about the situation so that the driver can take suitable action. Although, the second approach is slower due to the driver’s reaction time, automated emergency response technology is not mature enough to be implemented for DSRC safety applications. Note that, many smart cars are capable of automated emergency response based on in-car sensor data; however none of them rely on information coming from other cars. Relying on such information for automated response may jeopardize the safety and security of the car unless both technologies are well tested. The natural first step for using shared information using DSRC is to inform the driver through signals displayed in the dashboard about hazard situations such as the presence of a car in the blind spot. With the introduction of many safety applications, the driver may become overwhelmed by signals constantly com-
Chapter 1. INTRODUCTION

ing from every application all the time. So, out of all information available which information to show and when is an important research question.

Regardless of how information is presented, safety applications require that relevant information is collected from all vehicles within an appropriate range. For example, a pre-crash sensing application may need to know the location, speed and direction of movement of a nearby vehicle in an unavoidable crash situation to initiate collision counter measures. Whereas cooperative collision avoidance relies on information gathered from farther away vehicles to warn the driver about a slow moving car blocked from view by other vehicles. DSRC safety messages may need to be disseminated up to 1000 meters [7] through single hop or multi-hop communication. The latter mode of communication however does not require routing protocols as in MANET. This is because, instead of finding a route between the source and the destination, safety messages need to be broadcast to all vehicles in a region. In the simplest form of multi-hop broadcast, every vehicle receiving a safety message retransmits and forwards it to other vehicles which is called “flooding” [41,45]. However, this leads to a “broadcast storm” problem when every vehicle tries to spread it causing a heavily congested channel. There have been many proposals [6,55,96] to solve this problem by restricting the number of vehicles forwarding the safety message. Most of the proposals however are complex and may not be suitable for dynamically changing topology in a DSRC context.

Another cause of packet loss is imperfect channel conditions in the DSRC environment. High mobility of vehicles can make doppler effects become more severe. Also, metallic bodies of cars reflect electromagnetic waves causing fast fading. These physical (PHY) layer issues have been addressed in prior work through the use of techniques such as Orthogonal Frequency Division Multiplexing (OFDM). In urban environments, high rise buildings and structures cause shadow fading or slow fading which makes it difficult to communicate between vehicles without line of sight.
1.3 Contributions

In this section, we present the main contributions of the thesis.

Firstly in Chapter 3, the performance of standard WiFi MAC protocol in DSRC environment is modeled and investigated in terms of delay and packet delivery ratio. This analytical model is one of the first few \cite{22,24} to take hidden terminals into account in unsaturated broadcast network. While the mean delay and its variance stay well below the required threshold for safety applications, the protocol is unable to meet the QoS requirement for reliability. We also confirm that collisions due to the hidden terminal problem is the major source of collisions and direct collision only accounts for approximately 10\% of the total number of collisions. The effect of hidden terminal collisions is accurately captured in the proposed analytical model. The content of this chapter was published in \cite{37}. In later chapters, the analytical model is extended for the proposed retransmission based MAC protocols which shows the flexibility and usefulness of the model.

Secondly, in Chapter 4 we propose two MAC protocol extensions based on retransmission to improve reliability at the cost of some delay, which are negative acknowledgement (NACK) scheme based on out-of-band signalling \cite{38} and sequential scheme \cite{37} without requiring feedback. Although the concept of a busy tone \cite{34,89} or a black burst \cite{77,85} is not new, our proposed scheme is one of the first to use busy tone for NACK. Because DSRC system requires high reliability of safety messages, the use of busy tone for less frequently occurring NACKs is preferred to that for high number of ACKs. Analytical results validated by simulation show the advantage of feedback in improving reliability at low and moderate traffic loads.

However, when traffic density is higher, the reliability of safety message communication deteriorates due to excessive channel load caused by packet retransmissions. So, in Chapter 5 two extensions are proposed, namely blind sequential scheme and batch retransmission scheme, which improve reliability of emergency event safety messages without greatly penalizing the channel load. This is done by prioritizing
and retransmitting only emergency event safety messages which is a novel concept and unlike EDCA based prioritization [31]. We show that significant reliability improvement can be achieved when only small fractions of packets are prioritized. The performance is also compared with a feedback based protocol to justify the tradeoff between complexity and reliability. Note that, certain side effects such as multiple packet collision are not considered for batch retransmission protocol in Chapter 5 which is considered later in Chapter 6. Works presented in this chapter has been published in [39,40].

Lastly, based on the observations from previous chapters, we focus on simplifying the modeling in Chapter 6 by ignoring direct collision. We also enhance the extensions by providing adaptive extra delay between retransmission attempts to avoid repeat collisions while ensuring retransmission within packet life time. Despite the simplification the analytical model is comprehensive as we consider packet life time expiry for sequential schemes and multiple collisions for batch scheme with a better model for the hidden terminals. The enhancements to the extensions also show positive effects on the reliability of sequential schemes. We also show that the analytical model can be used to capture the trend of the reliability drop with increased vehicle density and also to identify which scheme performs better.

1.4 Publications


Chapter 2

Related Work

In this chapter, we provide a summary of the related works in the literature. At first, we discuss the concept of traffic safety applications supported by VANET. Next, we summarize existing MAC protocols proposed for safety applications followed works that address reliability issues. Finally, we present an overview of analytical models for IEEE 802.11 DCF in general and for unsaturated broadcast communication with hidden terminal in particular.

2.1 Vehicular Adhoc Networks

VANET can be considered as an special case of Mobile Ad-Hoc Networks (MANET) where the vehicles act as nodes. The term VANET was introduced to portray the ad-hoc nature of vehicular networks. Despite the similarity of the two networks in their names, the objective and the functionality of VANET is quite different from MANET. VANET covers a range of communication technology such as single-hop versus multi-hop communication and different architectures. For instance, cooperative collision avoidance (CCA) application is designed to improve traffic safety which relies on uncoordinated single hop broadcast of safety messages [47]. On the other hand, non-safety applications like enhanced route guidance and navigation [26] requires multi-hop geographical broadcasting as well as infrastructure support. In terms of architecture, VANET can be classified in to vehicle-to-infrastructure (V2I) and V2V networks. In both cases, vehicles are equipped with an on-board unit (OBU) with short range wireless communication capabilities. OBUs on neighbor-
ing vehicles form the V2V network and vehicles can disseminate safety messages through the network. In V2I, roadside unit (RSU) are placed along side the road which can extend the safety message dissemination range. RSUs can also be connected to a wired infrastructure for long range communication as well as internet connectivity. V2I provide essential support for traffic efficiency applications such as enhanced route guidance and navigation.

Currently, the major focus in VANET research includes improvement in road safety as well as transportation efficiency \[36\]. In this thesis, we concentrate on the safety aspect of VANET, especially performance evaluation and communication protocol design for cooperative collision avoidance. Road safety applications are supported by the transmission of routine status messages and event-driven emergency messages. Event-driven safety messages, referred to as “event messages” through the rest of the thesis, are triggered by rapid changes in vehicle behavior such as a hard brake or an airbag explosion. Also, through “routine messages” vehicles gain local neighborhood awareness which equips the safety applications enough information to evaluate potential traffic risks. Routine status messages are sent periodically to neighboring vehicles to inform them of the current status of the originating vehicle (e.g. location speed, direction), whereby the receiving vehicles/drivers can then anticipate any potential hazards (e.g. traffic jam ahead) and take necessary action. To enable preventative action, it is essential that both types of safety messages are received correctly by surrounding vehicles in a timely fashion; fast communication and timely message delivery is essential for proper functioning of the safety applications. Also, such messages are mostly relevant for vehicles close to an accident or hazard situation. Coupled with the fact that, communication range for OBUs can be as much as 1000m over line-of-sight communication \[7\], single hop communication is often enough for safety applications. However, for such a long transmission range reliable safety message communication is difficult due to fading and interference. As such, for some safety applications multi-hop communication can be utilized in the absence of infrastructure to extend communication range, although multi-hop
communication is prevalent in traffic efficiency applications.

Research in VANET specially for safety applications expanded after U.S. Federal Communication Commission (FCC) allocated 75MHz of spectrum in the 5.9 GHz band for DSRC use in 1999. DSRC refers to short range wireless communication for primarily safety message dissemination among vehicles in V2V and V2I networks. The DSRC wireless spectrum is divided into seven 10 MHz wide channels, and a reserved 5 MHz channel. One of the 10 MHz channels, called the control channel, is restricted to safety communications only, while the other channels are available for both safety and non-safety usage. The initial effort at standardizing DSRC radio technology took place in the ASTM 2313 working group [7]. Later, the IEEE Wireless Access in Vehicular Environment (WAVE) project has published specifications for the FCC DSRC spectrum based on an OFDM air interface. IEEE WAVE encompasses the IEEE 802.11p standard [44] for the MAC and PHY, and the IEEE 1609 family of standards, which define the higher layer protocols and the protocol architecture [94]. IEEE 802.11p is based on an existing WiFi protocol IEEE 802.11a, but with modifications to support vehicular communications with low latency. The 802.11p MAC protocol, like other 802.11 variants, uses the DCF for channel access. Several on going projects in Europe also address different aspects and issues of Intelligent Transportation System (ITS) [56]. ETSI [1] is managing the standardization process of the ITS communication stack based on IEEE 802.11p to harmonize with the DSRC standards as far as possible.

Requirement analysis for safety applications is one of the major concerns during standardizations. Depending on the concerned application, the transmission range, message frequency, allowable delay constraint and reliability requirement varies. Although in [7] the required transmission range for DSRC was mentioned to be 1000m, for some safety applications such as pre-crash sensing 50m transmission range is enough. For most of the safety applications though, the transmission range can vary anywhere from 150m to 300m. Using a larger than required transmission range is detrimental as communication channel can become congested. This is usually the
case for slow moving vehicles in a congested traffic environment. For routine safety message, the rate of message is around 10Hz for safety application like cooperative collision avoidance. The maximum allowable delay constraint is usually inversely related to the message rate and in the range of 100m \[63\]. Reliability is another factor in requirement analysis for safety applications. Vehicles form a dynamic topology and this mobility poses challenges to reliable safety message communications. This is specially true for multi-hop communication due to connectivity hole problem \[50\]. Dynamic topology also affects channel congestion which is related to packet loss. To quantify reliability, the PDR is defined as a measure of safety messages successfully delivered all intended recipients \[22\]. For safety applications it is essential that most messages are delivered in time. The required PDR threshold is chosen to be 90\% in \[7\].

One of the main challenges to achieve that objective is the loss of packets due to the presence of hidden terminals \[23, 89\]. This occurs when a node is transmitting to a target node while a third node that is unaware of the transmitter also starts its transmission and causes interference at the receiver. The hidden terminal problem can afflict all decentralized wireless networks, but is particularly severe when safety messages are broadcast in all directions. In this case, there are multiple receivers for each message, scattered in the transmission range of the sender. Any node that is within sensing range of any receiver but outside the transmission range of the sender is a potential hidden terminal. Therefore, the potential hidden terminal region is large for broadcast communication and the chance of packet loss due to hidden terminal problem is high. Quantifying and reducing the impact of hidden terminal problem on the reliability of safety messages is the major theme in our thesis.

### 2.2 Existing MAC Protocols

In DSRC, the wireless channel is shared among all vehicles to broadcast safety messages. As such, the MAC protocol, which enables multiple users to share a common
physical medium, has a great impact on the feasibility and performance of safety applications. Due to the nature wireless medium, transmission from any vehicle is heard by all neighboring vehicles. This is useful for safety applications, as safety messages are often relevant to the immediate neighboring vehicles. However, we need to consider the challenges for the MAC protocols in DSRC. Fast moving vehicles and frequent topology changes pose a major challenge to adapting existing MAC protocols for DSRC. Also, when the rigid constraints on delay and reliability for safety applications are considered, the choice of MAC protocol becomes more difficult. The communication in DSRC is also affected by the hidden terminal problem where transmission of node which is out of sensing range of another node interferes with its transmission. The hidden terminal problem is amplified in DSRC due to broadcast nature of communication as well as due to lack of coordination among vehicles.

On the other hand, the MAC protocols can also take advantage of some of the eccentricities of the DSRC environment, such as predictable directionality of relevant neighbor vehicles, since vehicles are often arrayed linearly on a road. And unlike some other ad hoc networks, resource limitations such as data storage and energy consumption are not major problems. Furthermore, it is reasonable to assume that most of the vehicles would carry a GPS device, which can be used for acquiring position information and for providing time synchronization. The latter is only critical for certain protocols; it should be noted that such protocols should account for the fact that the GPS service may fail in urban environments, tunnels, etc.

Several MAC protocols have been proposed for the DSRC environment which are summarized in [23,65]. In this section a survey of few of the relevant MAC protocols for DSRC are presented. As IEEE 802.11p DCF is the preferred MAC protocol for both standardization bodies and industry movements, we begin our discussion with the Carrier Sense Multiple Access (CSMA) based MAC protocols which include IEEE 802.11p DCF. The IEEE 802.11p standard proposed for DSRC is based on IEEE 802.11a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Chapter 2. RELATED WORK

MAC protocol which has been widely accepted for WiFi communication in the past decade. After that, we summarize other protocols that have been proposed for safety applications in DSRC environment. We classify those protocols in two sections based on whether or not they use singlehop or multihop communications.

2.2.1 CSMA-based MAC Protocols

CSMA-based MAC protocols such as IEEE 802.11 DCF have been widely used in wireless LANs and the technology has matured over the past decade. In CSMA-based protocols, a node must sense the channel for a period of time and transmit its data only if the channel is idle. To avoid collisions of data packets at the receiving nodes due to hidden terminals, some short signalling packets, e.g. request-to-send/clear-to-send (RTS/CTS), are introduced in multiple access collision avoidance (MACA) and multiple access collision avoidance for wireless lans (MACAW) protocols. IEEE 802.11 DCF is based on CSMA with collision avoidance where two types of sensing are employed to avoid collision: physical carrier sensing and virtual carrier sensing. While physical carrier sensing mechanism is the same as other CSMA-based protocols, the virtual carrier sensing is achieved by setting a duration field to specify how long the sender expects to use the medium. Other nodes hearing the packet can defer their transmissions for that duration.

CSMA-based protocols do not require any reconfiguration upon a change in network environment. Also, the protocol works in a distributed manner without the need for a central coordinator. As a result, this is the preferred approach for most of the VANETs MAC protocol standards such as the ASTM DSRC and the IEEE WAVE. Recent studies of CSMA-based protocols in DSRC environment suggest that the delay characteristic of such protocols under light to moderate load conditions meets the requirements for timely delivery of safety critical messages.
IEEE 802.11p Standard

The initial effort at standardizing DSRC radio technology took place in the ASTM 2313 working group [7]. The IEEE Wireless Access in Vehicular Environment (WAVE) project has published specifications for the FCC DSRC spectrum based on an OFDM air interface. IEEE WAVE encompasses the IEEE 802.11p standard [44] for the MAC and PHY, and the IEEE 1609 family of standards, which define the higher layer protocols and the protocol architecture [94]. IEEE 802.11p is based on IEEE 802.11a, but with modifications to support vehicular communications with low latency. The 802.11p MAC protocol, like other 802.11 variants, uses DCF for channel access.

In the IEEE 802.11 DCF, nodes contend for the channel using a carrier sense multiple access mechanism with collision avoidance (CSMA/CA) as shown in Fig. 2.1. When a node has a packet to send, the channel must be sensed idle for a guard period known as the distributed interframe space (DIFS). If during that period of time, the channel becomes busy, then the access is deferred until the channel becomes idle again and a backoff process is initiated. Backoff intervals are slotted, and stations are only permitted to commence transmissions at the beginning of slots. The discrete backoff time is uniformly distributed in the range $[0, CW - 1]$, where $CW$ is called the contention window. At the first transmission attempt, $CW$ is set equal to $W$, the minimum contention window. The backoff time counter is decremented by one at the end of each idle slot. It is frozen when a packet transmission is detected on the channel, and reactivated after the channel is sensed idle again for a guard period. The guard period is equal to a DIFS if the transmitted packet was error-free, and equal to the extended interframe space (EIFS) if the packet was in error. The station transmits when the backoff counter reaches zero. A collision occurs when the counters of two or more stations reach zero in the same slot. After every successful data packet transmission, a station initiates a post-transmission random backoff. If the next packet was already enqueued when the previous packet was sent, its defer time will span the entire backoff period, whereas a packet that
arrives at the MAC layer after the previous packet was sent would experience only part of the backoff period, or none at all if the backoff period has already elapsed.

DSRC safety messages are transmitted in broadcast mode, which is different in several ways from unicast communication for IEEE 802.11 DCF. First of all there is no ACK sent after the successful reception of a data packet, so the sender is unaware of any packet collision and there is no retransmission or augmentation of the contention window. In unicast communications, the RTS/CTS access method is provided to alleviate the hidden terminal problem. However, the implementation of RTS/CTS scheme for broadcast communications is not practical because it requires a handshaking exchange between sender and all the receivers which increases the channel load significantly. As such, the lack of channel reservation protocol and acknowledgement makes safety message broadcast prone to excessive packet loss.

2.2.2 Singlehop broadcast protocols

In this subsection, we summarize some of the non-contention based protocols that have been proposed for safety applications in DSRC environment. Most of these protocols, in general, try to reduce packet collision by channel reservation as opposed to contention. They can be further classified, according to how the channel is shared, into four categories — time-division multiple access (TDMA), space-division multiple access (SDMA), cluster-based, and directional antenna based protocols.
TDMA based protocols allocate fixed time slots or frequency channels for each node either statically or dynamically based on location, slot availability etc. The Reliable R-ALOHA (RR-ALOHA) protocol [18,19] is one such MAC protocol proposed for the DSRC environment where the channel is shared by defining frames with multiple time slots. The scheduling is based on the classical R-ALOHA protocol [27]. In R-ALOHA, a time slot is either *reserved* or *available* for transmission of a node. The reservation for the slot is made by trial and error method by each node individually. However, the proper operation of the protocol requires a central repeater which conveys the slot information to every node. RR-ALOHA removes the necessity of the repeater by transmitting additional frame information to inform every node about the status of each slot. The main benefit of RR-ALOHA is that the channel can be shared amongst vehicles with a reduced likelihood of collision. With proper operation of the protocol, hidden terminal and exposed terminal problems are also greatly reduced and high reliability can be achieved. However, time schedule-based protocols are sensitive to mobility and topology changes and require significant reconfiguration time. Also, a central coordinator in DSRC is not realistic. Dynamic coordination requires knowledge of all neighboring vehicles and it takes a few time cycles to agree on a stable schedule. As a result, the access delay in such a scenario is high. Another MAC protocol based on R-ALOHA namely the self-organizing TDMA (STDMA) protocol has been evaluated in the DSRC context [15] to support routine safety messages. The protocol does not require global frame synchronization rather slot synchronization is achieved by monitoring the channel for a full frame at the start.

Space division multiple access (SDMA) for the DSRC safety applications is proposed in [11], where a slot or a channel is uniquely mapped to a space division by its physical location. Each vehicle need to determine its position accurately and the mapping from location to slot or channel is globally known by all vehicles. A related protocol called the location-based channel access (LCA) protocol is proposed in [49], where they make provisions for multiple vehicles in the same space division.
Adaptive space division multiplexing (ASDM) is proposed in [17] to overcome the inefficiency associated with SDMA. The mapping function used in ASDM is also similar to SDMA, but vehicles can now utilize the unused time slots as well. Imperfect position accuracy and time synchronization among vehicles are some physical layer issues that can degrade the performance of these protocols. Also, these protocols generally require accurate power control to manage interference with other space divisions using the same channel.

There exist another group of MAC protocols [79, 105] which also relies on the geographic location of the vehicles. In those protocols, neighboring vehicles are grouped in small geographic clusters and a vehicle is elected as a cluster-head. The cluster-head acts as a coordinator for the cluster and relay for safety messages across cluster boundaries. A schedule-based approach is used for intra-cluster communication and a contention-based approach is used for inter-cluster communication. However, to separate intra-cluster communication from inter-cluster communication, the protocol requires either multi-channel communication or partitioning of each time cycle. The complexities of the schedule-based approach are also present in this approach. Moreover, switching between intra-cluster and inter-cluster communications consumes a significant amount of the limited bandwidth available for safety applications. The complexity of the protocol makes it less scalable in the DSRC environment.

The use of directional antennas in wireless ad hoc networks can enhance performance by permitting multiple concurrent transmissions in the same neighborhood [53, 54, 102], thereby increasing spatial reuse. A directional antenna can direct its transmission in any particular direction using a group of antenna elements. A number of non-overlapping beams can be formed to cover 360 degrees around the node. An additional omnidirectional antenna element can also be present to send control packets in all directions; otherwise omnidirectional transmission requires the use of all antenna elements at once. One of the major problems that can hinder D-MAC performance is the so-called “deafness” problem [25]. Deafness is caused
when a transmitter fails to communicate with its intended receiver because the receiver is beam-formed in a different direction. The degradation in performance due to deafness is also demonstrated in [102], where a reliable D-MAC protocol for broadcast communication is proposed and evaluated. The performance is shown to be worse compared to a MAC using omnidirectional antennas due to this deafness problem. Also, it is difficult to coordinate multiple simultaneous transmissions in practice. With high mobility of vehicles in V2V networks, antennas must be constantly tracked which further increases the system complexity.

As many of the above mentioned MAC protocols promise better reliability in terms of packet loss and in some cases they can combat hidden terminal problem better than the contention based protocols, many researchers proposed and evaluated those protocols for DSRC safety applications while IEEE 802.11p was being standardized.

### 2.2.3 Multihop broadcast protocols

Some of the MAC protocols are proposed to disseminate messages to a larger area by multihop broadcast. Safety messages can possibly be transmitted to a sufficiently large area by single hop transmission using higher transmission power. However, in some cases, this may not be suitable as the contention on the channel also increases with transmission power. Multihop broadcast protocols on the other hand have to deal with so called “Broadcast Storm Problem” [68] and connectivity hole problem [50].

A multi-hop directional broadcast protocol for urban VANET environment was proposed in [55]. The paper addresses the issue of broadcast storm problem and line of sight problem in urban areas. The proposed protocol, UMB, extends RTS/CTS for broadcast and addresses issue of selection of forwarding node. UMB uses blackburst method to determine furthest node as repeater. Fixed repeaters are required however to initiate directional broadcast from the traffic junctions.

[96] also focuses on the broadcast storm problem for multihop applications in
VANET. The situation arises due to blindly rebroadcasting packets which may lead to frequent contention and collision. The effect on message delay and packet loss is considered rather than message reachability and overhead which is common for MANET research. Without changing DSRC data link layer, the authors proposed three probabilistic and timer based suppression techniques. These techniques are influenced by other proposed protocols for broadcast suppression most of which work by prioritizes the forwarding nodes based on distance or signal strength. Broadcast storm is also a problem in MANET, where nodes need to flood the network during route establishment phase. However, the goal of route discovery is to acquire the route within a short time without excessive overhead to other traffics. For VANET, the broadcast packets constitute the majority of the traffic and packet loss minimization is the primary objective. In the protocols proposed in the paper, a relay node is selected implicitly which prioritizes distant nodes from the sender. The selection can either be probabilistic or deterministic within predefined slots. In the absence of a GPS signal, a signal strength based protocol is proposed. The simulation results confirm that, the proposed protocols can reduce the packet loss by up to 70 per cent with acceptable level of end-to-end delay.

An adaptive broadcast scheme was proposed in [6] to disseminate emergency messages to all vehicles within a 2-hop span. To suppress broadcast storm, the average probability of retransmission is dynamically calculated based on the local vehicle density. The relay node needs to have knowledge about number of nodes in the 2-hop span which it can gather by listening to periodical HELLO packets. The adaptive scheme works well compared to deterministic broadcast with lower overhead on the channel.

In [50] Khakbaz et al. focus on disseminating information in VANET by multihop broadcast and improving reception rate by overcoming connectivity hole problem. For forwarding broadcast message, instead of simple flooding a relay node can be chosen based on location information. All nodes that receive the message are potential relay nodes and they schedule the retransmission at a later time. However, upon
receiving the same message from any node in between, the message retransmission is canceled. To combat connectivity issue, the last relay node keep sending small messages asking all vehicles for their IDs and location. As long as there is a new vehicle in the range, the forwarder retransmits the original message. Simulation results confirm that this protocol ensures more coverage for the message compared to UMB protocol.

Another protocol was proposed in [91] called the Distributed Vehicular Broadcast (DV-CAST) protocol which addresses various connectivity conditions in V2V networks. The protocols operates in three modes depending upon network connectivity — well-connected, sparsely-connected, and totally disconnected. In the sparsely-connected scenario, a vehicle moving in the same direction as the message carries the message until it expires or can be retransmitted back to the original message forwarding direction. DV-CAST protocol requires local connectivity information such as whether or not there is a vehicle with in the transmission range in a particular direction. Such information can be collected via the use of periodic messages. In [73, 74] an ABSM protocol was proposed for V2V network extending PBSM protocol [51]. In both ABSM and PBSM protocols, nodes only retransmit packets if they belong to the connected dominating set (CDS) which is determined via exchanging of periodic messages. These messages also exchange local neighborhood information and in case of ABSM protocol piggybacked acknowledgement of the received packets.

A different multihop point-to-point communication protocol is proposed suitable for a city environment in [59]. In the proposed protocol, a node does not require maintaining a list of neighborhood list; however every node needs to have knowledge about topology information and also dynamic traffic information. The protocol operates in two stages — first it tries to find out the next junction and then forwarding the message towards that direction. To combat connectivity hole problem the packet is stored and retransmitted at a later time.
Chapter 2. RELATED WORK

2.3 Reliability

In this section, we identify some of the causes that hinder reliable communication in the context of safety applications in DSRC environment. Reliability can be measured by fraction of safety messages which are received by all intended receiving vehicles referred to as the PDR. For safety critical applications it is essential that most messages are delivered in time. The required PDR threshold is chosen to be 90% in [7].

Wireless networks is inherently unreliable due to path loss and fading in contrast to wired networks where congestion is the major cause of packet loss. Safety messages sent wirelessly may get corrupt due to physical layer issues such as channel error, multi-path fading, shadow fading. On the link layer, packet collisions among nodes within same contention region or nodes hidden to each other can destroy a safety message. These issues have been extensively addressed by researchers for WiFi networks, mobile ad hoc networks, sensor networks etc. The techniques to resolve these issues can be used for DSRC communication as well.

However, physical channel imperfections is severe in VANET due to highly mobile vehicles and signal reflections and scattering they cause [66, 82]. Buildings and other tall structures in urban environment also deteriorate channel condition through shadowing. Techniques such as cyclic prefix, guard interval, and use of pilot tones for OFDM systems can compensate some of the negative effects of fading [82, 104]. Also, for IEEE802.11p, the bandwidth was reduced from 20MHz to 10MHz to address severity of physical channel condition.

As wireless channel is shared by many vehicles, channel congestion and contention can cause packet loss due to collision. By prioritizing event safety messages over routine safety messages the reliability of the former can be improved. In [31] such prioritization is proposed using IEEE802.11p Enhanced Distributed Channel Access (EDCA) functionality where packets are classified in to different access categories. This improves saturation throughput for prioritized safety messages, however
effect on reliability in unsaturated settings, typical for safety applications in DSRC environment, is not presented. In the thesis, we present a different prioritizing method based on retransmission which works in an unsaturated settings.

The safety messages in VANET are usually transmitted through broadcasting. The drawback of broadcast mode is that it is less reliable, since it cannot support any request-response handshaking procedures that typically improve reliability such as conventional acknowledgement or virtual carrier sensing (RTS/CTS), due to the risk of a “storm” of response packets \[24, 68, 92\]. The CCA application typically requires a PDR of at least 90% \[7\], and it has been suggested in \[22\] that the conventional DCF broadcast protocol may be unable to meet this requirement. Several techniques to improve the reliability of DCF based on RTS/CTS have been proposed. In \[83\] a new protocol, Broadcast Support Multiple Access (BSMA), was proposed which incorporates RTS/CTS in broadcast mode by performing RTS/CTS handshaking to each neighbor individually before sending the DATA packet. However, this introduces excessive overhead on the channel and is not suitable in DSRC environment due to dynamic topology. Also, despite increased complexity, BSMA protocol does not guarantee absolute reliability as is expected of RTS/CTS. Another option is to emulate broadcast communication by sending multiple unicast messages as proposed in Broadcast Medium Window (BMW) \[84\] protocol. In this protocol, a sender polls every node in its neighborhood in a round robin fashion by extending RTS/CTS packets. Although BMW achieves better reliability than standard IEEE 802.11 DCF, it also requires a neighborhood list to be maintained by every node similar to BSMA protocol. BMW protocol is however different from BSMA as it does not require multiple RTS/CTS before data transmission. As such, channel reservation is not guaranteed for all nodes in its neighborhood and a packet may need to transmit multiple times. Also, number of RTS/CTS handshaking increases quadratically as number neighbor nodes increase which makes BMW suitable for only when traffic load is low.

One way to reduce RTS/CTS control packet explosion in broadcast mode, is to
choose a single candidate node for RTS/CTS handshaking. The Urban Multi-Hop Broadcast (UMB) protocol proposed in [55] uses this principle. Although, UMB is proposed for multi-hop directional broadcast of safety message in urban environment, the treatment of hidden terminals can be considered for single hop broadcast as well. In this protocol RTS/CTS control packets are extended for broadcast mode as request to broadcast (RTB) and clear to broadcast (CTB) packets. To select the furthest node in a particular direction as a candidate node for RTB/CTB handshaking all potential candidate nodes send in-band energy burst (a so-called black-burst or jamming signal [77]). The length of the black-burst is proportional to the distance between the receiver and the sender, so the furthest node finishes black-burst transmission last. Although, UMB performs well for reliably flooding safety messages in an urban environment with the help of repeaters installed in road intersections, the performance was not evaluated for single hop broadcast. As safety messages are typically short, multiple stages of RTB/CTB handshaking and black-burst communication for a single safety message transmission can lead to channel congestion. In [34] a dual busy tone multiple access (DBTMA) protocol has been proposed for unicast communication which uses two narrow-bandwidth, out-of-band busy tones. The RTS packets are protected by the transmitter busy tone and the receiver busy tone along with the RTS packet solve the hidden-terminal problem and exposed-terminal problem. However, for broadcast network exposed-terminal problem is not present and as such the use of an extra busy tone is unnecessary. Also, the use of receiver busy tone is not very different than the use of CTS packet and extending of DBTMA protocol for broadcast communication is not trivial. In contrast, we propose an extension based on a single busy tone which is used as negative acknowledgement in this thesis.

Another promising approach is to transmit the broadcast message multiple times [46, 47, 100]. In [47] message repetition is done based on piggybacking feedback information for previous successful packet receptions. With every safety message transmission a list IDs of most recently received messages is sent. Upon reception, a node
can infer negative acknowledgement of its last transmitted message if its ID is not in
the list. Based on such feedback, the piggybacked acknowledgement (PACK) pro-
tocol [46] enables selective retransmission that promises high efficiency of channel
use. However, the protocol is discussed on the conceptual level and details of how
a packet is retransmitted are not presented. In this thesis, we compare the perfor-
mance of our proposed protocol with PACK protocol with analytic modeling. We
also provide explicit technical details for implementing the piggybacked sequential
scheme.

A different approach without feedback is to randomly repeat packets over the life-
time [100]. Among several protocols proposed and evaluated in [100], Asynchronous
Fixed Repetition with Carrier Sensing (AFR-CS) protocol performs best and more
practical. In this protocol, repetition is carried out by all nodes asynchronously
and in fixed predetermined slots. The simulation results suggest up to ten times
improvement in packer reception failure (PRF) with nominal settings. However, in
nominal settings the channel busy time is below 10% and the PRF for IEEE 802.11
is as low as 2% which is well above reliability threshold. In more congested environ-
ment where PRF really needs to improve, AFR-CS improvement is less significant.

In terms of compatibility with the IEEE 802.11p DCF, the protocol extensions are
implemented above MAC in a separate layer. Still, four out six of these protocols
ignore carrier sensing completely and the rest do not follow carrier sensing in a
standard way, i.e., if carrier is not idle the packet is dropped instantly. In the thesis,
we propose retransmission based protocols which can be built on top of standard
IEEE 802.11p DCF. We evaluate our proposed scheme in wide range of channel con-
dition, especially where the standard IEEE 802.11p DCF fails to achieve required
reliability. Also, unlike protocols proposed in [100] we evaluate our protocol for event
safety messages, which are bursty in nature, in addition to routine safety messages.
2.4 Existing Analytical Models

The performance of CSMA/CA protocols, and the IEEE 802.11 DCF mechanism in particular, have been extensively studied in the wireless LAN environment. As we mentioned earlier, several applications envisioned for DSRC, especially safety related ones, rely on broadcast communications. Thus it is essential to consider the differences between broadcast and unicast communications. In this section, we present a short overview of some of the prominent analytical models that fall in two major different categories — unicast and broadcast communications, and discuss their viability for DSRC. We can also classify models according to other attributes such as traffic conditions (saturated versus unsaturated networks) and the presence of hidden terminals.

2.4.1 Models for unicast communication

There has been much work modeling the DCF mechanism in WiFi network for unicast communication [4, 14, 28, 29, 57, 58, 60, 64, 75, 86–88, 93, 98, 99, 106]. Most models follow the mean field approximation and fixed point formulation which was proposed by Branchia in [14] for saturated traffic. In his paper, the backoff process is modeled using a two dimensional Markov chain to accurately determine the collision probability in a fully connected network (i.e. there are no hidden terminals). The mean field approximation used in the model is that each packet collides with a constant and independent probability. This approximation has been adopted in most subsequent models from other researchers to simplify the analysis. Also, the model is based on renewal theory where it is sufficient to analyze a single renewal interval to derive the saturation throughput. The model has been extended in [97, 99] to incorporate maximum retransmission limit before the packet is dropped. Moreover, [29] has incorporated separate channel state during backoff countdown process to improve accuracy of the saturation model. A similar approach [57] to Markov chain model is based on renewal reward theorem where the total backoff period for a
packet is the renewal cycle and the number of attempts is the reward. It provides similar results as the Markov model while being more convenient and intuitive.

A mean-value technique was used to calculate attempt probability per slot in [86] for saturation network. Similar to Markov chain model, this model also involves solving a fixed point system between collision probability and attempt probability. However, the attempt probability is calculated as the inverse of the average number of backoff slots per stage. Similar mean-value technique was used in [75] to calculate the first two moments as well as generating function of access delay. However, all the models presented so far assume saturated traffic which does not account for most typical network communications in DSRC environment.

Maloney et al [64] extended the Markov model to the unsaturated case, but did not consider hidden terminals. They introduced additional states in the two dimensional Markov chain to capture the post-backoff effect and the tagged node’s idle state. To measure the degree of denaturation, additional model parameters are introduced, namely the channel idle probability and the buffer empty probability, and approximations are presented to calculate those parameters. A Poisson arrival process is assumed and the model yields the mean delay, throughput and conditional collision probability. Ticked and Shikar [88] develop an alternative model that is not based on a Markov chain. In the model, they utilize the probability of an empty buffer to account for unsaturated conditions. Each station is modeled as a G/G/1 queue with arbitrary packet arrival and size. The analysis gives expressions for the probability generating functions of the queue length and the delay. However, the analytical results for the collision probabilities show a large mismatch with the simulation results.

All the above mentioned papers assume a fully connected network. Although there exists a wide body of literature analyzing the hidden terminal problem, several limitations of those models are highlighted in [93] for the case of unicast communications. These limitations can be summarized as follows: “One of the fundamental assumptions in Markov chain-based analytical models [14, 64] is the existence of a
Chapter 2. RELATED WORK

renewal point. In the presence of hidden terminals this assumption is not valid due to the desynchronizing of the nodes.” Another modeling approach [5,88] for networks with hidden nodes is to assume independent and geometrically distributed transmission attempts instead of uniformly distributed attempts with an exponentially growing backoff window. Using that assumption, the probability of avoiding a packet collision due to hidden terminals is calculated by noting that a hidden node must not transmit for a number of successive slots during the vulnerable period (i.e. the time period when a transmission by a hidden node will cause a packet collision). However, the assumption may lead to inaccurate results for smaller values of backoff window when the collision probability due to hidden terminals is approaching one. In order to fix the above problems, [93] proposed a new model based on the notion of a fixed slot length instead of a variable length slot and first order dependence of two successive channel states. However, the scope of this model is restricted to a particular network topology with two competing hidden nodes. Also, it is not straightforward to extend the model to the unsaturated case.

2.4.2 Models for Broadcast communication

In contrast to unicast communication, broadcast communication does not support request-response protocol handshaking because it will lead to a “storm” of response messages. As a result, the broadcast mode cannot support positive acknowledgement and retransmission, nor can it have an RTS/CTS mechanism. As such, analytical models developed for unicast communications are not directly applicable to broadcast communication.

In [69], Oliveira et al. proposed an extension to the Markov chain model in [14] to support both unicast and broadcast communications in WiFi networks. They kept the original Markov chain for unicast communication and added an extra set of backoff states to model broadcast communication. The model assumes a saturated single-hop network without any hidden nodes. Another model was proposed by Campily et al. in [21] specifically broadcasting safety messages using IEEE 802.11p.
MAC protocol. For their model, they considered vehicles communicating using multiple channels including a control channel (CC) which is used for safety related and system control messages. All vehicles switch to CC channel every synchronization interval (100ms) for a fixed period of time (CC interval). In the model, they assumed every vehicle contends for channel access at the beginning of a CC interval to transmit one beacon message. Due to this assumption, the performance of the protocol depends greatly on the choice of the contention window as well as the number of contending windows. For instance, when contention window is small, all vehicles contend at the beginning of the CC interval causing high packet loss; whereas by choosing large contention window many packets are lost due to expiry of CC interval. Another model was proposed in [103] to estimate the efficiency and reliability of safety message broadcasting. In particular, they provide a closed form expression for the reliability measure in a saturated network considering interference from hidden nodes as well.

Rad et al. developed an analytical model to determine the probability of packet collision in the broadcast scenario [72]. To capture unsaturation they calculated the steady state probability that a node has a packet to transmit. They modeled each node as a two state Markov chain and expressed the transition probabilities by a set of equations. Though they did not give a closed form expression for the packet transmit probability, the set of equations can be solved numerically. Also, a bufferrers MAC was assumed for the initial modeling and then extended for a MAC with a finite buffer. They also provide a stability and sensitivity analysis for their model. In [95], Vined et al. presented a simpler model to estimate the probability of successful packet reception for beacon messages in the DSRC environment. They captured unsaturation in the model by calculating queue utilization probability and the number of active nodes by multiplying total number of nodes with that probability. Both these papers however assume single hop network without any hidden nodes.

Although there exists a wide body of literature [12, 22, 24, 35, 67, 70, 71, 89, 103]
analyzing the hidden terminal problem, several limitations of those models were highlighted in [93]. The work in [89] is one of the earliest to model hidden terminal for p-persistent CSMA. In this model, the so-called vulnerable period\(^1\) is divided into two parts which are modeled separately. We use a similar approach in this thesis; however, our model is more comprehensive as we consider direct collisions and repeat collisions. In [70, 71] two analytical models are presented which capture the effect of hidden terminals they rely on measurements taken from the underlying network. The models presented in [22, 24] attempted to capture the characteristics of the DSRC safety communications where broadcasting takes place in an unsaturated network with hidden terminals. However, the renewal theory based argument used in this model is not entirely suitable for hidden terminal analysis, as also pointed out in [93]. In particular, the models predict a non-zero successful transmission probability with arbitrary hidden collisions. However, it can be seen that when nodes are always backlogged with packets to send (i.e. in a heavy traffic scenario), the probability of successful transmission can be zero. This is because the transmitting node as well as other hidden nodes always use the same backoff window (i.e. no retransmission is enabled) and the vulnerable period of a node could actually be larger than its backoff window, thus guaranteeing a hidden collision. Note that the models are also inaccurate when there is a very little traffic on the channel. Furthermore, the IEEE 802.11 DCF protocol was not properly modeled since the analysis assumes that a backoff is initiated for each packet at a node irrespective of whether the channel is idle or busy. In this thesis, we addressed these issues and proposed an analytical model to properly capture the effect of hidden terminals for the standard IEEE 802.11p broadcast protocol.

\(^1\)Vulnerable period of a tagged node is the time period during which if any hidden node commences packet transmission it will be colliding with the transmission from the tagged node.
Chapter 3

Analytical Model For Delay And Reliability for Safety Message

In this chapter, we develop an analytical model to evaluate the performance of safety message dissemination in a DSRC environment. The main focus of the model is packet delay and reliability of the IEEE 802.11p DCF protocol discussed in Chapter 2. Although in this chapter we only develop the model for standard broadcast communication, it is extendable for repetition based extensions as we will see in chapter 4-6. The standard protocol for broadcast communication is quite susceptible to the hidden terminal problem in DSRC environment due to lack of its acknowledgement and channel reservation mechanism. Thus, we treat collisions due to hidden terminal separately from direct collisions in this model.

The chapter also provides a description of the system model for the rest of the thesis in Section 3.1 along with a set of modeling assumptions. We also only consider, the CCA safety application in a highway scenario [16, 22, 80, 81, 90] for performance evaluation of the MAC protocol. We limit the context in this thesis, as the traffic environment varies quite drastically depending on the type of roads (e.g. highway, urban road, or country road) and the performance requirements depend on the safety application considered, all of which are quite difficult to capture in a single model. Also, the model does not incorporate vehicle mobility as the time scale for the packet transmission is on the order of milliseconds which is very short for any significant vehicle movement.
Chapter 3. ANALYTICAL MODEL

3.1 System Model

In a DSRC environment, a wide variety of roads such as highway, urban road, or country road are present. Also, traffic environment varies a lot with different flows, densities, and speeds of vehicles. As such, there exists a number of modeling techniques to capture vehicular mobility. Although traffic pattern and mobility are important factors for reliable safety message communication, in our work we mainly focus on evaluation of MAC performance. For the following analysis, we consider a scenario of vehicle-to-vehicle communications for CCA applications on a highway which should give us an indication of the MAC performance in a DSRC environment.

We define the transmission (TX) range and the carrier sense (CS) range to be some region containing the a selected (tagged) vehicle acting as a wireless node. For the rest of thesis, we use the term “vehicle” and “node” interchangeably as we are only concerned regarding the communication aspect of the vehicle. In this section, we discuss some of the major assumptions; the rest of the assumptions appear in the analysis.

Assumption 1. For each node, there are $N_n$ nodes other than itself within the CS range whose transmissions it can sense and collide with, and $N_h$ “hidden” nodes whose transmissions it cannot sense but with whose transmissions its will collide.

Assumption 1 models the case that vehicles are distributed uniformly along a highway, which is narrow compared to the sensing range. So, we can map the vehicle locations on the highway to a single dimension straight line similar to [22]. In the numerical results, we will assume that vehicles form a homogeneous Poisson processes, and there is a transmission radius $R$ such that any vehicle in the range $[R, 2R]$ and $[-2R, -R]$ of the tagged vehicle is a potential hidden terminal. Let $\beta$ be the vehicle density in vehicles per meter on the highway. The average number of vehicles in the transmission range of the tagged vehicle including the tagged node is $N_n = 2\beta R$, and the average number of vehicles in the potential hidden terminal area is $N_h = 2\beta R$. 
Assumption 2. If a packet transmission by a node overlaps in time with one by any of its $N_n + N_h$ nodes, then both packets will be irretrievably corrupted.

Assumption 2 implies that there is no capture effect, and that the error correcting codes used are insufficient to recover packets from collisions. Also, we consider only collision related packet losses, and not those due to channel error. So, a node within the transmission range $R$ of the transmitter can reliably decode the message if no collision occurs. In chapter 5, we introduce “batch retransmission scheme”, an extension of the MAC protocol, where multiple copies of the same packet is transmitted back to back as a single transmission for increased reliability. Assumption 2 is relaxed for that scheme, as a collision may not necessarily destroy all the copies and at least one copy of the packet can still be decoded correctly at the receiving node.

Assumption 3. The transmission attempts of each node are independent of those from other nodes, except for the effect of carrier sensing. Moreover, the collision probability and probability of an arriving packet observing the channel busy are both constant regardless of the node’s state.

Assumption 4. All nodes generates safety packets according to independent Poisson processes, each with rate $\lambda$ [packets/sec].

Assumption 3 and the Poisson nature of assumption 4 are common in performance studies of the MAC protocol in mobile wireless ad-hoc networks [22] and help make the model analytically tractable, while still yielding meaningful indications of MAC performance.

Assumption 5. If a packet arrives when the channel is idle, it will not suffer a collision with any node within distance $R$.

To appreciate assumption 5, recall that when a packet arrives and finds the channel idle for DIFS period, the vehicle immediately sends the packet without performing a backoff. In this case, a collision can occur only when another packet is
generated at some other vehicle within the propagation delay. As the propagation delay in the studied transmission range is on the order of microseconds, we ignore any collisions of this type. In contrast, after a packet transmission, every vehicle waiting for safety message transmission initiates backoff process. During backoff every vehicle waits for a random number of slots uniformly distributed in the range $[0, CW - 1]$, where $CW$ is the contention window. If more than one vehicle selects the same number of backoff slots, then they start transmission on the same slot and a collision occurs.

**Assumption 6.** The probability of a given transmission colliding with more than one other transmissions is negligible.

Assumption 6 arises since multiple transmissions within a short period are a second-order effect when the load is relatively light. This assumption makes our results optimistic when the load is high, especially for batch retransmissions.

Apart from these main assumptions that are used for the rest of the thesis, other assumptions are introduced in later chapters as necessary. For instance, in chapter 5 we classify safety messages in two categories—routine safety messages transmitted at a regular interval and event safety messages transmitted as a result of some emergency events. We discuss them in detail in chapter 5 and for this chapter we treat both safety messages similarly.

In the next three sections, our objective is to develop an approximation to compute the collision probability and the packet delay experienced by the tagged vehicle. To this end, the fixed point approximation is established by combining the set of equations for the collision probability expressed in terms of the mean service time experienced by each packet sent by the tagged node, with an opposing set of equations for the mean service time expressed in terms of the collision probability. In Section 3.2 we calculate the direct collision probability, $d$ which is dependent on the probability $b$ that the channel is busy and queue utilization, $\rho$. In Section 3.4 we calculate the average service time of the packet, $E[S]$ where the service time, $S$, ...
is the sum of the time required for a node to acquire channel access and to trans-
mit the packet once the packet reaches the head of the queue. The average service
time, $E[S]$ again depends on $b$ and $\rho$. Now, for any single server queue, the queue
utilization, $\rho$ only depends on the average service time, $E[S]$ and the packet arrival
rate, $\lambda$ as expressed in the following equation

$$\rho = \lambda E[S], \quad (3.1)$$

Thus we form the set of equations for the fixed point calculation involving $d$, $b$, $\rho$,
and $E[S]$.

Now, note that calculating hidden terminal collisions probability in Section 3.3
is not involved in the fixed point. However, to calculate the packet delivery ratio
we need to consider probability of both collisions due to hidden terminal and direct
collisions, and thus the fixed point is required. When we show results for the delay
and PDR in Section 3.5 we observe that collisions due to hidden terminal is the major
cause of packet collision. With this insight about the cause of packet collision, we can
simplify the model by ignoring direct collision altogether and calculating the packet
delivery ratio directly based on the hidden terminal collision without requiring to
solve the fixed point which is done in Chapter 6.

In the following derivations, many quantities are distinguished by subscripts and
superscripts. For brevity, we use notation of the form $A_{j \in J} = f(j)$ to mean that
$A_j = f(j)$ for each $j \in J$.

### 3.2 Direct Collision

In this section, we derive the collision probability without accounting for hidden
terminals (i.e. “direct” collisions only), and in the next section, we modify the
model to allow for hidden terminals. We define $d$ as the direct collision probability,
which depends on the queue utilization factor, $\rho$ defined in (3.1) and the probability,
To calculate the collision probability of safety messages, we consider different scenarios that can confront a newly-generated packet in a vehicle in an unsaturated network. When the packet reaches the transmission queue, the queue may be either empty or non-empty. Also, before the packet is transmitted the node senses the channel for a DIFS period and if the channel is idle for the whole DIFS period then the transmission takes place. For reasons discussed later, we are only interested in channel idle/busy events for non-empty queue and thus we combine these events in to three scenarios as following:

1. A packet arrives to an empty buffer and finds the channel completely idle during the first DIFS period,

2. A packet arrives to an empty buffer and finds the channel not idle anytime during the first DIFS period,

3. A packet arrives to a non-empty buffer.

For the first case, the vehicle immediately sends the packet without performing a backoff. In this case, a collision can occur only when another packet is generated at some other vehicle within the propagation delay. As the propagation delay in the studied transmission range is on the order of microseconds, we can ignore any collisions of this type according assumption 5. So, the probability that the buffer is empty when a packet arrives is given by $1 - \rho$ where $\rho$ is the queue utilization factor defined in (3.1). Similarly, the probability that the channel is sensed idle for DIFS period is $1 - b$ where the expression for $b$ is to be derived later in this section. So, the probability for the first case is $(1 - \rho)(1 - b)$. Note that only in the first case, the packet does not go through a backoff process.

In the second case, the joint probability of a packet arrival to an empty buffer and the channel being busy at least once during the DIFS period due to transmission by other vehicles is $(1 - \rho)b$. 

$b$, that the channel is busy to be calculated later in this section.
For the last case, the probability of a packet arrival to a non-empty buffer is $\rho$. Note that for the last two cases, the packet must undergo the backoff process before it is transmitted. After the backoff counter reaches zero, the tagged vehicle sends the packet in the following slot, and if another vehicle sends a packet at the same slot, a collision occurs and the packets are lost.

Now, we calculate the busy probability, $b$, by quantifying the portion of time the channel is busy due to transmissions. We have $N_n$ vehicles other than the tagged vehicle transmitting $\lambda$ [packets/sec]. Also, we define $T$ as the complete transmission time of a packet including DIFS, $T = t_{data} + t_{difs}$, where $t_{data}$ is the transmission time of a packet and $t_{difs}$ is the duration of DIFS period. The reason for using complete transmission time including DIFS period instead of just using packet transmission time requires justification. Recall that, $b$ is the probability of finding the channel busy for a complete DIFS period. Another way to define $b$ is to define it as the probability that either any node is transmitting or about to transmit within the next DIFS period when the tagged node starts sensing. Also, note that the channel is always idle during the DIFS period prior to a transmission by any node. As such, we can combine the transmission time and the associated DIFS period as a complete transmission time, $T$, for each packet transmission. Now, if there is no collision, then all the packet transmissions in the CS range should take a fraction $T = N_n\lambda T$ of the time. However, when a collision occurs, exactly two nodes are involved (assumption \footnote{[ ]}), and their two transmissions coincide exactly due to carrier sensing. Thus, the transmission time to send the packets which collide is reduced by $N_n\lambda d/2T$ where $d$ is the probability that a packet is involved in a direct collision. Subtracting this from $T$ gives

$$b = N_n\lambda(1 - d/2)T. \quad (3.2)$$

Let $\tau$ be the probability that a vehicle attempts to transmit in an arbitrary slot
Chapter 3. ANALYTICAL MODEL

given that it has a packet in the queue. This is

\[ \tau = \frac{1}{(\bar{W} + 1)}, \]

(3.3)

where \( \bar{W} = (W - 1)/2 \) is the average number of backoff slots preceding a transmission. In contrast to the fixed point of Branchia \[14\], \( \tau \) is not part of the current fixed point because nodes never retransmit.

For any vehicle other than the tagged vehicle, the probability of transmitting in any arbitrary slot is \( \rho \tau \). A collision occurs when any of the \( N_n \) vehicles transmit in the same slot as the tagged vehicle given that the tagged vehicle sees either of the last two cases. So, the direct collision probability is given by

\[ d = (1 - (1 - \rho)(1 - b))(1 - (1 - \rho \tau)^{N_n}). \]

(3.4)

3.3 Hidden Terminals

In the previous section, we obtained the collision probability assuming no hidden terminals. Now we present an approach to calculate the PDR taking into account collisions due to hidden terminals. The PDR, however, also relies on the direct collision probability, \( d \), calculated in Section 3.2.

For a tagged packet to be successfully received, both of the following must occur. First, when the tagged vehicle starts its transmission, none of the hidden terminals can be in what we call the transmitting state; we call this event \( H^b \) (“hidden, before”). A hidden terminal is said to be in the transmitting state if it is either transmitting a packet or deferring for a DIFS period associated with an imminent packet transmission. Second, after the tagged vehicle starts its transmission given \( H^b \), none of the hidden terminals should start transmitting until after the tagged vehicle is finished; we call this conditional event \( H^a \) (“hidden, after”). As \( H^a \) is defined as a conditional event, the probability that both events occur is \( P(H^a) \cdot P(H^a) \).

The reason for splitting vulnerable period into two parts is that, although packets
arrive in the queue following a Poisson process, due to the channel access scheme of the CSMA/CA protocol packet transmissions are bursty. This is similar to how the vulnerable period was treated in [89].

Now, for event $H^b$, we follow a similar argument as (3.2) to calculate the probability of finding all hidden terminals in the non-transmitting state. We note that the event $H^b$ is the complement of the event of finding at least one hidden terminal in the transmitting state; we denote this complementary event as $H^b$. As we have $N_h$ hidden terminals transmitting $\lambda$ [packets/sec], if there is no direct collision, then all the packet transmissions should take $N_h\lambda T$ time each second. However, due to direct collisions among hidden terminals some packet transmissions will overlap. With the direct collision probability of $d$, we have $N_h\lambda d$ such overlapping packets. If we assume no direct collision involving three or more packets, the transmission time to send the collided packets would be $N_h\lambda Td/2$. Adjusting for this collision period we can express the probability of event $H^b$ as

$$P(H^b) = 1 - P(H^b) = 1 - N_h\lambda T(1 - d/2).$$  (3.5)

For event $H^a$, we need to calculate the probability that a packet is generated by the hidden terminal after the tagged vehicle starts its transmission and eventually collides with the transmission of the tagged vehicle. Note that packets generated at the hidden terminal in the last time portion of one DIFS period of the tagged vehicle’s transmission will not collide because the hidden terminal will still be deferring for a DIFS period when the tagged vehicle finishes its transmission. The combined packet arrival process from all the hidden terminals is a Poisson process and the total number of transmission attempts per second is $\lambda N_h$. Therefore, the condition $H^a$ is met if no packet is generated at any of the hidden terminals during $t_{data} - t_{difs}$ period and the probability of such an event is expressed as

$$P(H^a) = e^{-\lambda N_h(t_{data} - t_{difs})}.$$  (3.6)
Recall that the PDR is defined as the probability of delivering the packet to all intended receivers within the transmission range of a given transmitting node. As such, considering the fact that direct collisions and collisions due to hidden terminals are independent of each other, the packet delivery ratio for hidden terminal case can be expressed as

$$PDR = (1 - d) \cdot P(H^b) \cdot P(H^a).$$  \hspace{1cm} (3.7)

In this section, we derive the expression for PDR considering both direct collisions and collision due to hidden terminals. However, the fixed point is not complete yet as $\rho$ depends $E[S]$ for which we do not have any expression yet. In the next section, we derive an expression for mean service time, $E[S]$, to complete the fixed point.

### 3.4 Delay Calculation

In Section 3.2 and Section 3.3 we calculated PDR based on direct collisions and hidden terminal collision. In this section, we derive an expression for the mean service time of a tagged packet, $E[S]$, which is a part of the fixed point calculation described in 3.1. We also calculate the mean total delay of a tagged packet, $E[D]$.

The total delay (or sojourn time) experienced by a packet of a tagged vehicle includes the waiting time of the packet in the queue, $Q$, the access delay, $A$ and the complete time to transmit the packet, $T$. We denote the total delay of the packet by $D$ and write it as

$$D = Q + S = Q + A + T,$$  \hspace{1cm} (3.8)

where $Q$, $S$, and $A$ are random variables (r.v.’s) representing the queuing delay, service time, and access delay respectively and $T$ is the complete transmission time. The service time of the queue $S$ is defined as the sum of the access delay $A$ and the transmission delay $T$. The access delay, $A$, is defined as the time interval between the instant the packet reaches the head of the queue, to the instant when the packet
transmission starts. For each packet transmission, the channel is occupied for the duration of the actual packet transmission \( t_{\text{data}} \) and one DIFS. As such, we define the complete transmission time \( T \) as the sum of the actual packet transmission time and one DIFS period.

Recall that, for a newly arrived packet the probability of a non-empty buffer is \( \rho \), and the probability of finding the channel busy is \( b \). So, to determine the access delay, we refer to the three scenarios considered in Section 3.2 with corresponding probabilities.

1. A packet arrives to an empty buffer and finds the channel completely idle during the first DIFS period with probability \((1 - \rho)(1 - b)\). The access delay in this case is zero as the tagged vehicle transmits the packet without any backoff.

2. A packet arrives to an empty buffer but finds the channel not idle anytime during the first DIFS period with probability \((1 - \rho)b\). The vehicle must wait until the ongoing transmission is finished and then perform a backoff before transmitting the packet.

3. A packet arrives to a non-empty buffer with probability \( \rho \) and when it reaches the head of the queue, a backoff is performed before transmitting the packet.

We can express the access delay according to the above three cases as

\[
A = \begin{cases} 
0 \quad \text{w.p.} \quad (1 - \rho)(1 - b), \\
B + T_{\text{Res}} \quad \text{w.p.} \quad (1 - \rho)b, \\
B \quad \text{w.p.} \quad \rho, 
\end{cases} \tag{3.9}
\]

where \( T_{\text{Res}} \) is the residual lifetime of an ongoing packet transmission, \( B \) is the total backoff duration including periods when the backoff counter is suspended, and the notation ‘w.p.’ stands for ‘with probability’.
During the backoff process, every slot can be interrupted by successful transmissions or collisions of packets transmitted by other vehicles. During the interruption, the backoff counter is suspended and when the backoff counter is resumed, it starts from the beginning of the interrupted slot. For simplicity, we assume every backoff slot can be interrupted at most once. This simplification should not have a significant impact on accuracy, since the probability of multiple interruptions to the same slot is small. Thus, we can express $B$ as a random sum

$$B = \sum_{n=1}^{U} (\sigma + Y),$$

(3.10)

where $\sigma$ represents the duration of a backoff slot, $Y$ is the interruption period per slot, and $U$ is the backoff counter value which is uniformly distributed in the range $[0, W - 1]$.

If no other vehicle transmits in a given slot, an interruption does not occur and $Y$ equals zero. If one or more vehicles transmit in that slot, then the tagged vehicle will suspend its backoff process for the duration of the complete transmission, $T$. Recall that the probability that a vehicle attempts to transmit in an arbitrary slot given that it has a packet in its buffer is given by $\tau$ and the probability that the buffer is non-empty is $\rho$. Therefore, the probability of a vehicle transmitting in an arbitrary slot is $\rho \tau$ and a backoff slot of the tagged vehicle is interrupted when any of the other $N_n$ vehicles transmit in that slot, which occurs with probability $1 - (1 - \rho \tau)^{N_n}$. Therefore, we can write $Y$ as

$$Y = \begin{cases} 0 & \text{w.p.} \ (1 - \rho \tau)^{N_n}, \\ T & \text{w.p.} \ 1 - (1 - \rho \tau)^{N_n}. \end{cases}$$

(3.11)

where $1 - (1 - \rho \tau)^{N_n}$ is the probability that a slot is busy due to transmissions by other vehicles.
Chapter 3. ANALYTICAL MODEL

3.4.1 Mean and Standard Deviation

In this subsection, we determine the mean and standard deviation of the service time and the mean of the total delay. We express them using means and variances of the constituent random variables. From (3.8), since $A$ and $T$ are independent, we can write

$$E[S] = E[A] + E[T], \quad (3.12)$$

$$\text{StdDev}[S] = \sqrt{\text{Var}[S]} = \sqrt{\text{Var}[A] + \text{Var}[T]}, \quad (3.13)$$

where $E[X]$, $\text{StdDev}[X]$ and $\text{Var}[X]$ denotes the mean, standard deviation and variance of the random variable $X$. To calculate the mean total delay, $E[D]$ we need to calculate the mean queueing delay, $E[Q]$ as well. According to assumption 3 packets arrive at each node following a Poisson process, each node can be treated as an M/G/1 queue. As such, the queuing delay can be calculated using Pollard's Chi-nacrine formula [52] as

$$E[Q] = \frac{\lambda(\text{Var}[S] + E[S]^2)}{2(1 - \lambda E[S])}, \quad (3.14)$$

where $\text{Var}[S]$ is calculated from (3.13). The mean total delay is just the sum of mean service time and mean queuing delay, given by

$$E[D] = E[Q] + E[S]. \quad (3.15)$$

Considering fixed length packets for all vehicles, we have

$$E[T] = T, \quad (3.16)$$

$$\text{Var}[T] = 0. \quad (3.17)$$

From (3.9) the mean and variance of $A$ can be written as

$$E[A] = (1 - \rho)b(E[B] + E[T_{Res}]) + \rho E[B], \quad (3.18)$$
\[
\text{Var}[A] = (1 - \rho)(1 - b) E[A]^2 \\
+ (1 - \rho)b(\text{Var}[B] + \text{Var}[T_{\text{Res}}] \\
+ (E[A] - E[B] - E[T_{\text{Res}}])^2) \\
+ \rho(\text{Var}[B] + (E[A] - E[B])^2).
\] (3.19)

To calculate the mean and variance of the residual lifetime of an ongoing transmission, \( T_{\text{Res}} \), we first determine the probability distribution function of \( T_{\text{Res}} \). Note that the inter-arrival time of packets generated at each vehicle follows a memoryless exponential distribution with rate \( \lambda \). So the interval between the starting time of an ongoing transmission and the arrival of a new packet at the tagged vehicle also follows an exponential distribution and we define it as \( X \sim \text{Exp}(\lambda) \) where \( \text{Exp} \) represents the Poisson distribution. Therefore, we can represent the distribution of \( T_{\text{Res}} \) as the remaining transmission time, \( Y = T - X \), conditioned on \( X \leq T \).

Now, the probability distribution function of \( Y \) can be expressed as \( F_Y(y) = 1 - F_X(T - y) \), where \( F_Z(\cdot) \) here represents the distribution function of \( Z \). Applying the condition \( X \leq T \), we get

\[
F_{Y|X\leq T}(y) = 1 - F_{X|X\leq T}(T - y) = \frac{e^{-\lambda(T-y)} - e^{-\lambda T}}{1 - e^{-\lambda T}}.
\] (3.20)

Differentiating (3.20), we obtain the probability density function as

\[
f_{Y|X\leq T}(y) = \frac{\lambda e^{-\lambda(T-y)}}{1 - e^{-\lambda T}}.
\] (3.21)

Now, we can obtain the mean and variance of \( T_{\text{Res}} \) from (3.21) as follows:

\[
E[T_{\text{Res}}] = E[Y|X \leq T] = \int_0^T y f_{Y|X\leq T}(y) dy \\
= \frac{T}{1 - e^{-\lambda T}} - \frac{1}{\lambda},
\] (3.22)

\[
E[T_{\text{Res}}^2] = E[Y^2|X \leq T] = \int_0^T y^2 f_{Y|X\leq T}(y) dy
\]
Chapter 3. ANALYTICAL MODEL

\[
T^2 - 2T/\lambda + 2/\lambda^2,
\]

(3.23)

\[
\text{Var}[T_{Res}] = E[T_{Res}^2] - E[T_{Res}]^2 = \frac{1}{\lambda^2} - \frac{T^2 e^{-\lambda T}}{(1 - e^{-\lambda T})^2},
\]

(3.24)

Using well-known identities for the mean and variance of a random sum \[30\], it follows from (3.10) that

\[
E[B] = (\sigma + E[Y]) E[U],
\]

(3.25)

\[
\text{Var}[B] = \text{Var}[Y] E[U] + (\sigma + E[Y])^2 \text{Var}[U].
\]

(3.26)

As \( U \) is a r.v. which is uniformly distributed in the range \([0, W - 1]\), we have

\[
E[U] = \bar{W} = \frac{W - 1}{2},
\]

(3.27)

\[
\text{Var}[U] = \frac{W^2 - 1}{12}.
\]

(3.28)

For the interruption time \( Y \), we can calculate the mean and variance from (3.11) as

\[
E[Y] = (1 - (1 - \rho \tau)^N) T,
\]

(3.29)

\[
\text{Var}[Y] = (1 - (1 - \rho \tau)^N)(1 - \rho \tau)^N)(1 - (1 - \rho \tau)^N) T^2.
\]

(3.30)

Thus, based on (3.12)–(3.30), we can derive the mean and standard deviation of the service time in terms of \( b \) and \( \rho \). Now (3.1), (3.4), (3.2), and (3.12) constitute a non-linear system of equations that can be solved iteratively to calculate \( \rho, b, d, \) and \( E[S] \). The set of equations for this fixed point system is summarized in Fig. 3.1. This completes the Section 3.2 and Section 3.3 to allow PDR to be calculated from (3.7).
Chapter 3. ANALYTICAL MODEL

\[ \rho = \lambda E[S] \]  \hspace{2cm} (3.1)

\[ b = N_n \lambda (1 - d/2) T \]
\[ d = (1 - (1 - \rho)(1 - b))(1 - (1 - \rho \tau)N_n) \]  \hspace{2cm} (3.2) (3.4)

\[ E[Y] = (1 - (1 - \rho \tau)N_n)T \]
\[ E[B] = (\sigma + E[Y])E[U] \]
\[ E[A] = (1 - \rho)b(E[B] + E[T_{Res}]) + \rho E[B] \]  \hspace{2cm} (3.29) (3.25) (3.18)

\[ E[S] = E[A] + E[T] \]  \hspace{2cm} (3.12)

Converges? No

Yes

\[ P(H^b) = 1 - P(H^b) = 1 - N_n \lambda T(1 - d/2) \]  \hspace{2cm} (3.5)

\[ P(H^a) = e^{-\lambda N_n(t_{data} - t_{init})} \]  \hspace{2cm} (3.6)

\[ PDR = (1 - d) \cdot P(H^b) \cdot P(H^a) \]  \hspace{2cm} (3.7)

Figure 3.1: Summary of the equations involved in the fixed point system
3.5 Simulations

In this section, we present the simulation setup used to validate our analytical model and present the validation results. We used the nos simulator (version 2.28) \cite{2} to simulate and obtain packet delay and PDR in a DSRC environment under various conditions. To make the simulation results repeatable by others we provide detail description of the simulation settings. Some of the modeling assumptions presented in Section 3.1 are also applied to simulation as advised in \cite{78}. We adopted the patch for ns-2.28 provided in \cite{76} where they fixed the following bug. According to the IEEE802.11 specification \cite{43} (see Fig. 2.1), if the medium is sensed idle when a packet arrives at the MAC layer, the packet can be transmitted after an idle period of DIFS without any backoff. However, in the standard distribution of ns-2.28, a backoff is always started irrespective of whether the channel is idle or busy.

We use a ring topology in the simulation where we place vehicles on a circle to avoid any unwanted effects of stations located at the edge of the network. A similar technique is used in \cite{33} where a spherical surface is used to approximate a two dimensional disk to avoid edge effects. The perimeter of the circle is kept at least ten times larger than the transmission range of each vehicle so that the highway scenario is actually simulated. The vehicles are placed uniformly at random on the circle where the average inter-vehicle distance is a function of vehicle density, $\beta$. Each vehicle is configured to broadcast messages with varying packet size, $P$ and packet arrival rate, $\lambda$ following an unit disk model where the carrier sense range is the same as the transmission radius, $R$. All the other DSRC related parameters are listed in Table 3.1.

In the following, we validate our analytical model by comparing the numerical results with the simulation results. We present results for the mean total delay, the standard deviation of the access delay, and the PDR. Another objective of our numerical experiments is to investigate the effect of different load conditions on the delay and PDR. All the simulation results are plotted with 95% confidence intervals.
Table 3.1: DSRC System Parameters for Single Transmission Scheme

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>16</td>
<td>Range, $R$</td>
<td>0.5 km</td>
</tr>
<tr>
<td>Slot size, $\sigma$</td>
<td>16 $\mu$s</td>
<td>SIFS</td>
<td>32 $\mu$s</td>
</tr>
<tr>
<td>PHY preamble</td>
<td>32 $\mu$s</td>
<td>PLOP header</td>
<td>8 $\mu$s</td>
</tr>
<tr>
<td>Vehicle density, $\beta$</td>
<td>10 – 200 vehicles/km</td>
<td>Data rate, $R_d$</td>
<td>12, 24 Mbps</td>
</tr>
<tr>
<td>Packet arrival rate, $\lambda$</td>
<td>2, 10 packets/sec</td>
<td>Packet length, $P$</td>
<td>200, 400 bytes</td>
</tr>
</tbody>
</table>

Figure 3.2: Total delay for direct collision using the following parameter set: (data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes])

We first present and discuss results for the direct collision case. In Fig. 3.2, we plot the mean of the total delay (3.15) as a function of vehicle density, $\beta$, with different curves parameterized by the data rate $R_d$ [Mbps], packet arrival rate $\lambda$ [packets/sec], and packet size $P$ [bytes]. Observe that our analytical model agrees well with the simulation results. In the plotted range, the mean delay increases...
almost linearly with the vehicle density, with the slope for the $\lambda = 10$ case being larger than the $\lambda = 2$ case. The biggest delay observed is less than 0.5 ms which is well below the maximum delay constraint of 100 ms for safety applications [62].

In Fig. 3.3, we study the accuracy of our model in terms of the standard deviation. Note that we use the standard deviation of the service time in (3.13) as a proxy for the standard deviation of the total delay. We observe from the figure that the standard deviation for all cases is of the order of microseconds for low vehicle densities. This is because the channel is mostly idle and no backoff is required by the vehicles. With increasing vehicle density, the standard deviation increases almost linearly. We note that the analysis matches well with the simulation results for all cases. Figs. 3.2 and 3.3 give us an indication of the distribution of the delay. For example, for M/M/1 queue, the mean and the standard deviation of the total delay is same [30]. But, our results show significant differences in mean and standard
deviation, which confirms the need to use an M/G/1 queue model instead of the M/M/1 queue for each node.

Next, we plot the probability of no direct collisions in Fig. 3.4, where the analytical results PDR is the complement of the direct collision probability in (3.4). The analysis provides a reasonable match with the simulation results. For the $\lambda = 2$ case, we see that the PDR is above 99% for all vehicle densities; however, for the $\lambda = 10$ case, the PDR drops with increasing vehicle density.

For the hidden terminal case, the distribution of the packet delay is the same as for the direct collision case. This is because there is no retransmission and the presence of hidden terminals does not affect the backoff process of the tagged vehicle. For this reason we omit the results for the mean and standard deviation of the delay when there are hidden terminals.

In Fig. 3.5 we plot results for the PDR according to (3.7) which accounts for
hidden terminals and compare them with simulation. The PDR is above 90% for all cases under light load ($\beta \leq 20$) but drops linearly with increasing vehicle density. For higher vehicle densities, the PDR eventually drops below the reliability requirement of 90% for DSRC safety applications. We also observe that the PDR for the $\lambda = 10$ cases are much worse than that of the $\lambda = 2$ case. From Figs. 3.4 and 3.5 we can compare the PDR values obtained for the hidden terminal case with that for the direct collision case. Our comparative results show that packet collision due to hidden terminals is the major source of collisions and direct collision only accounts for unto 10% of the total collision. This observation has a significant impact on the modeling for the PDR. If we ignore direct collision, we can directly calculate the delay without the fixed point. In Chapter 6 we use this approach to calculate the PDR of the safety packet transmission.

In Fig. 3.6 we compare our analytical model with the model of Chen et al. [22].
Chapter 3. ANALYTICAL MODEL

Figure 3.6: Comparison of packet delay with Chen et al.’s model \cite{22} using the following parameter set: (data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes])

We plot the mean total delay versus vehicle density for the case where the data rate is 24 [Mbps], packet arrival rate is 10 [packets/sec], and packet size is 200 [bytes]. Observe that Chen’s model significantly overestimates the delay. This discrepancy in the delay can be explained as follows. In \cite{22}, the authors assumed that for every packet, a backoff is performed before transmission, whereas according to the IEEE 802.11 DCF standard, no backoff is required if a newly generated packet arrives to an empty buffer and the channel is sensed idle for a DIFS period \cite{43} (see Fig. 2.1). To clearly identify the source of improvement and accuracy in our model, we evaluate our model under the assumption that every packet undergoes backoff before transmission, and plot the resulting mean total delay as “Approximate Analysis” in Fig. 3.6. This result is close to that of Chen et al.’s model, confirming that the main improvement in our model compared to Chen et al.’s model in terms of delay stems from the correct handling of packets that do not undergo a backoff.
The PDR results from our model and Chen et al.’s model are compared in Fig. 3.7. Observe again that our model is a much better match with the results obtained from the ns2 simulation. Again we plot the PDR results under the assumption that every packet undergoes backoff (labeled “Approximate Analysis”), and we observe that the previous discrepancy in the delay does not account for the large inaccuracy of PDR in Chen et al.’s model. In our model, we divide the vulnerable period into two parts — before the tagged node starts transmission and after the tagged node starts transmission, and treat them differently in contrast to a single vulnerable period in Chen et al.’s model. Also, the model in [22] assumes that the vulnerable period could be divided into a number of independent variable slots. This assumption, however, is not accurate when the average backoff duration is smaller than the vulnerable period itself [93].

For DSRC safety applications, the maximum packet delay should be constrained
Table 3.2: Packet Delay for DSRC Safety Messages

<table>
<thead>
<tr>
<th>$R_d$ [Mbps]</th>
<th>$\lambda$ [packets/sec]</th>
<th>$P$ [bytes]</th>
<th>$\beta$ [vehicles/km]</th>
<th>Mean [ms]</th>
<th>Mean+S.D. [ms]</th>
<th>Mean+3S.D. [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>2</td>
<td>200</td>
<td>10</td>
<td>0.26</td>
<td>0.28</td>
<td>0.32</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>200</td>
<td>100</td>
<td>0.27</td>
<td>0.33</td>
<td>0.46</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>200</td>
<td>200</td>
<td>0.28</td>
<td>0.38</td>
<td>0.57</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>200</td>
<td>10</td>
<td>0.18</td>
<td>0.22</td>
<td>0.28</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>200</td>
<td>100</td>
<td>0.22</td>
<td>0.33</td>
<td>0.55</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>200</td>
<td>200</td>
<td>0.29</td>
<td>0.47</td>
<td>0.83</td>
</tr>
<tr>
<td>24</td>
<td>10</td>
<td>400</td>
<td>10</td>
<td>0.25</td>
<td>0.30</td>
<td>0.38</td>
</tr>
<tr>
<td>24</td>
<td>10</td>
<td>400</td>
<td>100</td>
<td>0.32</td>
<td>0.49</td>
<td>0.81</td>
</tr>
<tr>
<td>24</td>
<td>10</td>
<td>400</td>
<td>200</td>
<td>0.46</td>
<td>0.75</td>
<td>1.34</td>
</tr>
</tbody>
</table>

rather than the mean delay. To get an estimate on the maximum packet delay, we add one and three standard deviations to the mean delay and present them in TABLE 3.2. It can be seen that the maximum value of the delay in Table 3.2 is 1.34 ms which is still well below the delay constraint of 100 ms reported in [62].

3.6 Conclusion

In this chapter, we have developed an analytical model to evaluate the performance of the DSRC MAC protocol for safety applications. We have addressed the challenging task of modeling the significant detrimental effect of hidden terminals and have verified our model for CCA applications in highway scenario by network simulation. Insights gained from the results show that collision due to hidden terminal is the major cause of loss of reliability in DSRC environment. As such, in Chapter 6 we remove the fixed point calculation from the analytical modeling by completely ignoring direct collision.
Apart from reliability, packet delay is the other performance criteria considered in this chapter. However, in the simulated DSRC environment, the delay is found to be too low to have any negative impact on the performance. The reason for low delay is single hop broadcast communication without any retransmission. In chapter 4–6, we consider a few extensions over the standard MAC protocol, in which each packet is retransmitted multiple times to improve reliability at the cost of extra delay.
Chapter 4

Retransmission Based MAC Protocol Extensions

In the previous chapter, we have developed an analytical model to evaluate performance of safety message dissemination in DSRC environment. From the results and discussion, it is clear that, although the delay is quite low for safety message dissemination, the IEEE 802.11p DCF protocol is unable to meet the QoS requirement for reliability. So, the protocol would be more useful if the reliability can be improved even at the cost of some delay. It motivates us to propose two extensions to the existing MAC protocols where the main principle is to retransmit the safety packets for improved reliability.

In the first scheme (referred to as “NACK sequential scheme”), we propose an out-of-band signalling to send negative feedback or NACK from the receiver. Hearing NACK from the receiver(s), the sender then can retransmit the safety packets. So, this retransmission based scheme relies on some form of feedback. In the second scheme (referred to as a “blind sequential scheme”) we do not rely on any feedback and retransmit safety messages a fixed number of times. As there is no feedback mechanism, the blind sequential scheme generates more load on the channel compared to NACK sequential scheme. In this chapter, we evaluate the performance of the above two schemes and discuss whether or not the additional complexity of the NACK sequential scheme reflects on the performance. In Sections 4.2 and 4.3 we extend the analytical model developed in Chapter 3 to model packet retransmissions. We present the delay and PDR results for the proposed schemes in Section 4.4. We then conclude the chapter in Section 4.5.
4.1 Extensions

In this section, we describe the two proposed extensions to the standard DSRC MAC protocol — NACK sequential scheme and blind sequential scheme. In both schemes, safety messages are sent multiple times to improve reliability. However, in NACK sequential scheme, a packet is only retransmitted if the sender receives a negative feedback, whereas in blind sequential scheme a fixed number of retransmission attempts is made for each packet. The benefit of using feedback is less overhead on the channel, specially when the collision probability is low. On the other hand, blind sequential scheme is simpler to implement and does not rely on any out-of-band signalling.

4.1.1 NACK Sequential Scheme

In the NACK sequential scheme we do not use any extended RTS/CTS or similar mechanisms to combat hidden terminals in broadcasting [48], [13]. Instead, we propose an out-of-band receiver-based busy tone to represent a NACK signal back to the source. As the busy tone only represents 1 bit information about the latest unsuccessful packet, a narrow bandwidth is sufficient for this purpose. To listen to the busy tone, a simple energy detector would suffice rather than a fully-fledged transceiver.

The NACK is sent by the receiver at the end of the collision period when all the involved nodes have finished their transmission. Note that when the receiver starts transmitting the NACK busy tone other nodes have already finished transmitting and as such not interfere with the reception of the busy tone. This is immediately after one node finishes transmission, but for the other node there is a gap between when it finishes its transmission and when it hears NACK. This gap duration can be as large as the packet transmission time. During this period any other node can start transmitting its own packet. To avoid this situation, we increase the DIFS duration by at least one packet transmission time. However, this non-standard
size of DIFS causes loss of compatibility with the IEEE 802.11p standard and also makes it difficult to implement NACK scheme in DSRC wireless cards. As such we investigate other schemes which provide similar performance while being compatible with the standard in later chapters.

If the sender (or source) senses the busy tone (i.e. hears a NACK), it will perform a backoff and send the last packet again until the packet is received by all the nodes or the maximum transmission attempt, $m$, is reached. In the latter case, the packet is dropped. Because we do not use any handshake procedures (such as RTS/CTS) to avoid potential hidden collisions (i.e. collisions that are caused by hidden terminals), the same hidden nodes can collide again in the following retransmission attempts. To avoid successive collisions due to the same hidden terminals, we propose to separate the retransmission attempts using different backoff windows for different nodes involved in the collision. The backoff windows are larger compared to the transmission time of a packet so that one node can finish transmitting its packet while the other node is still backing off with high probability. The larger backoff window is used by the node finishing its transmission later than the other node. To determine which node finishes later, we assume that at most two nodes are involved in a hidden collision for a linear topology such as vehicles on a highway. As such, the node that hears a NACK immediately after finishing its transmission knows that it is the last node involved in the collision. This node will then use a larger contention window (four times of the normal contention window is used in our study) to select its backoff, while others keep theirs unchanged. In this way, successive collisions among the same hidden terminals will be reduced.

4.1.2 Blind Sequential Scheme

Now, we introduce a simple retransmission mechanism referred to as the blind sequential scheme. The retransmissions for this scheme are blind in the sense that there is no feedback from the receivers — every safety message is retransmitted a fixed number of times, and, to mitigate repeat collisions, a backoff process is
executed between retransmissions. The contention window, \( W \), remains constant regardless of the retransmission attempt. We keep the mechanism simple in order to maximize conformance with the 802.11p standard. Compared with the NACK sequential scheme, this approach does not require any extra hardware or complex protocol. Note that later in Chapter 5 and Chapter 6, we consider blind sequential scheme again. However, the schemes are different from the one presented in this chapter, as here we do not distinguish between event safety messages and routine safety messages where as in those chapters, the event safety message is prioritized over routine safety message and only event packets are retransmitted.

In the next two sections we will investigate the effectiveness of this retransmission mechanism. To this end, the analytical model developed in Chapter 3 is extended to cover the NACK sequential scheme and blind sequential scheme in Section 4.2 and in Section 4.3 respectively.

### 4.2 Analytical Model for NACK Sequential Scheme

In this section, we present the analytical model for NACK based retransmission scheme by extending the model developed in Chapter 3 for standard MAC protocol. For any retransmission based scheme, each transmission attempt of the same packet face different channel condition, mainly due to difference in backoff process and also due to repeat collisions of retransmitted packets. As such, we calculate the collision probabilities and delay for each attempt of the packet transmission. Then, based on expected number of transmission attempt per packet, we calculate the overall collision probabilities and delay of the packet. In the rest of this chapter, we use subscript, such as in \( X_i^n \), to denote the value of \( X \) for the \( i \)th retransmission attempt and We use \( n \) superscript to indicate the terms used for NACK sequential scheme.

First we redefine the direct collision probability calculated in (3.4) for the first attempt and successive attempts as \( d_n^l \) for the \( l \)th attempt. For the first attempt, the probability \( d_0^0 \) is similar to (3.4), but for the successive attempts, the probability
$d^n_i$ would be different. Recall from Section 3.2 that the probability direct collision is negligible when a packet arrives to an empty buffer and finds the channel idle for a DIFS period. This can happen for first transmission attempt with $(1-(1-\rho)(1-b^n))$ probability where $b^n$ represents the channel busy probability defined later. For later retransmissions the backoff is always performed between successive attempts. So, we can express the direct collision probability as

$$d^n_0 = (1-(1-\rho)(1-b^n))(1-(1-\rho\tau)^{N_n}),$$  \hspace{1cm} (4.1)$$
$$d^n_l = (1-(1-\rho\tau)^{N_n}),$$  \hspace{1cm} (4.2)$$

where $b^n$ represents the channel busy probability modified from (3.2) to incorporate retransmissions. It is expressed as

$$b^n = M^n N_n \lambda T (1 - \overline{d^n}/2),$$  \hspace{1cm} (4.3)$$

where, $M^n$ is the expected number of attempts per packet (to be derived later) and $\overline{d^n}$ is the average direct collision probability calculated from

$$\overline{d^n} = \frac{d^n_0 + (M^n - 1)d^n_l}{M^n}.$$  \hspace{1cm} (4.4)$$

Furthermore, recall that two necessary conditions must be met to avoid hidden terminal collision. We denote them as $H^{n,b}$ and $H^{n,a}$ for “hidden, before” and “hidden, after” events respectively. As our DIFS period is now longer than the actual packet transmission time, those conditions are slightly changed. The first condition, $H^{n,b}$, assumes that when the tagged node starts its transmission no other hidden node can be in the transmitting state. But due to the longer DIFS, it is now possible that when the tagged node starts its transmission, a hidden node is in the transmitting state waiting for the end of its DIFS and by the time it starts actual transmission the tagged node already finishes its transmission. For the second condition, $H^{n,a}$, we note that if $H^{n,b}$ condition is met, $H^{n,a}$ cannot occur
as by the time a hidden terminal is allowed to transmit (after a DIFS period), the tagged vehicle would have finished its transmission. So, we only have $H^{n,b}$ in this case which we differentiate for the first attempt, $H^{n,b}_0$, and any successive attempts, $H^{n,b}_i$. We define the probability of no hidden collision for the first attempt as

$$P(H^{n,b}_0) = 1 - M^n N_h \lambda 2 t_{data} (1 - \overline{d}/2).$$  \hspace{1cm} (4.5)$$

If there is a collision in the first attempt between two nodes, one of the nodes will increase its contention window to reduce the chance of successive collisions. We need to calculate the probability of successive collision denoted by $p_{scv}$. We note that a successive collision happens when the node with the larger contention window starts transmitting before the other node finishes its transmission. The mean time taken by the first node to finish its second transmission after the second node finishes its first transmission is $t_{data}/2 + (W - 1)/2$. Now, denoting the larger contention window used by the second node as $W'$, we can calculate the probability of successive collision as

$$p_{scv} = \frac{t_{data}/2 + (W - 1)\sigma/2}{W'\sigma}. \hspace{1cm} (4.6)$$

Now, we can assume that collision due to all other hidden nodes in the potential hidden range behave the same as previously. As such, the probability of no hidden collision for the successive attempts would be

$$P(H^{n,b}_i) = 1 - M^n N_h \lambda 2 t_{data} (1 - \overline{d}/2)p_{scv}. \hspace{1cm} (4.7)$$

Because direct collisions and collisions due to hidden terminals are independent, we get the expressions for the collision probabilities as

$$c^n_0 = 1 - (1 - d^n_0) P(H^{n,b}_0), \hspace{1cm} (4.8)$$

$$c^n_i = 1 - (1 - d^n_i) P(H^{n,b}_i). \hspace{1cm} (4.9)$$
The expected number of transmission attempts is given as

\[ M^n = 1 + c_0^n + c_0^n c_l^n + c_0^n (c_l^n)^2 + \cdots + c_0^n (c_l^n)^{m-2} = 1 + c_0^n \frac{1 - (c_l^n)^{m-1}}{1 - c_l^n} , \] (4.10)

where \( m \) is the maximum number of transmission attempts per packet.

To calculate the packet delivery ratio, we note that a packet is dropped when all the transmission attempts fail. So, the PDR can be expressed as

\[ PDR = 1 - c_0^n (c_l^n)^{m-1}. \] (4.11)

Now, we define the access delay conditioned on the number retransmission as \( A_l^n \), where the packet transmission is completed either successfully or unsuccessfully after \( l \) retransmission. With the collision probability \( c_l^n \) on each attempt, we can calculate the probability of \( l \) retransmission and express the access delay \( A^n \) as

\[
A^n = \begin{cases} 
A_0^n & \text{w.p. } (1 - c_0^n), \\
A_l^n & \text{w.p. } c_0^n (c_l^n)^{l-1} (1 - c_l^n), \\
A_{m-1}^n & \text{w.p. } c_0^n (c_0^n)^{m-2}.
\end{cases} \] (4.12)

where the access delay for first transmission attempt, \( A_0^n \) is similar to our previous model without retransmission

\[
A_0^n = \begin{cases} 
0 & \text{w.p. } (1 - \rho)(1 - b^n), \\
B_0^n + T_{Res} & \text{w.p. } (1 - \rho)b^n, \\
B_0^n & \text{w.p. } \rho.
\end{cases} \] (4.13)

and access delay for successive transmission attempt, \( A_{l \geq 1}^n \) is defined as

\[ A_l^n = A_{l-1}^n + B_l^n + T \]
\[ A^n_0 + \sum_{j=1}^{l} (B^n_j + T), \quad (4.14) \]

where \( B^n_j \) is the backoff duration for \( j^{th} \) retransmission attempt.

To calculate \( B^n_j \) we note that for each successive transmission attempt, the tagged node chooses its backoff counter with equal probability either in the range \([0, W - 1]\) or in the range \([0, W' - 1]\), where \( W' \) is the increased contention window. The backoff duration for the first case is the same as \( B \) defined in (3.10). For the second case, we define the backoff duration as

\[ B' = \sum_{n=1}^{U'} (\sigma + Y), \quad (4.15) \]

where \( U' \) is the backoff counter value which is uniformly distributed in the range \([0, W' - 1]\). Now we can define the backoff duration for the \( j^{th} \) retransmission attempt as \( B^n_j \).

\[ B^n_j = \begin{cases} B & \text{w.p. 0.5,} \\ B' & \text{w.p. 0.5.} \end{cases} \quad (4.16) \]

From the above equation, the expected value and variance of \( B^n_j \) can be calculated as

\[ \text{E}[B^n_j] = (\text{E}[B] + \text{E}[B'])/2, \quad (4.17) \]

\[ \text{Var}[B^n_j] = (\text{Var}[B] + (\text{E}[B] - \text{E}[B^n_j])^2)/2 \\
+ (\text{Var}[B'] + (\text{E}[B'] - \text{E}[B^n_j])^2)/2. \quad (4.18) \]

To get the expected value and variance of the access delay, we first calculate the expected value and variance of the access delay for each transmission attempt. For the first transmission attempt, the distribution of \( A^n_0 \) in (4.13) is a conditional
distribution, thus we have

\[
E[A^n_0] = (1 - \rho)b^n(E[B] + E[T_{Res}]) + \rho E[B], \tag{4.19}
\]

\[
\text{Var}[A^n_0] = (1 - \rho)(1 - b^n) E[A^n_0]^2
+ (1 - \rho)b^n(\text{Var}[B] + \text{Var}[T_{Res}]
+ (E[A^n_0] - E[B] - E[T_{Res}])^2)
+ \rho(\text{Var}[B] + (E[A^n_0] - E[B])^2). \tag{4.20}
\]

From (4.14), noting that \(A^n_0, B^n_j, T\) are all independent of each other, we can calculate the expected value and variance of the access delay for any retransmission attempt, \(A^n_l\) as

\[
E[A^n_l] = E[A^n_0] + l(E[B^n_l] + T), \tag{4.21}
\]

\[
\text{Var}[A^n_l] = \text{Var}[A^n_0] + l \text{Var}[B^n_l]. \tag{4.22}
\]

Finally, putting the expected value and variance of the access delay for each transmission attempt, \(A^n_l\) in (4.12) we have

\[
E[A^n] = (1 - c^n_0) E[A^n_0] + \sum_{l=1}^{m-1} c^n_0 (c^n_l)^{l-1} (1 - c^n_l) E[A^n_l]
+ c^n_0 (c^n_l)^{m-1} E[A^n_{m-1}], \tag{4.23}
\]

\[
\text{Var}[A^n] = (1 - c^n_0)\{ \text{Var}[A^n_0] + ((E[A^n_0]) - E[A^n])^2 \}
+ \sum_{i=1}^{m-1} c^n_0 (c^n_l)^{l-1} (1 - c^n_l)\{ \text{Var}[A^n_l] + ((E[A^n_l]) - E[A^n])^2 \}
+ c^n_0 (c^n_l)^{m-1}\{ \text{Var}[A^n_{m-1}] + ((E[A^n_{m-1}]) - E[A^n])^2 \}. \tag{4.24}
\]
4.3 Analytical Model for Blind Sequential Scheme

In the previous section, we modified the analytical model developed in Chapter 3 for NACK based retransmission scheme. In this section, we modify the model for blind sequential scheme, which is in many ways similar to the NACK sequential scheme. The main difference is that, with blind sequential scheme all the packets are retransmitted fixed number of times, \( m \), without any feedback from the receiver. Recall that, for NACK sequential scheme we calculated the expected number of transmission attempts, \( M^n \) in (4.10).

In the case of sequential retransmissions, the direct collision probability calculated in (3.4) will be different for the first attempt and successive attempts. So, we distinguish between them by denoting \( d^s_l \) as the direct collision probability in the \( l^{th} \) attempt. For the first attempt, the probability \( d^s_0 \) is similar to (3.4), but for the successive attempts, the probability \( d^s_l \) would be different as there is always a backoff between successive attempts. So, we can express the direct collision probability as

\[
\begin{align*}
    d^s_0 &= (1 - (1 - \rho)(1 - b^*)(1 - (1 - \rho\tau)^N)) (1 - (1 - \rho\tau)^N), \\
    d^s_l &= (1 - (1 - \rho\tau)^N),
\end{align*}
\]

where \( b^* \) represents the busy probability modified from (3.2) to incorporate retransmissions and it is expressed as

\[
b^* = mN_n\lambda T (1 - \overline{d^s}/2),
\]

where, \( m \) is the number of attempts per packet and \( \overline{d^s} \) is the average direct collision probability calculated from

\[
\overline{d^s} = \frac{d^s_0 + (m - 1)d^s_l}{m}.
\]

Furthermore, recall that two necessary conditions must be met to avoid hid-
den terminal collision. We denote them as $H^{s,b}$ and $H^{s,a}$ for “hidden, before” and “hidden, after” events respectively. The probability of such events on the first transmission attempt are calculated in a similar way as in Section 3.3 except for the fact that the load on the channel is $m$ times larger. So, we calculate these probabilities as

$$P(H^{s,b}_0) = 1 - m N_h \lambda 2t_{data} (1 - \overline{d}/2), \quad (4.29)$$
$$P(H^{s,a}_0) = e^{-m N_h \lambda (t_{data} - t_{difs})}. \quad (4.30)$$

Because the events $H^{s,b}_0$ and $H^{s,a}_0$ are independent, the probability that no collision occurs during the first attempt due to hidden terminal is given as

$$P(H^*_0) = P(H^{s,b}_0)P(H^{s,a}_0). \quad (4.31)$$

Now, we calculate the probability for hidden terminal collision in the successive transmission attempts given that hidden collisions occurred for all the previous attempts and the other packet is not in its last attempt. Recall that we have calculated successive collision probability for NACK sequential scheme in (4.6). The same equation applies for blind sequential scheme with $W' = W$ as the contention window remains unchanged in the blind sequential scheme. Now, the probability that the other packet is not in its last attempt is $\frac{m-l}{m}$ for the $l^{th}$ retransmission. We assume that collision due to all other hidden nodes in the potential hidden range can be calculated as previously. As such, the probability of no hidden collision for the successive attempts given that hidden collisions occurred on all previous attempts is

$$P(H^*_l) = \left(1 - m(N_h - 1) \lambda 2t_{data} (1 - \overline{d}/2)\right) \left(e^{-m(N_h-1)\lambda(t_{data}-t_{difs})}\right) \left(1 - \frac{m-l}{m} p_{scv}\right). \quad (4.32)$$

Because direct collisions and collisions due to hidden terminals are independent,
we get the expressions for the collision probabilities as

\[ c_s^0 = 1 - (1 - d_n^0)P(H_s^0), \]  \hspace{1cm} (4.33)  
\[ c_s^l = 1 - (1 - d_n^l)P(H_s^l). \]  \hspace{1cm} (4.34)  

To calculate the packet delivery ratio, we note that a packet is dropped when all the transmission attempts fail. So, the PDR can be expressed as

\[ PDR = 1 - c_s^0(c_s^l)^{m-1}. \]  \hspace{1cm} (4.35)  

Now, we define the access delay for as \( A^s \) for blind sequential scheme which is again similar to the NACK sequential scheme except number of retransmission attempt is fixed at \( m \). So, We can express the access delay \( A^s \) as

\[ A^s = A_0^s + \sum_{l=1}^{m-1} (B^s + T), \]  \hspace{1cm} (4.36)  

where the access delay for first transmission attempt, \( A_0^s \) is similar to our previous model without retransmission

\[ A_0^s = \begin{cases} 0 & \text{w.p. } (1 - \rho)(1 - b^s), \\ B^s + T_{Res} & \text{w.p. } (1 - \rho)b^s, \\ B^s & \text{w.p. } \rho. \end{cases} \]  \hspace{1cm} (4.37)  

From (4.36), noting that \( A_0^s, B^s, T \) are all independent of each other, we can calculate the expected value and variance of the access delay for any retransmission attempt, \( A_l^s \) as

\[ E[A^s] = E[A_0^s] + m(E[B^s] + T), \]  \hspace{1cm} (4.38)  
\[ \text{Var}[A^s] = \text{Var}[A_0^s] + m \text{Var}[B^s]. \]  \hspace{1cm} (4.39)
Figure 4.1: Total delay for NACK sequential scheme with three transmission attempts using the following parameter set: (data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes])

4.4 Simulations

In this section, we present the analytical and simulation results for the mean of the total delay and the PDR for our proposed retransmission protocols. For the following set of results, the maximum number of transmission attempts, $m$ is set to 3. For NACK-based retransmission protocol, we restrict our observations up to PDR=85% which covers the required PDR threshold of 90% stipulated by the ASTM [7]. For blind sequential scheme, the PDR is much lower than the 90% threshold for the vehicle densities studied and because of that we use a larger range of PDR values.

In Fig. 4.1, we plot the mean of the total delay as a function of vehicle density, $\beta$, with different curves parameterized by the data rate $R_d$ [Mbps], packet arrival rate $\lambda$ [packets/sec], and packet size $P$ [bytes] denoted as a three-tuple $(R_d, \lambda, P)$ for the NACK sequential scheme. Observe that our analytical model falls within the
95% confidence interval of the simulation results. We note that for the $\lambda = 2$ case the mean delay compared to Fig. 3.2 is proportionately larger due to longer DIFS used for our proposed protocol. For the $\lambda = 10$ cases, the mean delay increases sharply because of more collision and subsequent retransmissions. However, the largest delay observed is still less than 2 ms which is well below the maximum delay constraint of 100 ms for safety applications [62].

In Fig. 4.2 we plot results for the PDR according to (4.11) for NACK sequential scheme and compare them with simulation. As mentioned earlier, we plot the PDR results in the range above PDR=85%. For the $\lambda = 2$ case, we observe that the PDR is always better than 95% which is a significant improvement over Fig. 3.5. In particular, at $\beta = 200$ we observe a 10% increase in PDR value with the enhanced protocol. For the (24,10,200) and (24,10,400) cases in Fig. 4.2 the PDR eventually falls below 90% at $\beta = 60$ and $\beta = 100$, respectively. However, similar performance
Chapter 4. RETRANSMISSION BASED MAC PROTOCOL EXTENSIONS

Figure 4.3: Improvement in Packet Delivery Ratio for NACK sequential scheme with three transmission attempts using the following parameter set: (vehicle density [vehicles/km], data rate [Mbps], packet size [bytes]) can only be observed in Fig. 3.5 using the original protocol at a much lower density, at $\beta = 30$ for $(24,10,200)$ case, and at $\beta = 50$ for $(24,10,400)$ case. Thus the enhanced protocol can support up to two times the vehicle density for the required PDR threshold. Overall, Fig. 4.2 shows a significant improvement in terms of PDR using our proposed protocol.

Using the analytical model, the improvement in PDR of the proposed protocol compared to that of single transmission is shown in Fig. 4.3 for various arrival rates. The vehicle density is fixed at 50 [vehicles/km]. The improvement is increasing with increased arrival rate up to 14% at $\lambda = 10$ for both $(50,12,200)$ and $(50,24,400)$ cases. In general, we see that increasing packet arrival rate has similar effect on PDR as increasing vehicle density as in both cases the network load is increased.

It can be observed from our results that for light and medium traffic loads, the proposed NACK-based extension is an effective one as it improves PDR and extends
Chapter 4. RETRANSMISSION BASED MAC PROTOCOL EXTENSIONS

Table 4.1: PDR with reduced transmission range using 24 [Mbps] data rate and 10 [packets/sec] arrival rate

<table>
<thead>
<tr>
<th>P[bytes]</th>
<th>β [vehicles/km]</th>
<th>Single Tx 500 m</th>
<th>NACK sequential scheme 500 m</th>
<th>NACK sequential scheme 250 m</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>60</td>
<td>0.856</td>
<td>0.973</td>
<td>0.994</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>0.774</td>
<td>0.898</td>
<td>0.984</td>
</tr>
<tr>
<td></td>
<td>150</td>
<td>0.660</td>
<td>0.549</td>
<td>0.955</td>
</tr>
<tr>
<td>400</td>
<td>60</td>
<td>0.792</td>
<td>0.903</td>
<td>0.977</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>0.686</td>
<td>0.700</td>
<td>0.947</td>
</tr>
<tr>
<td></td>
<td>120</td>
<td>0.582</td>
<td>0.207</td>
<td>0.900</td>
</tr>
</tbody>
</table>

the range of vehicle densities where the strict QoS requirement of safety applications is met. At very high vehicle density (and traffic load), there are scenarios where the PDR falls short of the required value. To address these situations, the proposed protocol could be combined with some other approach that reduces the effective channel load; examples of ways to reduce the channel load are to adaptively reduce the transmission range or message rate when the observed traffic load is high. To demonstrate the PDR performance of our NACK-based protocol if used in conjunction with a reduced transmission range, we provide some simulation results in Table 4.1 for a 250 m transmission range for various packet sizes and vehicle densities. For comparison purposes, we include simulation results for a 500 m transmission range for both the NACK-based scheme and conventional DCF. It can be seen from the table that the NACK-based scheme satisfies the 90% PDR requirement for a 250 m range. While the detailed algorithms to adaptively adjust the transmission range are out of the scope of this chapter, examples in Table 4.1 suggest that the required QoS can be met at high densities of vehicles by combining our out-of-band NACK sequential scheme with an adaptive transmission range approach.
Figure 4.4: Total delay for blind sequential scheme with three transmission attempts using the following parameter set: (data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes])

In Fig. 4.4, we plot the mean of the total delay as a function of vehicle density, $\beta$, with different curves parameterized by the data rate $R_d$ [Mbps], packet size $P$ [bytes], and packet arrival rate $\lambda$ [packets/sec] for blind sequential scheme. Observe that our analytical model agrees well with the simulation results. In the plotted range, the mean delay increases almost linearly with the vehicle density, with the slope for the $\lambda = 10$ case being larger compared to the $\lambda = 2$ case. The biggest delay observed is less than 2 ms which is well below the maximum delay constraint of 100 ms for safety applications [62].

Next, we plot the packet delivery ratio in Fig. 4.5 where the analytical results are computed according to (4.35). The analysis provides a reasonable match with the simulation results. For the $\lambda = 2$ case, we see that the PDR is above 90% up to medium vehicle densities ($\beta \leq 0.12$). however, for the $\lambda = 10$ case, the PDR drops sharply with increasing vehicle density.
In Fig. 4.6 we compare the PDR results for blind sequential scheme with that of a single transmission scheme generated from the analytical model. For higher vehicle densities, the higher load on the channel due to retransmission causes the PDR performance to degrade compared to the single transmission case. However, we see slight improvement in PDR for lower vehicle densities, specially when the PDR is above 90%. The two major reasons for suboptimal performance in the blind sequential scheme are repeated collisions and higher load on the channel.

Compared with NACK sequential scheme, the blind sequential scheme can not improve PDR as much due to lack of feedback mechanism. In low load scenario, most of the packets are transmitted successfully the first time. So, in NACK sequential scheme no retransmission occurs, while in blind sequential scheme every packet is retransmitted. As a result the channel load increases significantly and negates benefit of retransmission. So, although requiring an additional narrow band channel
Chapter 4. RETRANSMISSION BASED MAC PROTOCOL EXTENSIONS 74

Figure 4.6: Comparison of Packet Delivery Ratio for blind sequential scheme with three transmission attempts with single transmission scheme using the following parameter set: (data rate [Mbps], packet arrival rate [packets/sec], packet size [bytes]) and a simple transceiver, the NACK sequential scheme does a good job on improving reliability compared to the blind sequential scheme.

4.5 Conclusion

In this chapter, we have proposed two MAC protocol extensions based on retransmission and presented the analytical model to evaluate these schemes for safety applications. The results show that, the NACK sequential scheme improved PDR for light and medium traffic load by utilizing out-of-band signalling to recover from collision due to hidden terminal. The blind sequential scheme also improved PDR, albeit not as much as the NACK sequential scheme due to lack of feedback. In high traffic scenario, both the retransmission based schemes add more load on the channel and as a consequence the reliability drops rapidly. However, we can still argue that
in such scenario, the PDR of the 802.11p DCF protocol is already below acceptable level. We have also demonstrated the effect of reduced transmission range to maintain high reliability. This suggests that adaptive transmission power based on traffic density can be useful for safety packet dissemination. Our proposed schemes can be used for such scheme in conjunction as well to improve PDR even further. Another possibility, which is presented in the next Chapter, is to prioritize event safety packets and retransmit only those packets. This way retransmission does not add much load on the channel, yet improve reliability of event safety packets.
Chapter 5

Safety Message Prioritization Using Retransmissions

In the previous chapter, we have proposed two extensions for the IEEE 802.11p MAC protocol to improve reliability by retransmitting the safety packets multiple times. We have observed that, although retransmission has a positive impact on improving PDR, yet it puts extra load on the channel, especially for sequential scheme without any feedback. So, in this chapter, we distinguish between routine safety message and event safety message and prioritize the later by retransmitting only those messages. This is to ensure that the additional channel load is less prominent. We introduce two retransmission based extensions — firstly, the blind sequential scheme which is a slight variation of the blind sequential scheme proposed in Chapter 4 and secondly, the batch scheme where packets are sent back to back. We also refer to a piggybacked sequential scheme which relies on feedback for retransmission similar to NACK sequential scheme, but instead of relying upon out-of-band signalling it achieves feedback through PACK [47]. In this chapter, we evaluate the performance of the two proposed schemes and compare it with the piggybacked sequential scheme to see how much performance improvement can be gained through feedback. In Section 5.1 we explain the proposed extensions. In Sections 5.2 and 5.3 we extend the analytical model developed in Chapter 3 to incorporate packet retransmissions for event safety messages. We present the delay and PDR results for the proposed schemes in Section 5.4 and finally conclude the chapter in Section 5.5.
5.1 Extensions

In the previous chapter, we proposed two extensions to improve the performance of broadcasting communication in DSRC environment. While the NACK sequential scheme was effective in improving reliability, it requires out-of-band signalling for feedback. For the blind sequential scheme, on the other hand, the improvement was less prominent as retransmitted packets put additional load on the channel. In this chapter, we separate safety messages into two types — routine safety messages and event safety messages. The routine safety messages typically contain information about vehicle state, such as position/direction and speed, and are broadcast regularly by all vehicles. These messages constitute the majority of traffic load on the DSRC control channel. The event messages, on the other hand, are triggered by event situations such as sudden braking. These messages occur only occasionally, but can contribute significantly to the traffic load on the control channel when they do occur. Clearly the event safety messages have a more stringent requirement in terms of fast and guaranteed delivery, while routine messages may tolerate a higher packet error rate. So, the goal for the extensions proposed in this chapter, is to improve reliability of event messages through retransmission while maintaining a low channel load.

In Section 3.1, we characterized the packet arrival process by Assumptions 3 and 4 for routine safety messages and event safety messages combined. Now, as we distinguish between them and treat them differently, we need to have separate arrival processes for both types of safety messages.

**Assumption 7.** All nodes generate event messages according to independent Poisson processes, each with rate $\alpha \lambda$ [packets/sec] with $\alpha \in [0, 1]$, and generate routing safety messages as independent Poisson processes with rate $(1 - \alpha)\lambda$.

Note that DSRC event messages are bursty in nature; emergency events such as an animal running across a road will cause a surge of event messages from multiple vehicles. However, in this work, we model the period after an emergency event
has occurred when the chance of packet drop is the highest. It is within this short interval that we apply a Poisson model. This model captures the phenomenon of having a “rate” of event messages, without assuming them to be periodic. The Poisson nature of the arrival process is not disturbed by MAC effects, since the time scale of milliseconds for message delivery is small compared with the duration of the surge (of the order of a human reaction time, around 1 s [32]). Moreover, events such as hard braking, which may be expected to have high correlation, actually have weak correlation between vehicles [10]. Such weak correlation between many agents naturally leads to a Poisson process. The model uses this assumption in two places; at each place, we explain how the model would differ if this assumption were relaxed.

Given the need to retransmit event messages, we propose two schemes, namely blind sequential scheme and batch retransmission scheme, that enable performance improvement without any additional protocol overhead. In particular, both are “blind” retransmissions schemes in the sense that no feedback is required from the receivers — every event message is retransmitted a fixed number of times. Since these schemes only retransmit event messages, which are rare, they do not impose an excessive increase in load. Note that these proposed protocols are compatible with the EDCA extension to the DCF protocol. In addition, we examine the idea proposed in [47] to develop a so-called piggybacked sequential scheme as a way of providing feedback without out-of-band signalling, but with some protocol overhead. In the following, we will describe each of the schemes in detail.

5.1.1 Blind Sequential Retransmission

In the blind sequential scheme (shown in Fig. 5.1(a)), the retransmissions are automatically carried out without feedback from the receivers, i.e., every event message is retransmitted a fixed number of times. In Chapter 4 we have already proposed the blind sequential scheme, although now we only consider retransmission for event messages. Furthermore, to mitigate repeat collisions, the backoff process executed between retransmissions uses a larger contention window than the initial one. The
Figure 5.1: Retransmission-based extensions to IEEE 802.11 MAC protocol
scheme is simple and compatible with the new standard, and hence can be easily deployed. When an emergency event occurs, instead of sending a single event message to the MAC layer, multiple copies are sent. The larger contention window before successive retransmission can be achieved by assigning an access categories to the first copy and a different access category to the remaining copies using the EDCA mechanism of the DSRC standard. However, the larger contention window can not eliminate the repeat collisions entirely. As such, in the next chapter we modify the blind sequential scheme to introduce a random gap time between retransmission attempts, which is independent of the MAC layer backoff period, to further reduce repeat collisions.

Note that a similar approach using message retransmission has been proposed in [101] where the lifetime of the safety message is divided into slots and multiple copies are scheduled in different slots. However, all proposed protocols in [101] requires an extended MAC sublimer for scheduling packets in slots. Two protocols require slots to be synchronized among all nodes while the rest of the protocols do not require that. All proposed protocols however require significant changes in the MAC protocol. For example the best performing protocol AFR-CS requires that a packet is dropped if channel is sensed busy instead of performing the backoff.

5.1.2 Batch Retransmission

In the batch scheme (shown in Fig. 5.1(b)), multiple copies of an event messages are transmitted back-to-back with only small inter-frame spaces (SIFS). This can be achieved using the Transmission Opportunity (TOP) feature of EDCA mechanism. The only condition under which all copies within a batch are corrupted, is when it coincides with a batch of event messages from another node, or when the batch collides with multiple routine or event messages that are close together. The batch retransmission scheme has an advantage compared to the blind sequential scheme in that it reduces the number of collisions resulting in packet lost when there is only partial overlap of packets, reminiscent of the benefits of slotted Aloha over unspotted
Aloha [3]. It is to be expected that this will reduce the loss probability. The delay experienced by retransmissions in this scheme is also expected to be negligible. Note that the TOP option of the EDCA mechanism has been explicitly removed from ad hoc operation in the current version of the standard. We argue that its performance poses an attractive alternative for V2V system design and configuration, and that it should be allowed as it is in regular 802.11.

5.1.3 Piggybacked Sequential Retransmission

The piggybacked sequential scheme (shown in Fig. 5.1(c)) is an extension to the PACK protocol proposed in [47]. The basic idea is to place some additional information in each outgoing safety message such as the sender’s position, the intended range of reception, a randomly generated message ID, and the list of IDs of the most recently received messages. Ideally each message ID should be unique in the local neighborhood, which can be achieved with high probability by choosing a sufficiently long ID.

In [47] the usefulness of the piggybacking was measured, but retransmission based on PACK was not discussed. As such, many details of how one can use PACK to recover a lost message and improve reliability are missing. We propose a specific algorithm for the retransmission of event messages based on information gained from PACK. The goal is to retransmit the packet if any of the intended recipients has not received it. However, it is not necessary to wait until feedback has been received from all intended recipients, since occasional spurious retransmissions are acceptable. Upon receiving a piggybacked ACK from a node within its intended range, a sending node checks to see if the ID of the message it sent is among the received IDs. If the ID is absent, then the sending node flags that the message needs retransmission. To avoid consecutive collisions between hidden terminals, the retransmission is scheduled after a random time that is in the order of a packet transmission time. In the simulation, this time is chosen uniformly in the range of $0ms - 5ms$. This waiting time is carried out independently of the backoff process.
This parameter value is chosen arbitrarily which corresponds to around 312 idle backoff slots. Choosing a large waiting time ensures independence among successive transmission attempts. However, it also increases delay. Note that the lifetime of each safety message is limited, and beyond that no retransmission is allowed. As such, the larger the gap between two successive transmission attempts, the lower the number of retransmission attempts possible within the lifetime of the packet. Also, if a newer event message is generated before the retransmission, the older message is considered obsolete and the newer message is sent instead.

The piggybacked sequential scheme is somewhat similar to the NACK sequential scheme proposed in Chapter 4 in the sense that both protocols require feedback from the receivers. Although, for NACK sequential scheme an out-of-band signalling is used whereas for piggybacked sequential scheme feedback is sent on the same channel. So, similar to the NACK sequential scheme, the advantage of the piggybacked sequential scheme over the batch and blind sequential schemes is that the expected number of transmission attempts per event message is lower. However, the list of IDs can constitute a considerable increase in packet overhead in dense network. For example, if there are 100 vehicles within the reception range, and each message ID is 2 [bytes] long, it will add an additional 200 [bytes] to the safety packet. The overhead could be reduced by either limiting the number of acknowledged messages or introducing a maximum allowable delay at the cost of reduced feedback accuracy.

### 5.2 Analysis of Packet Deliver Ratio

In this section, we calculate the direct collision probability, \( d \), and the probability that the tagged packet is not corrupt due to hidden collision, \( P(H) \), using both blind sequential and batch schemes for both routine safety messages and event safety messages. The PDR for each case can be calculated from these two quantities. We also calculate the channel busy probability, \( b \), which affects the backoff process and as a result the direct collision probability as well.
5.2.1 Direct collision

Let $b^s$ and $b^b$ represent the probability that the channel is busy for the blind sequential scheme and batch scheme respectively. Also, let $d^i_k$ denote the direct collision probabilities for routine ($k = r$) and event ($k = e$) packets under the blind sequential ($i = s$) and batch ($i = b$) retransmission schemes. Since routine packets are treated the same by both schemes, we will first consider $d^i_r^{e(s,b)}$. Then the probability of losing an event packet due to direct collisions which differs for the two schemes will be considered in turn.

Routine packets

For routine packets, each packet is transmitted only once. The direct collision probability for routine packets is similar to (3.4). Recall from Section 3.2 that the probability direct collision is negligible when a packet arrives to an empty buffer and finds the channel idle for a DIFS period. This can happen for first transmission attempt with $(1 - (1 - \rho)(1 - b^i))$ probability where $b^i$ represents the channel busy probability. So, we can express the direct collision probability as

$$d^i_s = (1 - (1 - \rho)(1 - b^i))(1 - (1 - \rho \tau)^{N_{n}}). \quad (5.1)$$

Event packets: blind sequential scheme

For the blind sequential scheme, the first transmission of an event packet is equivalent to a routine packet, and so the direct collision probability for the first attempt of event packets, denoted by $d^e_{c,0}$, is

$$d^e_{c,0} = d^e_c = (1 - (1 - \rho)(1 - b^c))(1 - (1 - \rho \tau)^{N_{n}}), \quad (5.2)$$

where $b^c$ will be calculated later in (5.7).

For any subsequent attempts of the event packet for the blind sequential scheme, we note that there is always a backoff preceding the packet transmission. As a result
the slots are synchronized among the neighboring nodes and any attempt to transmit multiple packets in the same slot results in a collision. So, letting \( d_{e,l}^s \) denote the probability of direct collision in the \( l^{th} \) retransmission attempt of an event packet for the blind sequential scheme, we have for \( l = 1, \ldots, m - 1, \)

\[
d_{e,l}^s = (1 - (1 - \rho \tau)^{N_n}). \tag{5.3}
\]

Since the events in (5.2) and (5.3) are independent, the probability of a packet being undeliverable is

\[
d_e^s = d_{e,0}^s \prod_{l=1}^{m-1} d_{e,l}^s = (1 - (1 - \rho)(1 - b^s))(d_{e,l}^s)^m. \tag{5.4}
\]

In order to calculate the fraction of time the channel is busy, consider the mean direct collision probability,

\[
\overline{d}_e^s = \frac{d_{e,0}^s + \sum_{l=1}^{m-1} d_{e,l}^s}{m} = \left( 1 - \frac{(1 - \rho)(1 - b^s)}{m} \right) d_{e,l}^s. \tag{5.5}
\]

We have \( N_n \) vehicles in the CS range other than the tagged vehicle, transmitting \((1 - \alpha)\lambda \) [packets/sec] for routine safety packets and \( \alpha \lambda \) [packets/sec] with \( m \) transmission attempts per packet for event packets. If there is no collision, then all the packet transmissions should take \( T = N_n \lambda((1 - \alpha) + m\alpha)T^* \) time each second. However, when a collision occurs, exactly two nodes are involved, and their two transmissions coincide exactly due to carrier sensing. Thus, the transmission time to send the packets which collide is reduced by \( N_n \lambda((1 - \alpha)d_e^s/2 + (m\alpha)d_e^s/2)T^* \) where \( T^* \) is the complete transmission time of a packet including the DIFS period.
for the blind sequential scheme,

\[ T^s = t_{\text{data}} + t_{\text{difs}}. \]  

(5.6)

Subtracting this from \( T \) gives the probability that the channel is sensed busy when a new packet arrives for the blind sequential scheme,

\[ b^s = N_n \lambda ((1 - \alpha)(1 - d^c_s/2) + m\alpha(1 - d^e_s/2))T^s, \]  

(5.7)

**Event packets: batch scheme**

To calculate the direct collision probability of the event packets for the batch scheme, note that a single routine packet can overlap with at most two copies of the event packet. This means that if \( m \geq 3 \) then an event packet can always be received unless it collides with another event packet. As the rate of arrival of event packets is \( \alpha \lambda \), the direct collision probability of event packets under the batch scheme can be shown, similarly to (5.1), to be

\[ d^b_e = (1 - (1 - \rho)(1 - b^b))(1 - (1 - \alpha\rho T^b)^N_n). \]  

(5.8)

Like in the blind sequential case, the probability that the channel is sensed busy when a new packet arrives for the batch scheme is

\[ b^b = N_n \lambda ((1 - \alpha)(1 - d^b_r/2)T^b_r + \alpha(1 - d^b_e/2)T^b_e), \]  

(5.9)

where \( T^b_r \) and \( T^b_e \) are the complete transmission time of a packet including the DIFS period for routine and event packets respectively given by

\[ T^b_r = t_{\text{data}} + t_{\text{difs}}, \]  

(5.10)

\[ T^b_e = mt_{\text{data}} + (m - 1)t_{\text{aifs}} + t_{\text{difs}}. \]  

(5.11)
5.2.2 Hidden terminal

In the following, we calculate the probability $P(H)$ that a packet is not involved in a hidden collision firstly for blind sequential scheme and secondly for batch scheme. For both schemes, the derivations of those terms for routine packets are similar to the single transmission case; so, routine packet calculations are done first and event packet calculations are done subsequently.

**Blind sequential scheme**

For the blind sequential scheme, we denote the first condition as $H_{s,b}^r$ for routine safety messages and as $H_{e,l}^{s,b}$ for the $l^{th}$ attempt ($l = 0, 1, \ldots, m - 1$) of an event messages. Note that only event packets are sent multiple times and collision in the first attempt has the same probability as the collision for routine safety packets. By a similar argument as used to derive (5.7), the probability of finding all hidden terminals in the non-transmitting state is

$$P(H_{s,b}^r) = P(H_{e,0}^{s,b}) = 1 - N_h \lambda \left( (1 - \alpha)(1 - d_{sr}/2) + m\alpha(1 - d_{se}/2) \right) T_s. \quad (5.12)$$

The “after” event is separated in to $H_{s,a}^r$ for a routine safety packet and $H_{e,l}^{s,a}$ for an event packet in its $l^{th}$ attempt. The probability of no hidden packets transmitting after the tagged transmission starts is

$$P(H_{s,a}^r) = P(H_{e,0}^{s,a}) = \exp \left( - N_h \lambda \left( (1 - \alpha) + m\alpha \right) (t_{\text{data}} - t_{\text{difs}}) \right). \quad (5.13)$$

For notational convenience, let $H_{e,0}^s = H_{e,0}^{s,b} \land H_{e,0}^{s,a}$ be the event that the first attempt of a tagged event packet does not collide with any packets from a hidden terminal, sent either before or after itself.

It remains to calculate the probability for hidden terminal collision in the subsequent transmission attempts for the blind sequential scheme given that hidden collisions occurred for all the previous attempts. Note that hidden collisions in sub-
sequent attempts are not independent. If a collision occurs in the first attempt where the colliding packet is not in its last transmission attempt, subsequent transmission attempts are more likely to result in collisions. We need to calculate the probability of a subsequent collision, $p_{scv}$, given that the first attempt resulted in a collision due to a hidden terminal and the other packet is not in its last attempt.

Let the two nodes in the collision be denoted $u$ and $v$, and let $u$ be the one that transmitted first. Consider the (usual) case that $u$ also starts its retransmission before $v$ finishes its original transmission. A collision will occur if and only if $v$’s retransmission starts before $u$’s retransmission finishes. Let $t$ be the time at which $u$’s previous transmission finishes. The expected time for $u$’s retransmission to finish is $t + t_{\text{data}} + WE[Y]$, where $Y$ is the random duration of a backoff slot. The expected time for $v$’s next backoff period to start is $t_{\text{data}}/2$. Hence, the collision probability on the subsequent attempt can be approximated by the probability that $v$’s backoff lasts less than $t_{\text{data}}/2 + (W - 1)E[Y]/2$. This backoff is $E[Y]$ multiplied by an integer uniformly distributed on $[0, (W - 1)]$, if $W$ is large enough that the ensemble average $E[Y]$ is experienced. Hence the probability of a collision on the subsequent attempt can be modeled as

$$p_{scv} = \min\left(\frac{t_{\text{data}}/2 + (W - 1)E[Y]/2}{WE[Y]}, 1\right).$$

(5.14)

The probability that the other packet is not in its last attempt is $\frac{m-1}{m}$ for the $l^{th}$ retransmission attempt. We assume that the probability of collision due to all other hidden nodes can be calculated as previously. The probability that none of them collide is then

$$P(H') = \exp\left(- (N_h - 1)^+ \lambda((1 - \alpha) + m\alpha)(t_{\text{data}} - t_{\text{difs}})\right)$$

$$\left(1 - (N_h - 1)^+ \lambda((1 - \alpha)(1 - d_{\text{e}}/2) + m\alpha(1 - d_{\text{e}}/2))T^s\right),$$

(5.15)

where $(x)^+ = \max(0, x)$. As such, the probability of no hidden collision for the
Chapter 5. SAFETY MESSAGE PRIORITIZATION

subsequent attempts given that hidden collisions occurred on all previous attempts is

\[ P(H_{e,l}^*) = P(H') \left( 1 - \frac{m - l}{m} p_{scv} \right). \]  

(5.16)

**Batch scheme**

Consider first the “before” event, \(H^{b}\). Following a similar argument to the derivation of (5.7), we can show that the probability of event \(H^{b}\) for routine safety packets under the batch scheme, denoted \(H_{r}^{b,b}\), is

\[ P(H_{r}^{b,b}) = 1 - N_h \lambda \left( (1 - \alpha)(1 - d_{l}/2)T_{r}^b + \alpha(1 - d_{e}/2)T_{e}^b \right). \]  

(5.17)

For event packets, condition \(H^{b}\) can be relaxed; the packet is retransmitted multiple times back to back and lost only when it collides with the first transmission of another event packet since otherwise the last transmission of the tagged packet will succeed, by the assumption that each packet collides with only one other. The probability of the “before” condition for event packet, \(H_{e}^{b,b}\), is thus

\[ P(H_{e}^{b,b}) = 1 - N_h \alpha \lambda (1 - d_{l}/2)(t_{data} + t_{difs}). \]  

(5.18)

For event \(H^{a}\) we need to calculate the probability that a packet is generated by the hidden terminal after the tagged vehicle starts its transmission and eventually collides with the transmission of the tagged vehicle. Again, there are two cases, \(H_{r}^{b,a}\) and \(H_{e}^{b,a}\), when the tagged packet is a routine or event packet, respectively. The combined packet arrival process from all the hidden terminals is a Poisson process and the total number of transmission attempts per second is \(\lambda N_h\) for the batch scheme. Condition \(H_{r}^{b,a}\) is met if no packet is generated at any of the hidden terminals during the period of length \(t_{data} - t_{difs}\). For event packets, \(H_{e}^{b,a}\) should only consider collisions with event packets within the first transmission attempt, which
form a Poisson process with rate $\alpha \lambda$. The event collision probabilities are then

$$P(H_{r}^{b,a}) = \exp \left( - \lambda N_{h}(t_{\text{data}} - t_{\text{difs}}) \right), \quad (5.19)$$

$$P(H_{e}^{b,a}) = \exp \left( - \alpha \lambda N_{h}(t_{\text{data}} - t_{\text{difs}}) \right). \quad (5.20)$$

### 5.2.3 Packet delivery ratios

To calculate the packet delivery ratio, we approximate direct collisions and collisions due to hidden terminals as independent, and note that a packet is dropped when all the transmission attempts fail. Thus, the PDR for DCF and for both type of packets under both schemes can finally be expressed as

$$PDR = (1 - d)P(H^{b})P(H^{a}), \quad (5.21)$$

$$PDR_{r}^{s} = (1 - d_{r}^{s})P(H_{r}^{s,b})P(H_{r}^{s,a}), \quad (5.22)$$

$$PDR_{e}^{s} = (1 - d_{e}^{s}) \left( 1 - \prod_{i=0}^{m-1} (1 - P(H_{e,i}^{s})) \right), \quad (5.23)$$

$$PDR_{r}^{b} = (1 - d_{r}^{b})P(H_{r}^{b,b})P(H_{r}^{b,a}), \quad (5.24)$$

$$PDR_{e}^{b} = (1 - d_{e}^{b})P(H_{e}^{b,b})P(H_{e}^{b,a}). \quad (5.25)$$

### 5.3 Delay Calculation

In this section, we derive an expression for the packet delay. The total delay (or sojourn time), $D$ experienced by a packet of a tagged vehicle includes the complete time to transmit the packet, $T$, the access delay, $A$, and the waiting time of the packet in the transmit node’s queue, $Q$, if any. The access delay of a packet is defined as the time interval between the instant the packet reaches the head of the queue, to the instant when the last attempt of the packet transmission starts. Thus, the access delay consists of the backoff periods associated with all the transmission attempts and the time of all the collisions of that packet. We also derive the expression for
the service time, $S$, as a sum of access delay and transmission time. So, denoting the total delay of the packet under retransmission scheme as $i \in \{s, b\}$ by $D^i$, we get

$$D^{i\in\{s,b\}} = Q^i + S^i = Q^i + A^i + T^i,$$  \hspace{1cm} (5.26)

where $Q^{i\in\{s,b\}}$ are r.v.’s representing the queueing delay, and $S^{i\in\{s,b\}}$ is the service time, during which the MAC protocol is attempting to transmit the packet.

**Remark 1.** The delay experienced by the application is the time until the packet is first received successfully. The “total delay” $D^{i\in\{s,b\}}$ is an over-estimate of this “application delay”, which is quite conservative if the probability of success is high, especially for the blind sequential scheme.

### 5.3.1 Distribution of service time

To calculate the distribution of the service times under both of the proposed schemes, we first define some terms.

For each packet transmission in the blind sequential scheme, the channel is occupied for the duration of the actual packet transmission ($t_{data}$) and one DIFS; recall that we define the complete transmission time $T^s$ as the sum of the actual packet transmission time and one DIFS period. The complete transmission time $T^b_r$ for routine safety packets in the batch scheme is also the sum of the actual packet transmission time and one DIFS period; however, for event packets the complete transmission time $T^b_e$ consists of one DIFS, actual transmission time for all the attempts and SIFS periods in between transmissions. We also define the service time of the queue $S$ as the sum of the access delay $A$ and the transmission delay $T$. The service times for the blind sequential and batch schemes depend on whether the packet is an event packet or a routine safety packet, and can be expressed as

$$S^{i\in\{s,b\}} = \begin{cases} A^i_r + T^i_r & \text{w.p.} \ 1 - \alpha, \\ A^i_e + T^i_e & \text{w.p.} \ \alpha \end{cases}$$ \hspace{1cm} (5.27)
where $A_{i,j}^{\{s,b\}}$ are the access delays.

To determine the access delay, we identify three scenarios that can confront a newly-generated packet similar to 3.4 as follow:

1. A packet arrives to an empty buffer and finds the channel idle with probability $(1 - \rho)(1 - b)$. The access delay for the first attempt in this case is zero as the tagged vehicle transmits the packet without any backoff.

2. A packet arrives to an empty buffer but finds the channel busy with probability $(1 - \rho)b$. The vehicle must wait until the ongoing transmission is finished and then perform a backoff before transmitting the packet.

3. A packet arrives to a non-empty buffer with probability $\rho$ and when it reaches the head of the queue, a backoff is performed before transmitting the packet.

Now, for the blind sequential scheme, event packets are sent multiple times with a backoff in between each transmission attempt. Routine safety packets for both scheme are sent only once and also multiple transmission attempts of an event packet for the batch transmission scheme can be considered as a single transmission attempt with larger duration. In the cases $(i,j) \in \{(s,r), (b,r), (b,e)\}$, there is a single transmission attempt, whose access delay is

$$A_{i,j} = \begin{cases} 
0 & \text{w.p. } (1 - \rho)(1 - b^i), \\
B_j^i + T_{\text{Res}}^i & \text{w.p. } (1 - \rho)b^i, \\
B_j^i & \text{w.p. } \rho, 
\end{cases}$$

(5.28)

where $T_{\text{Res}}^i$ is the residual time of the packet using the medium when the tagged packet arrives, and $B_j^s$ and $B_j^b$ represent the total backoff duration including periods when the backoff counter is suspended. For blind sequential scheme, all packets have length $T^s$ and so $T_{\text{Res}}$ is uniformly distributed on $(0, T^s)$. For batch transmissions, the remaining time depend on the probability that the arrival occurs during an event.
packet, and satisfies

\[ T_{Res}^b \sim \begin{cases} U(0, T_b^e) & \text{w.p. } \frac{\alpha T_b^e}{\alpha T_b^e + (1-\alpha) T_r^e} \\ U(0, T_r^e) & \text{w.p. } \frac{(1-\alpha)T_b^e}{\alpha T_b^e + (1-\alpha) T_r^e} \end{cases} \] (5.29)

where \( U(a, b) \) denotes a uniform random variable on the interval \((a, b)\).

Using blind sequential scheme, the delay for the first attempt of an event packet is also the same as above. However, each subsequent transmission attempt follows a backoff period. So, the total access delay for event packets in the blind sequential scheme can be defined as

\[ A_e = A_r + \sum_{n=1}^{m-1} (B_{e,n} + T^s) \] (5.30)

where, \( m \) is the number of transmission attempts for each of the packets and \( \{B_{e,n}\} \) is a sequence of i.i.d. r.v.s representing the backoff duration for each transmission attempt.

During the backoff process, every slot can be interrupted by successful transmissions or collisions of packets transmitted by other vehicles. During the interruption, the backoff counter is suspended and when the backoff counter is resumed, it starts from the beginning of the interrupted slot. Thus, we can express \( B \) as a random sum

\[ B = \sum_{n=1}^{U} Y_n \] (5.31)

where \( \{Y_n\} \) is a sequence of i.i.d. r.v.s representing the duration of each slot, and \( U \) is the backoff counter value which is uniformly distributed in the range \([0, W-1]\).

If no other vehicle transmits in a given slot then \( Y = \sigma \), where \( \sigma \) is defined to be the duration of an idle backoff slot. If one or more vehicles transmit in that slot, then the tagged vehicle will suspend its backoff process for the duration of the complete transmission, \( T \). Recall that, the probability that a vehicle attempts to transmit in an arbitrary slot given that it has a packet in its buffer is given by \( \tau \).
and the probability that the buffer is non-empty is $\rho$. Therefore, the probability of a vehicle transmitting in an arbitrary slot is $\rho \tau$ and a backoff slot of the tagged vehicle is interrupted when any of the other $N_n$ vehicles transmit in that slot with probability $1 - (1 - \rho \tau)^{N_n}$. Now, for the blind sequential scheme both routine and event packets have the same transmission time, $T^s$. Therefore, $Y^s$ for the blind sequential scheme is

$$Y^s = \begin{cases} 
\sigma & \text{w.p.} \ (1 - \rho \tau)^{N_n}, \\
\sigma + T^s & \text{w.p.} \ 1 - (1 - \rho \tau)^{N_n}.
\end{cases} \quad (5.32)$$

where $1 - (1 - \rho \tau)^{N_n}$ is the probability that a slot is busy due to transmissions by other vehicles.

For batch transmission, the slot period is $Y = \sigma$ if no interruption occurs, it can be $\sigma + T^b_r$ if the slot is interrupted by a routine packet, or it can be $\sigma + T^b_e$ if the slot is interrupted by an event packet. Since collisions are rare, we estimate the slot period given a transmission as $T^b_e$ with probability $\alpha$ and $T^b_r$ otherwise. We can calculate $Y^b_e$ and $Y^b_r$ for the batch scheme similar to (5.32) as

$$Y^b_{j \in \{e,r\}} = \begin{cases} 
\sigma & \text{w.p.} \ (1 - \rho \tau)^{N_n}, \\
\sigma + T^b_e & \text{w.p.} \ \alpha(1 - (1 - \rho \tau)^{N_n}), \\
\sigma + T^b_r & \text{w.p.} \ (1 - \alpha)(1 - (1 - \rho \tau)^{N_n}).
\end{cases} \quad (5.33)$$

These equations determine the distribution of the delay. From the distribution of the delays we can calculate the mean and variance of the service time in the next section. Then, from those values the mean queueing delay and the mean total delay are calculated.
5.3.2 Mean and Variance of Delay

The mean total delay of a packet is an important performance metric. In addition, the service time is needed to obtain the fixed point for $\rho$. In this section, we determine the mean and variance of the service time and the mean of the total delay. We express them using means and variances of the constituent random variables.

First, consider the mean service time, which is required to complete the fixed point. From (5.27), noting that the complete transmission times $T_s$, $T_b\ell$, and $T_b\ell$ are constant we can express the mean service time for both schemes as

$$E[S_{i\in\{s,b\}}] = (1 - \alpha)(E[A_i^s] + T_i^s) + \alpha(E[A_i^b] + T_i^b), \quad (5.34)$$

where the expected values of the access delay $E[A_{ij}]$ can be calculated from (5.28) and (5.30).

Thus, based on (5.34), we can derive the mean service time in terms of $b$ and $\rho$. Now (3.1), (5.1), (5.5), (5.7), (5.8), (5.9) and (5.34) constitute a non-linear system of equations that can be solved iteratively to calculate $\rho$, $b$, $p$, and $E[S]$. This completes the fixed point calculation of the direct collision probabilities.

Each station will typically only have one message to send at a time, in which case $E[S]$ given by (5.34) is the total delay. However, if the load is unusually high, then the queueing delay can be calculated using the following calculations. This is the second place in which the Poisson assumption is used.

The total packet delay can be approximated by considering each node to be an M/G/1 queue. Note that this is only an approximation, since the service time here depends on whether or not it arrives at an empty queue, whereas that is not the case in the M/G/1 model. In order to use the M/G/1 model, we require the variance of the service time. This can be obtained analogously to the mean.

From (5.27), noting that the complete transmission times $T_s$, $T_r\ell$, and $T_b\ell$ are...
constant, we can express the variance of the service time for both schemes as

\[
\text{Var}[S_{i \in \{s,b\}}] = (1 - \alpha)(\text{Var}[A_i] + (E[S_i] - E[A_i] - T_i)^2) \\
+ \alpha(\text{Var}[A_i] + (E[S_i] - E[A_i] - T_i)^2). 
\] (5.35)

The variances of the access delays \(\text{Var}[A_i]\) in (5.35) can again be calculated from (5.28) and (5.30).

Using those values we can derive the mean queueing delay, \(E[Q_i]\), as follows

\[
E[Q_{i \in \{s,b\}}] = \lambda(\text{Var}[S_i] + E[S_i]^2) \frac{2(1 - \lambda E[S_i])}{2(1 - \lambda E[S_i])}. 
\] (5.36)

Note that the both event and routine safety packets share the same queue, so the queueing delay is same for both types of packets. Also, the terms \(E[S_i]\) and \(\text{Var}[S_i]\) are irrespective of the packet types.

The mean total delay for both types of packets are given by

\[
E[D_{i \in \{s,b\}}] = E[Q_i] + E[S_i]. 
\] (5.37)

Recall that this is a conservative bound on the delay experienced by the application, which is the time until the packet is first received successfully.

### 5.4 Simulations

In this section, we investigate the proposed schemes using a combination of simulation and the model derived in the previous section. The simulation environment is similar to the one used in Chapters 3 and 4. However, we have used a shorter transmission range of 250 m instead of 500 m to reduce the simulation time. In the previous chapter, we showed that the lower transmission range improves the PDR. But we should still be able to see the effect of the retransmission compared with the single transmission case. Also, we concentrate on the light traffic condition for the
Table 5.1: DSRC System Parameters for Retransmission Based Schemes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>32</td>
<td>Range, $R$</td>
<td>250 m</td>
</tr>
<tr>
<td>Slot size, $\sigma$</td>
<td>16 $\mu$s</td>
<td>DIFS</td>
<td>64 $\mu$s</td>
</tr>
<tr>
<td>SIFS</td>
<td>32 $\mu$s</td>
<td>$\alpha$</td>
<td>0.1,0.5</td>
</tr>
<tr>
<td>Vehicle density, $\beta$</td>
<td>10–100 $km^{-1}$</td>
<td>Data rate, $R_d$</td>
<td>12 Mbps</td>
</tr>
<tr>
<td>Packet arrival rate, $\lambda$</td>
<td>10 $s^{-1}$</td>
<td>Packet length, $P$</td>
<td>400 bytes</td>
</tr>
</tbody>
</table>

following simulation results. At higher traffic load additional mechanism is required to improve PDR which can be combined with our proposed protocol. Each vehicle is setup to broadcast messages with packet size $P = 400$ [bytes] and overall packet arrival rate $\lambda = 10$ [packets/sec] of both routine and event messages following a Poisson process. All the other DSRC related parameters are listed in Table 5.1.

Before evaluating the overall benefits of the proposed schemes, we first validate the analytical model for the blind sequential and batch schemes by comparing the numerical results with the simulation for $m = 3$ transmission attempts per packet. All simulation results are plotted with 95% confidence intervals.

Results in Figs. 5.2 and 5.3 are generated assuming 10% of safety messages are event packets ($\alpha = 0.1$). Fig. 5.2 shows the mean of the total delay as a function of vehicle density, $\beta$. Different curves are plotted for the delay of routine and event messages for the blind sequential and batch schemes, while the delay for standard DCF is represented by a single curve since standard DCF does not differentiate between routine and event messages. The analytical results are plotted using solid lines while the simulations results appear as dashed lines. Observe that the proposed analytical model agrees well with the simulation results. Simulation results for the piggybacked sequential scheme [46] are also plotted for comparison, and we will return to this shortly.

The longest mean delay observed for our proposed blind sequential and batch
Figure 5.2: Total delay until last transmission for the blind sequential, batch, standard DCF and piggybacked sequential schemes with $\alpha = 0.1$. Analytical results use solid lines, while simulation results use dashed lines. Only simulation results are given for the piggybacked sequential scheme.

schemes is around $2.1\,ms$ which is well below the maximum delay constraint of $100\,ms$ for safety applications [62]. This is despite the “total delay” for event packets being measured as the delay until the last copy is sent, rather than until the packet is first received; if the probability of success is high, then this will greatly overestimate the delay penalty for using the retransmission schemes. Note also that the actual delays are more closely clustered around the mean for DSRC than for protocols with binary exponential backoff, and so it is unlikely that any packet incurs a delay near $100\,ms$. In the plotted range, the mean delay increases almost linearly with the vehicle density. Also, the delays for routine safety packets for both blind sequential and batch schemes are similar. Under both schemes, the delay for event packets is greater than that for routine safety packets due to retransmissions,
with the difference being greater for the blind sequential scheme due to the backoff between each transmission attempt.

We also compare our results with simulation results for the piggybacked sequential scheme proposed in [46]. Note that in the original piggybacked sequential protocol, a packet was retransmitted only if the fraction of recipients that did not acknowledge it was above a threshold. Herein we take that threshold to be 0; thus any packet suffering loss is simply retransmitted until either it is received by all intended receivers, or the number of retransmission reaches the maximum limit \( m = 3 \). Fig. 5.2 shows that for the piggybacked sequential scheme, the delay until the last transmission is significantly higher than both the blind sequential and batch schemes when the vehicle density is not low. This is because of the need to wait for the piggybacked feedback before each retransmission.
The packet delivery ratio is plotted in Fig. 5.3, where the analytical results are computed according to (5.21)–(5.25). The model matches reasonably well with the simulation results, except that the model over-estimates the PDR for event messages in the batch scheme for high vehicle densities. The reason is that the model ignores the possibility of a batch colliding with multiple packets. The model could be extended to account for this, but at the expense of additional complexity. For both blind sequential and batch schemes, there is a significant improvement in PDR for event packets over routine packets. For example, the simulated PDR for event packets stays above 90% for all studied vehicle densities, while the PDR for routine packets drops to around 70% for high vehicle densities.
Figure 5.5: PDR for the blind sequential, batch, standard DCF and piggybacked sequential schemes with $\alpha = 0.5$
Figs. 5.4 and 5.5 show the mean of the total delay and the PDR for all schemes when 50% of safety messages are event packets ($\alpha = 0.5$). The increase in the proportion of event packets causes only a slight increase in the mean total delay; as before, the piggybacked sequential scheme has the largest delay for moderate to high vehicle densities. However, there are significantly more collisions (i.e., lower PDR) for all schemes for the larger value of $\alpha$.

Figs. 5.3 and 5.5 show that the batch and blind sequential retransmission schemes perform similarly for event messages. The model captures this similarity at low loads, while at high loads, it over-estimates the PDR for event messages in the batch scheme as already mentioned. For routine messages, Figs. 5.3 and 5.5 show that the batch scheme gives a slightly higher PDR than the blind sequential scheme. The routine message PDR for blind sequential and batch schemes is less than that of standard DCF (particularly at $\alpha = 0.5$), which is the penalty for improving the PDR of event messages through retransmissions.

The PDR for event messages in the piggybacked sequential scheme is worse than that of the blind sequential and batch schemes at low and moderate vehicle densities, but slightly better at high vehicle density. The PDR for routine messages in the piggybacked sequential scheme is similar to that of standard DCF at low vehicle density. This is because the piggybacked sequential scheme retransmits fewer packets than the blind sequential and batch schemes. At high vehicle density, however, the PDR of routine messages drops and is comparable to the blind sequential and batch schemes.
Figure 5.6: Relative improvement of the PDR for the blind sequential and batch transmission schemes with $\beta = 0.01$

Figure 5.7: Relative improvement of the PDR for the blind sequential and batch transmission schemes with $\beta = 0.05$
We now use the model to evaluate the improvement due to both of the proposed schemes. Figs. 5.6 and 5.7 show the percentage improvement (or degradation) of the PDR between using single transmission and the two proposed retransmission schemes.

Fig. 5.8 shows the impact of the number retransmissions, $m$, on PDR for blind sequential scheme. In this figure, we numerically optimized $m$ in the range 1 to 5 for the blind sequential scheme. We observe that at light load it is beneficial to use high number of retransmission attempts, $m$. However, at higher load, reducing $m$ helps by reducing channel load.

For low vehicle density ($\beta = 0.01$), the performance improvement in the PDR of event messages using retransmission is moderate as shown in Fig. 5.6. This is because at low traffic load, a single transmission would be sufficient to achieve adequate PDR performance for safety applications. On the other hand, at high vehicle density ($\beta = 0.05$) the relative improvement in PDR is higher. In particular, 10–15% improvement compared with using a single transmission is obtained for both retransmission schemes. The downside of using retransmission is a slight decrease in the PDR of routine safety messages, of up to 15%, which would require that they be sent slightly more frequently to maintain a target arrival rate. The degradation due to batch retransmissions is less than that due to blind sequential transmissions since it causes fewer partial collisions.

To show the influence of the contention window size $W$, we plot the PDR for the blind sequential scheme against different $W$ in Fig. 5.9. For event packets, the PDR improves with increased $W$ since the larger space between retransmissions increases the temporal diversity. Although, the model is somewhat conservative, it captures the large gap between the routine and event packets, and also the trend in PDR as $W$ increases. The performance of the batch scheme can be expected to be less sensitive to the contention window size, $W$, since it does not affect the diversity of the retransmissions.
Figure 5.8: The PDR for the blind sequential scheme with optimal $m \in [1, 5]$ and $\alpha = 0.5$

Figure 5.9: PDR for the blind sequential scheme with varying contention window, $W$ for $\beta = 0.05$ and $\alpha = 0.1$


5.5 Conclusion

In this chapter, we have proposed two extensions for the broadcast mode of the 802.11 DCF and EDCA protocols to prioritize and retransmit event safety packets. The analytical model presented in the last two chapters is also modified for this extensions. The results show that, batch retransmission, in which three copies of the packet are sent back-to-back, improves the packet delivery ratio of the important messages by up to 40% when 10% of packets are important. However, as our model has not considered multiple packet collision for batch scheme, the numerical results are optimistic compared to simulation results. In the current 802.11p standard the TXOP parameter is disallowed for ad hoc transmissions. If TXOP parameter is to be reinstated, the implementation of the batch scheme would become more feasible. Blind sequential retransmission, in which there is a random backoff between retransmissions, improves the PDR as well. We have also used simulation results for piggybacked sequential scheme which relies on feedback similar to the NACK sequential scheme presented in Chapter 4 but sending the feedback on the same channel. We have observed that the added cost of using feedback is only beneficial in high traffic load scenarios.

In this chapter, we did not consider multiple collisions for batch scheme which caused inaccuracy in the model. Future work will refine the batch model to consider multiple packet collisions. Once we have that, we can use these models to determine the conditions under which batch scheme outperform blind sequential scheme, and how high the load must be for the basic scheme with no retransmissions to be better.
Chapter 6

Protocol Enhancement

In this chapter, we focus on enhancing the extensions proposed in the Chapter 5 for the IEEE 802.11p MAC protocol. Through modeling and simulation, we have learned from previous chapters that direct collision is not as important as hidden terminal collision. We have also learned that the MAC layer delay is usually much lower than the QoS requirement. So, in this chapter, we focus on simplifying the modeling by ignoring direct collision and MAC layer delay while enhancing the extensions by adding extra delay between retransmission attempts.

As the operation of both blind sequential and piggybacked sequential schemes are similar apart from feedback, we classify the three extensions discussed in Chapter 5 into two categories:

1. sequential retransmission:
   
   (a) blind sequential retransmission,
   
   (b) piggybacked sequential retransmission.

2. batch retransmission.

Apart from the piggybacked sequential scheme, the other two schemes are analyzed in Chapter 5, while for the last extension only simulation results were presented. Neither sequential or batch retransmission schemes relies on any feedback from the receiving stations, nor introduce any additional protocol overhead. However, feedback is required in the piggybacked sequential scheme where negative acknowledgement will trigger the retransmission.

To this end, the main contributions of this chapter are:
1. the first analytic performance model of the piggybacked sequential scheme;

2. the provision of explicit technical details for the implementation of the piggybacked sequential scheme;

3. an extensible model for the batch scheme considering multiple collisions;

4. showing the impact of overhead induced by the piggybacked sequential scheme on the protocol performance.

6.1 Extensions

As in Chapter 5, we have proposed and evaluated two retransmission based extensions to the standard MAC protocol. Based on the observations, we present some modifications to the extensions and discuss the changes in the following subsections.

6.1.1 Sequential Retransmission

Similar to Chapter 5 we have a sequential retransmission scheme with and without feedback from the receivers. In both of these schemes, we only consider retransmission for event messages. For the blind sequential scheme, every event message is retransmitted a fixed number of times, whereas for the piggybacked sequential scheme, retransmission is based on the NACK from the intended receiver.

In this chapter, we keep the basic principle of the sequential scheme as before, but change the backoff mechanism between transmission attempts. Previously, we have ensured the gap between attempts for the blind sequential scheme using a larger MAC layer backoff window. For piggybacked sequential scheme, we have used a random gap time in the upper layer as we need to read the piggyback information to decide whether to retransmit or not. Now, for comparison between these two schemes it is useful to employ a similar upper layer gap time for both schemes. Also, we use a different random interval as a gap between two transmission attempts. We set a
minimum value for the gap time, $G_{\text{min}}$ to ensure that two successive transmission attempts does not collide with the same transmission. The maximum value for gap time, $G_{\text{max}}$ depends on the number of the retransmission attempt, $m$ and also the life time of the packet, $L$ sec. For the blind sequential scheme, $G_{\text{max}}$ can be set to a value such that all transmission attempts complete within the lifetime of the packet. For the piggybacked sequential scheme, this is harder to ensure as there is random delay in getting feedback from the receiver as well. So, we set $G_{\text{max}} = 0.6L/(m - 1)$ for both schemes which ensures delay to be bounded below $0.6L$ sec for blind sequential scheme, while for piggybacked sequential scheme allocating $0.4L$ sec for the feedback delay

### 6.1.2 Batch Retransmission

The batch scheme is essentially same as we have proposed in Chapter 5. However, we are making some changes in our assumptions when modeling the packet delivery ratio of event packets. Previously, we have not considered multiple packets colliding with a batch transmission and destroying all the subpackets. This assumption means our model for the batch scheme was optimistic compared to simulation results. In this chapter, we no longer make that assumption for event packets. Instead, we assume packet arrival as a Poisson process and calculate the probability of up to two packet arrivals during an event packet transmission. Note that, for routine packets, we still hold that assumption and model accordingly.

### 6.2 Sequential Retransmission

Our objective is to develop an approximation to compute the collision probability ignoring direct collision and the end-to-end packet delay experienced by the tagged vehicle. In the following derivations, many quantities are distinguished by subscripts and superscripts. For brevity, we use notation of the form $A_{j \in J} = f(j)$ to mean that $A_j = f(j)$ for each $j \in J$. 
6.2.1 Hidden Collision

We will derive an expression for the probability of collisions involving hidden terminals for routine and event messages. To do this, we consider two periods of vulnerability, before and after the transmission of a tagged packet. For a tagged packet not to be lost due to collisions with packets from hidden terminals, both of the following events must occur.

The first event is $H^b$ (“hidden, before”): the event that, when the tagged vehicle starts its transmission, none of the hidden terminals is in the destructive state. For each transmission attempt the terminal will be in the destructive state for a period of length $V^b$. This is the period of the packet transmission plus the preceding DIFS.

The second event is $H^a$ (“hidden, after”): the event that, none of the hidden terminals starts transmitting until after the tagged vehicle has left its vulnerable state. The tagged node is said to be in the vulnerable state when it is transmitting and a collision occurs if a node in the CS range starts transmitting. Let $V^a$ be the duration of the vulnerable state.

Unlike in the analysis of Aloha, these cases must be considered separately in CSMA systems, since the Poisson arrival of packets does not correspond to Poisson transmission of packets. In pure ALOHA network, the packets are sent immediately after generation regardless of the channel state. In contrast, CSMA relies on carrier sensing for scheduling packet transmission to reduce packet collision. As such, packets generated at different nodes within a packet duration time are spread out. This effect is not captured when we model packet transmission according to Poisson process. So, assuming the nodes hidden from each other are not synchronized, the average load on the channel is considered for “hidden, before” events. Once the packet transmission starts we assume new packets arrive as a Poisson process in the CS range resulting in collision for “hidden, after” events.

In the linear topologies considered in this paper, a hidden node to the left of the tagged node will only cause collisions with receivers that are also to the left of the tagged node. Hence we consider separately the collision events of the groups $L$ and
Chapter 6. PROTOCOL ENHANCEMENT

R of nodes respectively left and right of the tagged node, denoted \( \mathcal{H}_g^j \), for \( g \in \{L, R\} \) and \( j \in \{a, b\} \). By the symmetry assumption, each group experiences \( N_h / 2 \) hidden nodes.

First, consider the “hidden, before” collisions. These occur with a probability dependent on the fraction of time the channel is busy with that fraction of traffic from hidden nodes which can destroy the tagged node’s message. Thus the collision probability for a packet in \( g \in \{L, R\} \), is

\[
P(H^b_g) = 1 - \frac{N_h}{2} \sum_{c \in C} \gamma_c V^b.
\]

(6.1)

where \( C = \{r, e\} \) represents the set of all packet types (e.g. routine and event) and \( \gamma_c \) is the rate of batches of packets for packet type \( c \in C \).

Next, consider the “hidden, after” collisions \( H^a \). It is sufficient to consider the probability of this event given that \( H^b \) has occurred; that is, that none of the hidden terminals was in a destructive state when the tagged node started transmitting. In this case, carrier sensing has no effect, and arrivals should be modeled as Poisson. The arrival process of batches from the hidden terminals in group \( g \in \{L, R\} \) is a Poisson process. Event \( H^a_g \) occurs if no packet of is generated at any of the hidden terminals in group \( g \) during the \( V^a \) period. The conditional probability of this is

\[
P(H^a_g | H^b_g) = \exp \left( - \frac{N_h}{2} \sum_{c \in C} \gamma_c V^a \right).
\]

(6.2)

6.2.2 Number of Affected Nodes

The number of nodes affected by a transmission from a hidden node depends on the node distribution within the transmission range as well as in the potential hidden region. If the hidden node is further away from the tagged node, a lower number of receiving nodes can detect a collision. The number of nodes that have not yet successfully received the packet also depends on the number of the transmission attempts. Let the hidden node affecting the \( l^{th} \) transmission attempt from the
tagged node be placed distance $R - X_l$ away from the edge of the transmission region of the tagged node so that the distance between the tagged node and the hidden node is $2R - X_l$. All nodes on the same side of the sender as the hidden node within the range $[R - X_l, R]$ experience a collision on $l$th attempt. Assuming independence between transmissions of hidden nodes and uniformity of the placement of vehicles, the distribution of $X_l$ is given by $X_l \sim U(0, R)$ where $U$ represents the uniform distribution.

Now, for the first attempt, all nodes in the range $[R - X_1, R]$ sense collision. However, after the $l$th attempt, a node will only have failed to receive the packet if it experienced a collision on all $l$ attempts. That means we are only interested in nodes located in the range $[R - \min(X_1, X_2, \ldots, X_l), R]$. Now, let $X_{(l)} = \min(X_1, X_2, \ldots, X_l)$ which is the $l$th order statistic of $X_1, X_2, \ldots X_l$. The probability density function of $X_{(l)}$ is

$$f_{X_{(l)}}(x) = \frac{\binom{l}{i} \left( -\frac{2}{R} \right)^i}{\binom{R}{i} \frac{1 - x}{R}} \left( 1 - \frac{x}{R} \right)^{(l-1)}.$$  \hspace{1cm} (6.3)

Now, let $N_{c,l}$ be the number of nodes that have not received the packet in one side of the transmitter after the $l$th attempt. For a given $X_{(l)}$ the number of nodes follows a Poisson distribution. As we know the distribution of $X_{(l)}$, using the law of total probability we can also calculate the distribution of $N_{c,l}$. 

$$P[N_{c,l} = n] = \int_0^R P[N_{c,l} = n | X_{(l)} = x] f_{X_{(l)}}(x) dx$$

$$= \int_0^R e^{-\frac{N_n x}{2R}} \frac{(\frac{N_n x}{2R})^n}{n!} \cdot \frac{\binom{l-1}{i}}{\binom{R}{i}} \left( 1 - \frac{x}{R} \right)^{(l-1)} dx$$

$$= \int_0^R e^{-\frac{N_n x}{2R}} \frac{(\frac{N_n x}{2R})^n}{n!} \cdot \frac{\binom{l-1}{i}}{\binom{R}{i}} \sum_{i=0}^{l-1} \binom{l-1}{i} \left( \frac{l-1}{i} \right) \left( -\frac{x}{R} \right)^i \Gamma(n+i + 1, \frac{N_n x}{2R})$$

$$= \sum_{i=0}^{l-1} \binom{l-1}{i} \frac{\binom{l-1}{i}}{\binom{R}{i}} \Gamma(n+i + 1, \frac{N_n x}{2R}) $$
\[
\sum_{i=0}^{l-1} \left( -1 \right)^i \binom{l-1}{i} \frac{1}{i!} \left( \frac{2}{N_n} \right)^{(i+1)} \Gamma(n+i+1, N_n/2), \tag{6.4}
\]

where, \( \Gamma(n, x) \) is the incomplete gamma function.

### 6.2.3 Delay

Now, we will calculate the delay experienced by event packets due to gap between transmission attempts and waiting for feedback. We ignore the MAC access delay and packet transmission delay as they are two orders of magnitude less than the packet life time. However, the gap time and time required to get feedback can be significant. If the total delay is more than the packet life time, \( L \), the packet is dropped. For the blind sequential scheme, we can set the gap such that all transmission attempts are sent before the life time expires.

First we consider the delay caused by the gap time. Let \( T_{G,l} \) be the gap time after \( l^{th} \) transmission attempt which follows uniform distribution in the range \([G_{\text{min}}, G_{\text{max}}]\). So, the average delay experienced between each transmission attempt is \( \mathbb{E}[T_{G,l}] = \frac{(G_{\text{min}} + G_{\text{max}})}{2} \).

Next, we consider delay due to feedback defined as \( T_{F,l} \) which is only applicable for piggyback sequential scheme. The delay to receive feedback depends on number of nodes that have not yet received the packet, \( N_{c,l} \) up to the last packet transmission attempt. As each of those \( N_{c,l} \) nodes sends packets at a rate of \( \lambda \), total rate of packets with feedback is \( \lambda N_{c,l} \). The time required to get the first packet with feedback, \( T_{F,l} \) is exponentially distributed with rate \( \lambda_{c,l} \) conditioned on \( N_{c,l} \). Note that, \( N_{c,l} = 0 \) means despite hidden transmission, no collision is detected as there is no node in the collision range. Now, we consider \( N_{c,l} = 0 \) as a successful transmission attempt and for conditioning the time required to get feedback, \( T_{F,l} \) we only consider the case \( N_{c,l} > 0 \). The distribution for \( T_{F,l} \) can be calculated as

\[
P[T_{F,l} < t] = \sum_{n=1}^{\infty} \left( P[T_{F,l} < t | N_{c,l} = n] P[N_{c,l} = n] / P[N_{c,l} > 0] \right)
\]
Chapter 6. PROTOCOL ENHANCEMENT

\[
= \sum_{n=1}^{\infty} \left( 1 - e^{-\lambda nt} \right) \frac{P[N_{c,l} = n]}{P[N_{c,l} > 0]}, \quad (6.5)
\]

Once, we know the distribution of delay due to gap time, \(T_{G,l}\) and delay due to feedback, \(T_{F,l}\) for \(l^{th}\) attempt, we can calculate the total delay as

\[
T_l = \sum_{l=1}^{m-1} T_{G,l} + T_{F,l}. \quad (6.6)
\]

6.2.4 Packet Delivery Ratio

To calculate the packet delivery ratio, we ignore direct collision and we consider the left and right groups separately for hidden collisions. A packet is successfully delivered to the group if any of the transmission attempts was successfully received by the left most node for the left group and symmetrically by the right most node for the right group. Note that successful transmission occurs by either having no hidden transmission or having no node in the collision range. Let \(P(S_g)\) denote the probability of successful transmission for the group \(g \in \{L, R\}\) and estimate it by

\[
P(S_{l,g}) = P(H^b_g)P(H^a_g|h^b_g) + \left(1 - P(H^b_g)P(H^a_g|h^b_g)\right) \cdot P[N_{c,l} = 0]. \quad (6.7)
\]

So, the PDR for the each of the groups can be expressed as

\[
PDR_{g,c} = P(S_{1,g}) + (1 - P(S_{1,g})) \cdot P[T_1 < L] \cdot P(S_{2,g}) + \]

\[
\cdots + \prod_{l=1}^{m_c-1} (1 - P(S_{l,g})) \cdot P[T_{m_c} < L] \cdot P(S_{m_c,g})
\]

\[
= \sum_{i=1}^{m_c} \left( P[T_i < L] \cdot P(S_{i,g}) \prod_{i=1}^{i-1} (1 - P(S_{l,g})) \right). \quad (6.8)
\]

where \(m_c\) is the maximum number of attempts for each message of type \(c \in C\).

Finally, considering both left and right group together, the PDR for class \(c\) can
be estimated by

\[ PDR_c = PDR_{g,c}^2. \] (6.9)

Calculating the collision probability (6.1), (6.2) requires the load \( \gamma_c \) for each class of packets. Let \( M_e \) denote the (random) number of transmission attempts for an event message. For the piggyback sequential scheme, \( M_e \) is the number of attempts until the message is received successfully in both the left and right groups. For the blind sequential scheme, \( M_e = m \). So we have,

\[ g_r = \lambda_r = (1 - \alpha)\lambda, \] (6.10)
\[ g_e = E[M_e] \lambda_e = E[M_e^a] \alpha \lambda. \] (6.11)

The complete transmission time and the vulnerable periods for each transmission are

\[ T = t_{\text{data}} + t_{\text{difs}} + t_{\text{oh}}, \] (6.12)
\[ V^b = t_{\text{data}} + t_{\text{difs}} + t_{\text{oh}}, \] (6.13)
\[ V^a = t_{\text{data}} - t_{\text{difs}} + t_{\text{oh}} \] (6.14)

where \( t_{\text{oh}} \) is an overhead time. For the blind sequential scheme, \( t_{\text{oh}} = 0 \). For the piggyback sequential scheme, \( t_{\text{oh}} \) depends on the time \( t_{\text{id}} = 2^n / R_d \) required to send a single message ID, where \( R_d \) is the data rate and \( n_i \) is the length of the message ID in bits. It also depends on the number of packets being acknowledged, which is a random number that depends on the vehicle density. Since only the most recent event message is acknowledged for each neighboring station, the mean over head is

\[ \overline{t_{\text{oh}}} = N_n t_{\text{id}}. \] (6.15)
Effect of ID bits

The choice of $n_i$ incurs a tradeoff: If IDs are too long then the overhead is excessive, but if they are too short then many packets can have the same ID. If two packets share the same ID then acknowledging one will appear to acknowledge the other. If the probability of this is negligible, then (6.8) and (6.9) can be used to estimate the PDR. Otherwise, they must be modified as follows. A retransmission will occur if either the left or right group sends a NACK. This couples the left and right groups so that (6.9) no longer holds. Recall that each packet ACKs the most recent event packet from each station within its range, and a NACK consists of a packet not ACKing the tagged packet.

If the transmission radius is $R$ then the most recent event packet from any station within $R$ of the furthest node in $g$ could block a NACK from group $g$. This occurs when the tagged node is not received, but a packet from the other station with the same packet ID is received and acknowledged. If each of these packets has a probability of $2^{-n_i}$ of blocking the NACK, then the probability that a NACK is blocked can be approximated by

$$F = 1 - (1 - 2^{-n_i})^{N_n}, \quad (6.16)$$

where $N_n$ is the number of transmitters within the transmission range of the tagged node. It assumes that packets are received by all nodes within radius $R$; this is likely if $\lambda \gg 1/L$, but is optimistic otherwise.

The PDR when $m = 2$ can be found by considering the four possible outcomes of the first transmission attempt: success or failure in the left and right groups. Let $P = P(S_g)$ and let $X = F(1 - P(S_g))$ be the probability of a collision in group $g$ that does not receive a NACK. Since the tagged packet will be retransmitted if either the left or right group sends a NACK, the PDR is

$$PDR_e = P^2 \cdot 1 + 2P(1 - P) \cdot (1 - F)P + (1 - P)^2 \cdot (1 - F^2)P^2$$
\[ P^2[1 + 2(1 - P) + (1 - P)^2 - 2F(1 - P) - F^2(1 - P)^2] \]
\[ = (1 - (1 - P(S_g))^2) - P(S_g)^2(2X + X^2). \]  
(6.17)

### 6.2.5 Simulation Results

In this section, we validate the analytical model developed in Section 6.2.4 using simulation, and compare the performance of the piggybacked sequential scheme with that of a simple blind retransmission scheme.

We use a similar simulation environment as that described in Section 4.4. Each vehicle broadcasts messages using \( P = 200 \) [bytes] packets with the total arrival rate of both routine and event messages being \( \lambda = 10 \) messages per second. Event packets are generated following a Poisson process with a rate of \( \alpha \lambda \) [packets/sec] whereas routine packets are sent with a rate of \( (1 - \alpha)\lambda \). The transmissions routine packets are almost periodic, except that (a) to remove any synchronization effect, 10\% of jitter is introduced and (b) the inter-arrival time is reset after each event packet is generated. Because scheduled routine packet transmission is reset once an event packet is generated, if we set the rate of generating routine packets at \( (1 - \alpha)\lambda \) then actual rate would be lower than that. In such case we cannot compare the simulation results with numerical results. As such we generate routine packets at a rate \( \frac{-\lambda \alpha \log(1-\alpha)}{\log(1-\alpha)} \) so that the actual rate of routine packets is \( (1 - \alpha)\lambda \).

For both schemes there is a gap between two transmission attempts which is uniformly distributed between \( G_{\text{min}} \) and \( G_{\text{max}} \). The minimum gap time, \( G_{\text{min}} \) is set to 5 \( ms \) to reduce the probability of successive collisions, where as the maximum gap time is chosen as \( G_{\text{max}} = 60 \) \( ms \) and 30 \( ms \) when using up to two \( (m = 2) \) and three \( (m = 3) \) transmission attempts respectively. Furthermore, in the piggybacked sequential scheme, a node has to wait until it receives a negative feedback from the receiving node. As a result, the retransmission may be delayed even after the expiration of the packet’s lifetime \( L \) of the event message (which is set to 100 \( ms \) in our study). To alleviate this problem, upon receiving the feedback if there is less than
Table 6.1: DSRC System Parameters for Retransmission Based Schemes

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>32</td>
<td>Range, $R$</td>
<td>250 m</td>
</tr>
<tr>
<td>Slot size, $\sigma$</td>
<td>16 $\mu$s</td>
<td>DIFS</td>
<td>64 $\mu$s</td>
</tr>
<tr>
<td>SIFS</td>
<td>32 $\mu$s</td>
<td>$\alpha$</td>
<td>0.1, 0.5</td>
</tr>
<tr>
<td>Vehicle density, $\beta$</td>
<td>10 – 100 km$^{-1}$</td>
<td>Data rate, $R_d$</td>
<td>6 Mbps</td>
</tr>
<tr>
<td>Packet arrival rate, $\lambda$</td>
<td>10 s$^{-1}$</td>
<td>Packet length, $P$</td>
<td>200 bytes</td>
</tr>
</tbody>
</table>

$G_{\text{max}}$ remaining of the packet’s lifetime, the retransmission will be brought forward by randomly and uniformly choosing the backoff within the remaining time. Also, if a routine packet is generated while an event message is scheduled for retransmission, both packets are sent back to back. For the piggybacked sequential scheme the packet size is increased as the vehicle density increases to reflect the overhead in providing feedback. However, the list of IDs is not explicitly transmitted with the packets. The number of bits for each packet ID is chosen to be 16 bits. Later, from Fig. 6.5 we will justify the choice of ID bits per packet.

All the other DSRC related parameters are listed in Table 6.1. In the following we show validation results for both schemes using up to two ($m = 2$) and three ($m = 3$) transmission attempts at various vehicle densities. We show results for scenarios where 10% and 50% of messages (i.e. $\alpha = 0.1, 0.5$) are event messages representing both typical and extreme situations in event triggered safety communication. All the simulation results are plotted with 2$\sigma$ confidence intervals.

In Figs. 6.1 and 6.2 the PDR is plotted against vehicle density when 10% of messages are event packets. Observe that the model matches reasonably well with the simulation results despite the simplifications made in the model such as ignoring the direct collisions. It can be seen that for both single ($m = 2$ in Fig. 6.1) and two retransmissions ($m = 3$ in Fig. 6.2), the PDR for event messages is significantly improved compared to the single transmission case (i.e. no retransmission), although
the PDR for routine messages is slightly worse as expected. In particular, the PDR for event messages stays above about 90% in the single retransmission even at high density, and is around 95% for all the densities studied when there were two retransmission. Compared to single transmission case the PDR improvement can be up to 17% at medium density of 50 [vehicles/km]. Surprisingly, the PDR of the blind sequential scheme has outperformed that of the piggybacked sequential scheme indicating that the overhead outweighs the benefit of the selective retransmission.

Note that at high vehicle densities, the numerical results are optimistic compared with simulation results. The inaccuracy is due to two main factors. Firstly, in our analysis the potential hidden region is fixed regardless of the vehicle density. This is because we assumed the furthest receiving node from the tagged node is at the boundary of the transmission range. However, when the vehicle density is low, the furthest receiving node is well within the transmission range and as such, the
potential hidden region shrinks. Secondly, for analytical simplicity we assumed independence between transmission from two hidden nodes. But if both nodes are receiving a packet from a node located between them and both also have packets to send, they will wait until the transmission of the ongoing packet is finished, and then transmit at nearly the same time with high probability of collision. In addition, there is also a chance that a new event message is generated before the successful reception or the expiration of packet’s lifetime of the previous event message. All of the above can be accounted for in the model at the expense of additional complexity.

Despite the inaccuracy, however, the model both captures the trend of the PDR drop with increased vehicle density and correctly identifies which scheme performs better. As mentioned earlier the piggybacked sequential scheme performs worse than blind sequential scheme despite having fewer attempts per event message. This is due to the increased overhead per packet, especially at high vehicle density. Routine
messages for the piggybacked sequential scheme also perform worse due to the same overhead.

Also observe in Fig. 6.2 that increasing in the number of retransmission attempts (from $m = 2$ to $m = 3$) results in a higher PDR with significant improvement at high densities. There is up to 5% improvement in PDR for event messages at a density of 100 [vehicles/km]. The PDR for routine messages drops only slightly compared to Fig. 6.1. Note that this is for $\alpha = 0.1$, when only 10% of all the messages are event messages. When the fraction of event messages increases (i.e. $\alpha = 0.5$), so does the channel load, and the PDR for both routine messages and event messages drops as seen in Figs. 6.3 and 6.4. In this extreme case where 50% of messages are event packets, the PDR requirement of 95% can still be achieved at medium vehicle density with two retransmissions. The blind sequential scheme continues to perform better than the piggybacked sequential scheme in this case. At this density,
the relative PDR improvement compared to single transmission can still reach up to 17% for $m = 3$, but drops to 15% for $m = 2$ case. This suggests that for $\alpha = 0.1$ case $m = 2$ retransmission attempts provides optimum PDR performance while for $\alpha = 0.5$ case $m = 3$ retransmission attempts are required. Note also that for the piggybacked sequential scheme there is a larger gap between analysis and simulation than for the blind sequential scheme due to the fact that the tagged node needs to wait for feedback from a node that suffered the collision before it can retransmit.

As the message life time is limited ($L = 100 \text{ms}$) some of the lost packets are not retransmitted due to lack of feedback which is not modeled.

In Fig. 6.5 we investigate how varying the number of ID bits per packet (i.e. the overhead) affects on PDR for the piggybacked sequential scheme. Initially, when number of bits per packet ID is increased from 8 bits to 12 bits we see improvement in PDR as the false positive rate decreases. However, increasing it further causes
the PDR to drop, as the overhead for piggybacking now has negative impact on PDR. Observe that approximately 12 bits overhead gives the best performance for piggybacked sequential scheme regardless of the amount of event messages. However, we choose 16 bits as the number of bits per packet ID for all the simulations which provides close to optimum PDR performance while being on the conservative side.

In order to test the predictive power of the models, we use them to estimate the “crossover” fraction $\alpha$ of event messages for which piggyback and blind sequential schemes have equal PDR; at higher $\alpha$, piggybacked sequential scheme will perform better because its overhead is less sensitive to $\alpha$. For the nominal value of $\lambda = 10$ [packets/sec], the blind sequential scheme always seems to outperform the piggybacked sequential scheme, and so we studied the higher rate of $\lambda = 20$ [packets/sec]. The results, shown in Fig. 6.6, are for $P = 200$ [bytes] packets with the optimal number of bits (12) for packet IDs. The crossover points predicted using the model agree quite closely with simulations for a range of $\alpha$ values and vehicle densities.

Figure 6.5: PDR for piggybacked scheme with varying ID bits for $m = 2$. 
6.3 Batch Retransmission

For the batch scheme, we have multiple subpackets within a single batch of transmission for event packets. Note that multiple packets may collide with a single event packet and destroy the packet. There are many possible ways an event packet can be corrupted by multiple collisions, specially when number of subpackets per batch transmission, $k$, is high. For routine packets, however, the chance of multiple collision is small as in blind sequential scheme. So, we derive the expression of packet delivery ratio for routine packets and event packets separately in the following subsections.

6.3.1 Routine Packets

For routine packet, we follow the same approach as blind sequential scheme.
Since there is a single batch transmission per packet, the rates of batch transmission are

\[ \gamma_r = \lambda_r = (1 - \alpha)\lambda, \]  
\[ \gamma_e = \lambda_e = \alpha\lambda. \]  

For routine packet, the PDR is calculated from (6.1) and (6.2). To apply those equations, we calculate the vulnerable period for routine packets. As vulnerable period depends on the type of colliding packets, we denote \( V_{j\in\{a,b\}}^{c\in\{r,e\}} \) as the period when a routine packet is vulnerable to collision by a packet of type \( c \) transmitted before \( (j = b) \) or after \( (j = a) \) itself. The complete transmission time and vulnerable period for each packet are

\[ V_e^b = T_e = k \cdot t_{\text{data}} + (k - 1) \cdot t_{\text{sifs}} + t_{\text{difs}}, \]  
\[ V_r^b = T_r = t_{\text{data}} + t_{\text{difs}}, \]  
\[ V_e^a = t_{\text{data}} - t_{\text{difs}}, \]  
\[ V_r^a = t_{\text{data}} - t_{\text{difs}}. \]

Here, a gap between successive subpacket of a single batch is maintained. However, later in Subsection 6.3.2 we will consider the batch as successive subpackets without any gap for simplicity.

### 6.3.2 Event Packets

Now, we need to calculate PDR for event packets in the batch scheme. Let us define a Poisson Point process \( R(t) \) which represents the routine packet arrival process with a rate \( N_h \gamma_r \). Also, we define the arrival process of event packets as \( E(t) \) with a rate \( N_h \gamma_e \). We denote the starting time and finishing time of \( i^{th} \) subpacket as \( S_i \) and \( E_i \) respectively for \( i \in [1,k] \).

We are only interested in the probability of \( R(t) \) or \( E(t) \) having at least one event
Chapter 6. PROTOCOL ENHANCEMENT

in any time interval. To ease notation, let $R(A)$ for any interval $A$ denote the event that $R(t) \geq 1$ for some $t \in A$, and define $E(A)$ analogously. Further, define

$$R_{-i} = R([S_1 - it_{\text{data}}, S_1 - (i-1)t_{\text{data}}])$$
$$R_{+i} = R([S_1 + (i-1)t_{\text{data}}, S_1 + it_{\text{data}}])$$
$$E_{-i} = E([S_1 - it_{\text{data}}, S_1 - (i-1)t_{\text{data}}])$$
$$E_{+i} = E([S_1 + (i-1)t_{\text{data}}, S_1 + it_{\text{data}}])$$

(6.24)

The probability of each of the above mentioned events is directly calculated from the Poisson distribution as

$$P[R_i] = 1 - e^{-\frac{Nh_2}{2}t_{\text{data}}}$$
$$P[E_i] = 1 - e^{-\frac{Nh_2}{2}t_{\text{data}}}$$

(6.25)

Let us now formally define a collision,

**Definition 1.** The $i^{th}$ subpacket collides with a routine packet arriving at $t$ if $t \in [S_i - T_r, E_i]$ and $R(t) = 1$ and similarly the $i^{th}$ subpacket collides with an event packet arriving at $t$ if $t \in [S_i - T_e, E_i]$ and $E(t) = 1$.

**Definition 2.** The $i^{th}$ subpacket experiences a collision with routine packet if $\exists t$ s.t. the $i^{th}$ subpacket collides with a routine packet arriving at $t$ and similarly $i^{th}$ subpacket experiences a collision with an event packet if $\exists t$ s.t. the $i^{th}$ subpacket collides with event packet arriving at $t$.

From Definition 2, we calculate the probability of a collision with routine packet and with event packet as

$$P[\text{collision with routine packet}] = P[R([S_i - T_r, E_i])]$$
$$P[\text{collision with event packet}] = P[E([S_i - T_e, E_i])]$$

(6.26)
Definition 3. A batch of subpackets experiences a loss if \( \forall i \exists t \) s.t. \( i^{th} \) subpacket collides with a routine packet or an event packet arriving at \( t \).

Theorem 1. The probabilities of a loss for \( k = 2 \) is

\[
P[event \ loss] = 1 - e^{-\frac{Nk}{h}(\gamma_r + 2\gamma_e)T_{data}}(1 - (1 - e^{-\frac{Nk}{h}M_{data}})^2). \tag{6.27}
\]

Proof.

\[
P[event \ loss] = P[\forall i (R([S_i - T_r, E_i]) \text{ or } E([S_i - T_e, E_i]))]
\]

Ignoring gaps between subpackets and also DIFS spacing, we can replace \( T_r = t_{data} \) and \( T_e = 2t_{data} \)

\[
P[event \ loss] = P[\forall i (R([S_i - t_{data}, S_i + t_{data}]) \text{ or } E([S_i - 2t_{data}, S_i + t_{data}]))]
\]

Expanding the equation for both subpackets we get two sets of condition, all of which must be met

\[
P[event \ loss] = P([R([S_1 - t_{data}, S_1 + t_{data}]) \text{ or } E([S_1 - 2t_{data}, S_1 + t_{data}])) \text{ and } (R([S_2 - t_{data}, S_2 + t_{data}]) \text{ or } E([S_2 - 2t_{data}, S_2 + t_{data}]))]
\]

Using (6.24) we have

\[
P[event \ loss] = P([R_{-1} \text{ or } R_{+1} \text{ or } E_{-2} \text{ or } E_{-1} \text{ or } E_{+1}]) \text{ and } (R_{+2} \text{ or } E_{-1} \text{ or } E_{+1} \text{ or } E_{+2})]
\]

Each of the \( R_{+1}, E_{-1} \) and \( E_{+1} \) events destroys all subpackets and so, these events
can be taken out of the two sets of conditions for each subpacket

\[ P[\text{event loss}] = P[\mathbb{R}_i \text{ or } \mathbb{E}_i \text{ or } \mathbb{E}_{i+1} \text{ or } ( (\mathbb{R}_{i-1} \text{ or } \mathbb{E}_{i-2}) \text{ and } (\mathbb{R}_{i+2} \text{ or } \mathbb{E}_{i+2}) )] \]

Following DeMorgan Laws we have

\[ P[\text{event loss}] = 1 - (1 - P[\mathbb{R}_i]) (1 - P[\mathbb{E}_i]) (1 - P[\mathbb{E}_{i+1}]) \]
\[ (1 - P[(\mathbb{R}_{i-1} \text{ or } \mathbb{E}_{i-2}) \text{ and } (\mathbb{R}_{i+2} \text{ or } \mathbb{E}_{i+2})]) \]

Now, we expand and simplify the probability \( P[(\mathbb{R}_{i-1} \text{ or } \mathbb{E}_{i-2}) \text{ and } (\mathbb{R}_{i+2} \text{ or } \mathbb{E}_{i+2})] \) as

\[ P[(\mathbb{R}_{i-1} \text{ or } \mathbb{E}_{i-2}) \text{ and } (\mathbb{R}_{i+2} \text{ or } \mathbb{E}_{i+2})]
= P[(\mathbb{R}_{i-1} \text{ or } \mathbb{E}_{i-2})] P[(\mathbb{R}_{i+2} \text{ or } \mathbb{E}_{i+2})]
= (1 - P[\mathbb{R}_{i-1}] P[\mathbb{E}_{i-2}]) (1 - P[\mathbb{R}_{i+2}] P[\mathbb{E}_{i+2}]) \]

As all the \( \mathbb{R}_i \) events are identically distributed and \( \mathbb{E}_i \) events are also identically distributed

\[ P[\text{event loss}] = 1 - (1 - P[\mathbb{R}_i]) (1 - P[\mathbb{E}_i])^2 (1 - (1 - P[\mathbb{R}_i] P[\mathbb{E}_i])^2)
= 1 - e^{-\frac{N_\mathbb{E}}{\eta} \gamma t_{data} e^{-\frac{N_\mathbb{E}}{\eta} \gamma t_{data}}} (1 - (1 - e^{-\frac{N_\mathbb{E}}{\eta} \gamma t_{data} e^{-\frac{N_\mathbb{E}}{\eta} \gamma t_{data}}})^2)
= 1 - e^{-\frac{N_\mathbb{E}}{\eta} (\gamma t_{data} + 2\gamma t_{data})} (1 - (1 - e^{-\frac{N_\mathbb{E}}{\eta} \lambda t_{data}})^2) \]

For notational convenience, let us define \( \mathbb{R}\mathbb{E}_x \) event which occur when either a routine packet or an event packet arrives such that it only affect \( x^{th} \) subpacket. Similarly, define \( \mathbb{R}\mathbb{E}_{xy} \) event which affects both \( x^{th} \) and \( y^{th} \) subpackets. In particular,
we define the following four terms.

\[
\begin{align*}
R_E_1 &= R - 1 \text{ or } E - 3 \\
R_E_{12} &= R + 1 \text{ or } E - 2 \\
R_E_{23} &= R + 2 \text{ or } E + 2 \\
R_E_3 &= R + 3 \text{ or } E + 3
\end{align*}
\] (6.28)

As routine packet arrival and event packet arrival are independent events, the probability of each of the above mentioned events can be directly calculated from Poisson distribution as follow

\[
P[R_E_i] = 1 - e^{-\frac{Nh}{2} \gamma t_{data}} e^{-\frac{Nh}{2} \gamma t_{data}} = 1 - e^{-\frac{Nh}{2} \lambda_{data}}
\] (6.29)

**Theorem 2.** The probabilities of a loss for \(k = 3\) is

\[
P[\text{event loss}] = 1 - e^{-Nh \gamma t_{data}} (3e^{-Nh \lambda_{data}} - 2e^{-3Nh \lambda_{data}}).
\] (6.30)

**Proof.**

\[
P[\text{event loss}] = P[\forall i \ (R((S_i - T_r, E_i)) \text{ or } E((S_i - T_e, E_i)))]
\]

Ignoring gaps between subpackets and also DIFS spacing, we have \(T_r = t_{data}\) and \(T_e = 3t_{data}\)

\[
P[\text{event loss}] = P[\forall i \ (R((S_i - t_{data}, S_i + t_{data})) \text{ or } E((S_i - 3t_{data}, S_i + t_{data})))]
\]

Expanding the equation for all three subpackets we get two sets of condition, all of
Figure 6.7: Karnaugh Map to simplify the expression \(((\text{RE}_1 \text{ or } \text{RE}_{12}) \text{ and } (\text{RE}_{12} \text{ or } \text{RE}_{23}) \text{ and } (\text{RE}_{23} \text{ or } \text{RE}_3))\) to calculate the loss probability of event packets using batch scheme with 3 subpackets.

which must be met

\[
P[\text{event loss}] = P[\text{RE}([S_1 - t_{\text{data}}, S_1 + t_{\text{data}}]) \text{ or } \text{RE}([S_1 - 3t_{\text{data}}, S_1 + t_{\text{data}}])]
\]

and \(\text{RE}([S_2 - t_{\text{data}}, S_2 + t_{\text{data}}]) \text{ or } \text{RE}([S_2 - 3t_{\text{data}}, S_2 + t_{\text{data}}])\)

and \(\text{RE}([S_3 - t_{\text{data}}, S_3 + t_{\text{data}}]) \text{ or } \text{RE}([S_3 - 3t_{\text{data}}, S_3 + t_{\text{data}}])\)

\[
= P[\text{RE}([S_1 - t_{\text{data}}, S_1 + t_{\text{data}}]) \text{ or } \text{RE}([S_1 - 3t_{\text{data}}, S_1 + t_{\text{data}}])]
\]

and \(\text{RE}([S_1, S_1 + 2t_{\text{data}}]) \text{ or } \text{RE}([S_1 - 2t_{\text{data}}, S_1 + 2t_{\text{data}}])\)

and \(\text{RE}([S_1 + t_{\text{data}}, S_1 + 3t_{\text{data}}]) \text{ or } \text{RE}([S_1 - t_{\text{data}}, S_1 + 3t_{\text{data}}])\)

\[
= P[\text{RE}_-1 \text{ or } \text{RE}_+1 \text{ or } \text{RE}_-3 \text{ or } \text{RE}_-2 \text{ or } \text{RE}_-1 \text{ or } \text{RE}_+1]
\]

and \(\text{RE}_+1 \text{ or } \text{RE}_+2 \text{ or } \text{RE}_-2 \text{ or } \text{RE}_-1 \text{ or } \text{RE}_+1 \text{ or } \text{RE}_+2\)

and \(\text{RE}_+2 \text{ or } \text{RE}_+3 \text{ or } \text{RE}_-1 \text{ or } \text{RE}_+1 \text{ or } \text{RE}_+2 \text{ or } \text{RE}_+3\)]

Each of the \(\text{RE}_-1\) and \(\text{RE}_+1\) events destroys all subpackets and so, these events can be
Chapter 6. PROTOCOL ENHANCEMENT

taken out of the three sets of conditions for each subpacket

\[ P[\text{event loss}] = P[E_{-1} \text{ or } E_{+1}] \]
\[ \quad \text{or } ((R_{-1} \text{ or } R_{+1} \text{ or } E_{-3} \text{ or } E_{-2}) \]
\[ \quad \text{and } (R_{+1} \text{ or } R_{+2} \text{ or } E_{-2} \text{ or } E_{+2}) \]
\[ \quad \text{and } (R_{+2} \text{ or } R_{+3} \text{ or } E_{+2} \text{ or } E_{+3})) \]
\[ = P[E_{-1} \text{ or } E_{+1}] \]
\[ \quad \text{or } ((RE_{1} \text{ or } RE_{12}) \text{ and } (RE_{12} \text{ or } RE_{23}) \text{ and } (RE_{23} \text{ or } RE_{3})) \]

Following DeMorgan Laws we have

\[ P[\text{event loss}] = 1 - (1 - P[E_{-1}])(1 - P[E_{+1}]) \]
\[ \quad (1 - P[(RE_{1} \text{ or } RE_{12}) \text{ and } (RE_{12} \text{ or } RE_{23}) \text{ and } (RE_{23} \text{ or } RE_{3})]) \]

Using Karnaugh Map shown in Figure 6.7 we have

\[ P[\text{event loss}] = 1 - (1 - P[E_{-1}])(1 - P[E_{+1}]) \]
\[ \quad \cdot (1 - (P[RE_{12} \text{ and } RE_{23}] + P[RE_{12} \text{ and } RE_{23} \text{ and } RE_{1}] \]
\[ \quad + P[RE_{12} \text{ and } RE_{23} \text{ and } RE_{3}])) \]
\[ = 1 - (1 - P[E_{-1}])(1 - P[E_{+1}]) \]
\[ \quad \cdot (1 - P[RE_{12}]P[RE_{23}] - (1 - P[RE_{12}])P[RE_{23}]P[RE_{1}] \]
\[ \quad - P[RE_{12}](1 - P[RE_{23}])P[RE_{3}] \]

As all the \( R_i \) events are identically distributed and \( RE_i \) events are also identically distributed

\[ P[\text{event loss}] = 1 - (1 - P[E_i])^2(1 - P[RE_i]^2 - 2(1 - P[RE_i])P[RE_i]P[RE_i]) \]
The probabilities for the events are calculated from (6.25) and (6.29)

\[ P[\text{event loss}] = 1 - (e^{-\frac{Nh}{2} \gamma e_t data})^2 (1 - (1 - e^{-\frac{N_h}{2} M_{data}})^2 - 2e^{-\frac{N_h}{2} M_{data}}(1 - e^{-\frac{N_h}{2} M_{data}})^2) \]

\[ = 1 - e^{-\frac{N_h}{2} \gamma e_t data} (3(e^{-\frac{N_h}{2} M_{data}})^2 - 2(e^{-\frac{N_h}{2} M_{data}})^3) \]

\[ = 1 - e^{-\frac{N_h}{2} \gamma e_t data} (3e^{-N_h M_{data}} - 2e^{-3\frac{N_h}{2} M_{data}}) \]

Finally, the PDR for routine and event packets can be calculated from the probability of a packet loss as

\[ PDR_r = P[\text{routine loss}], \]  
\[ PDR_e = P[\text{event loss}]. \] (6.31)  
\[ (6.32) \]

### 6.3.3 Simulation Results

In this subsection, we evaluate the batch scheme with numerical results as well as simulation results. The simulation environment is the same as Sub-section 6.2.5. For the following results we have used \( m = 2 \) and \( m = 3 \) transmission attempts per packet. All the simulation results are plotted with a 95% confidence interval.

In Fig. 6.8 the PDR is plotted against vehicle density. The PDR for event messages is better than single transmission case, although PDR for routine messages are slightly worse as expected. In terms of modeling accuracy, at low load the model is slightly pessimistic. This can be due to the fact that there may be no node located in the collision region as discussed for blind sequential scheme. At higher vehicle densities, the numerical results become optimistic compared with simulation results.

In Fig. 6.9 we see a similar trend as Fig. 6.8 with larger gaps between numerical and simulation results. As half of the packets are now event packets, the channel load increases significantly and routine packet suffer more. The advantage of transmitting \( m = 2 \) copies of each event packet diminishes as \( \alpha \) increases. The accuracy of the model, however, is much better than what we have observed in previous chapter. This suggests that multiple collision is a major cause of packet loss in batch scheme.
Figure 6.8: Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 2$.

Figure 6.9: Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 2$. 
In Fig. 6.10 and Fig. 6.11 we increase the number of retransmission attempts from \( m = 2 \) to \( m = 3 \). As long as, the fraction of event packets, \( \alpha \), is low, the PDR for event packets improves significantly while maintaining low cost on routine packets. With \( \alpha = 0.5 \) the model predicts improvement for the PDR of event packets with significantly higher chance of packet loss for routine packets. From the simulation, however, the improvement for event packets is less prominent despite increased loss for routine packets. In terms of modeling accuracy, we compare the results of this model to the ones presented in Chapter 5. The numerical results for batch scheme presented in Fig. 5.5 shows up to 5% difference between model and simulation and in Fig. 5.5(a) the discrepancy reaches up to 10% specially near high vehicle density (\( \beta = 100 \) [vehicles/km]). In contrast results obtained from the new analytical model differ from simulation by only 1% and 5% respectively for \( \alpha = 0.1 \) and \( \alpha = 0.5 \) case. The improvement in accuracy is because we consider multiple collisions in event packet which we ignored in the previous model.

Next, we compare the PDR for all three schemes with varying fraction of event packets in Figs. 6.12 and 6.13. The vehicle density is kept constant at \( \beta = 50 \) [vehicles/km] and rate of safety message, \( \lambda = 10 \) [packets/sec]. For all values of \( \alpha \) we observe that batch scheme performs worst, and the PDR drops below single transmission case when most of the safety packets are event packets. A similar trend is observed for blind sequential scheme, where PDR drops as \( \alpha \) increases due to increased load on channel. For piggybacked sequential scheme however, we do not observe much decrease in PDR as \( \alpha \) increases due to low number of retransmissions. Still, blind sequential scheme outperforms piggybacked sequential scheme due to extra overhead for feedback as well as expiry of life time for event packets.
Figure 6.10: Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.1$ and $m = 3$.

Figure 6.11: Comparison of PDR for batch retransmission scheme, comparing simulations (dashed) with the model (solid) for $\alpha = 0.5$ and $m = 3$. 
Figure 6.12: PDR (numerical) for different schemes with varying fraction of event packets for $m = 2$ and $\beta = 50$.

Figure 6.13: PDR (numerical) for different schemes with varying fraction of event packets for $m = 3$ and $\beta = 50$. 
6.4 Conclusion

We have incorporated some modifications to the extensions proposed earlier and evaluated their performance. Despite making some simplifications for the analytical model, simulation results validate the accuracy of the model. Specially for the batch scheme, the accuracy is improved greatly by considering multiple collisions. The enhancements made to the extensions have shown positive effects on the PDR for sequential schemes. The PDR stays above 90% when only 10% of the packets are event packets while deteriorating as more event packets are sent. Despite inaccuracy of the model in some cases, the model both captures the trend of the PDR drop with increased vehicle density and correctly identifies which scheme performs better. Contrary to what we have observed in Chapter 5, the batch scheme performs worst among the three schemes. However, this is not due to change in the modeling assumptions, rather due to enhancement provided for sequential schemes and a better model with multiple collision for batch scheme. For the new model differences between the PDR calculated numerically and through simulation are at most 1% and 5% respectively for $\rho = 0.1$ and $\rho = 0.5$ case compared to 10% difference observed in the previous model. For the sequential schemes the relative improvement of PDR for event safety message compared to single transmission case can reach up to 17% for medium vehicle density. This can be achieved with $m = 2$ retransmission attempts when 10% of messages are event packets but require $m = 3$ retransmission attempts for 50% event messages. Also, the PDR of the blind sequential scheme has outperformed that of the piggybacked sequential scheme indicating that the overhead outweighs the benefit of the selective retransmission. We have also shown the effect of overhead for the piggybacked sequential scheme which can be minimized with 12 bit feedback per packet.
Chapter 7

Conclusion

Several safety applications are envisioned to reduce the number of road crashes and their impact by exchanging safety messages in DSRC environment. Reliable and timely delivery of these safety messages is essential for these applications to function properly. The performance of the safety applications greatly depends on the efficient use of the shared wireless channel by the MAC protocol. The standard MAC protocol for DSRC is IEEE 802.11p DCF which is based on the standard WiFi MAC protocol. Despite success of WiFi in various scenario, the highly mobile and dynamic topology of the DSRC environment poses challenges in reliable communication due to the lack of acknowledgement and channel reservation mechanisms in broadcast communication. So, prior to deployment of the safety applications in DSRC, performance evaluation of the standard MAC protocol is required and further improvement may need to be in place.

7.1 Contributions

In this thesis, our first contribution is to evaluate the performance of the standard MAC protocol analytically and through simulation. We have developed and verified an analytical model to capture the detrimental effect of hidden terminals on the performance of the DSRC communication protocol. Insights gained from the results show that collisions due to hidden terminals is the major cause of loss of reliability in DSRC environment. This urges further research to address and resolve the effect of hidden terminals in DSRC. We have also shown that the delay is so small as not to
have any negative impact on the performance in single hop broadcast communication without any retransmission.

Then, we have proposed two MAC protocol extensions based on retransmissions to improve reliability at the cost of additional delay. The results show that, the NACK sequential scheme which requires feedback performs better than the blind sequential scheme without feedback and both schemes improve PDR for light and medium traffic loads. In high traffic loads the proposed schemes are not able to improve PDR, but in those conditions standard MAC protocol also can not meet the reliability requirement. More importantly, we show that the NACK sequential scheme can support the safety applications’ reliability requirement for up to twice the traffic load, which is a significant performance improvement.

In order to prioritize and improve the reliability of event safety messages, which have a more stringent requirement for fast and reliable delivery, two additional extensions have been proposed to retransmit only event safety packets. Another extension has also been proposed which is based on the existing piggybacked acknowledgement technique to evaluate the benefit of feedback. Contrary to the NACK sequential scheme, which carries out the feedback mechanism through out-of-band signalling, piggybacked sequential scheme suffers due to excessive feedback overhead. In addition to that, the additional complexity of piggybacked sequential scheme makes the blind sequential scheme a better alternative. For the batch scheme the PDR results were optimistic as we did not consider multiple packet collisions.

Based on the results and insights gained from them, we have incorporated some modifications to the proposed extensions as well as to the analytical model. We have observed that the sequential schemes suffer from repeat collisions despite the IEEE 802.11p backoff mechanism. As such we introduce a randomized gap between retransmissions to avoid repeat collisions. The enhancements made to the extensions have shown positive affects on the PDR for the proposed schemes. For the sequential schemes the relative improvement of PDR for event safety message compared to single transmission case can reach up to 17% for medium vehicle density. We have
also improved the accuracy of the batch scheme model by considering multiple packet collisions per batch transmission. The model is useful in capturing the trend of the PDR drop with increased vehicle density and identifying which scheme performs better.

7.2 Future Work

In the thesis, we have proposed and evaluated few extensions to standard MAC protocol based on retransmissions. However, they can be incorporated with other mechanisms to improve reliability. For instance, in Section 4.4 we have demonstrated the effect of reduced transmission range to maintain high reliability even when the traffic density is high. This suggests that adaptive transmission power based on traffic density can be useful for safety packet dissemination. Our proposed schemes can be used in conjunction with such a scheme to improve PDR even further. In addition to controlling the transmission range, the rate of routine safety messages can be changed adaptively to limit the channel load.

We have shown that the proposed schemes work well for up to three retransmission attempts. However, in certain low traffic load situations a higher number of attempts can be beneficial, whereas in high load the number of attempts can be limited to two to reduce channel load. In future, we can find the optimum point by extending the analytical model presented in the thesis. We can also improve the performance of the protocols by dynamically adapting the number of retransmissions based on the traffic load.

Adaptive selection of parameters such as transmission range, message rate, and the number of retransmission attempts require the knowledge of the traffic density. Instead, the effect of the traffic density on the channel can be estimated from other measures. For instance, a node can monitor the number of packets received over a period and the number of packets lost. The ratio of those two measures can give an estimate of the channel congestion so that the protocol parameters can be
adjusted. The total number of packets received from neighbors can be also used as an indication of vehicle density and the number of retransmission can be adjusted accordingly.

Also, PDR, the measure of reliability, was defined as the probability that all nodes receive a packet in the thesis. As this is a conservative measure, we can also investigate other measures such as fraction of nodes receiving the packet [61]. Also, the PDR measure disregards the distance between the sender and receiver. However, the safety messages are mostly relevant to the closest vehicles of the sender. As such, there is a need to devise a suitable reliability measure which depends on the distance as this will better evaluate the performance of the MAC protocol for this application.

7.3 Final Remarks

To conclude, in this thesis we have proposed some extensions to existing MAC protocol in single hop vehicle-to-vehicle network to improve reliability of DSRC communication for safety applications. Through analytical models developed in the thesis and simulation, we have shown the positive impacts of those protocols on the performance of safety message dissemination, specially they extend the range of scenarios which can support stringent reliability requirement of the DSRC protocol. As such, the proposed schemes open up exciting new possibilities for myriad safety applications envisioned to improve traffic safety and save hundreds of lives.
Bibliography


[89] Fouad A. Tobagi and Leonard Kleinrock. Packet Switching in Radio Channels: Part II–The Hidden Terminal Problem in Carrier Sense Multiple-


