Title

Ad-hoc Medium Access Control Protocol Design and Analysis for Vehicle Safety Communications

Authors

Sengupta, Raja
Xu, Qing
Mak, Tony
et al.

Publication Date

2004-09-01

CALIFORNIA PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Ad-hoc Medium Access Control Protocol Design and Analysis for Vehicle Safety Communications

Raja Sengupta, Qing Xu,
Tony Mak, Jeff Ko

California PATH Research Report
UCB-ITS-PRR-2004-34

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation; and the United States Department of Transportation, Federal Highway Administration.

Final Report for Task Order 4224

September 2004

ISSN 1055-1425

Ad-hoc Medium Access Control Protocol Design and Analysis for Vehicle Safety Communications

Final Report

PATH Task Order 4224

Raja Sengupta
Qing Xu
Tony Mak
Jeff Ko

California Partners of Advanced Transits and Highways
(PATH)
Richmond, CA94804-4603
February 2004

Abstract

This paper studies the design of ad-hoc Medium Access Control (MAC) protocols for a vehicle or the roadside to send safety messages to other vehicles. Such a protocol is needed by Advanced Vehicle Safety Systems (AVSS) and the national Dedicated Short Range Communications (DSRC) architecture. The problem is formulated to meet the communication requirements of vehicle safety applications and the DSRC multi-channel operation model. We propose several ah-hoc protocols, all based on the principles of repetition coding. Analytical bounds of the protocols' performance are derived. Simulations are conducted to compare the performance of the protocols in terms of probability of reception success and channel busy time. The best among the proposed protocols is shown to significantly outperform IEEE 802.11 MAC protocol in vehicle safety communication environment. We obtain the optimal relation between the performance and protocol design, in particular that of data rate and transmission power. The sensitivity of the protocol performance is tested under various communication conditions as well as vehicle traffic conditions. Feasible combinations of the communication and highway traffic parameters are found to meet specific performance requirements on communication.

Keywords:Vehicle Safety Communications, MAC Protocol design, Dedicated Short Range Communications (DSRC)

Contents

1 Introduction **1**

2 Previous Work **4**
2.1 Ad-hoc Random Access MAC Protocol Design and Analysis . 4
2.2 Communication requirements of Highway Safety Application . 8

3 The MAC Protocol design problem in DSRC V-V/R-V communication **11**
3.1 Probability of Reception 12
3.2 Channel Busy Time 13

4 Protocols and Analysis **15**
4.1 Description of Protocols 15
4.2 Analysis of the protocols 18
4.2.1 Probability of Reception Failure: SPR protocol 19
4.2.2 Probability of Reception Failure: APR Protocol 23

5 Numerical Results and Discussions **25**
5.1 Determining Parameters of the V-V/R-V Safety Communication Performance 25
5.2 Simulation Implementations 31
5.3 Validation of Simulation 32
5.4 Comparison of Protocols in the Nominal Setting 33
5.5 Optimal Data Rate 36
5.6 Sensitivity of AFR-CS Protocol on Design Parameters 39
5.6.1 Dependence on Communication Range and Network Topology 39
5.6.2 Sensitivity on All Parameters 40

5.7 Bursts of Reception Failures 43

6 Conclusion and future work **48**

7 Appendix **50**
7.1 Proof of Lemma 1 50
7.2 Proof of Lemma 2 51
7.3 Proof of Lemma 3 54
7.4 Proof of Lemma 5 55

List of Figures

3.1 The geo-cast concept 13

4.1 The Concept of Repetitive Transmission 17

5.1 Validation of Simulation Results with Analytical Model 32
5.2 Probability of Reception Failure for Proposed Protocols in the Nominal Setting 34
5.3 Channel Busy Time for Fixed Repetition Protocols in the Nominal Setting 35
5.4 Probability of Reception Failure for Various Data Rate Under Nominal Setting: AFR-CS Protocol 38
5.5 Performance of AFR-CS Protocol as a Function of Interference Indicator 41
5.6 Probability of Reception Failure for Various Communication Ranges: AFR-CS Protocol 43
5.7 Comparison of AFR-CS and 802.11 for Various Communication Range 44
5.8 Probability of Reception Failure for Various Message Generation Intervals: AFR-CS Protocol 44
5.9 Probability of Reception Failure for Various Packet Sizes: AFR-CS Protocol 45
5.10 Feasibility Regions for Probability of Reception Failure < 0.01 and CBT $< 50\%$ 46
5.11 Probability of message failure bursts conditioned on one message failure: AFR-CS protocol 46
5.12 Probability of message failure bursts vs. repetition number: AFR-CS Protocol, Communication Range = 240 m 47

Chapter 1

Introduction

In recent years, much effort has been made to enhance the safety and efficiency of highway/urban traffic with the aid of wireless communication techniques. Both vehicle-vehicle (V-V) communication and roadside-vehicle (R-V) communication are considered as candidate implementations of such a system. Many vehicle safety systems that use communicated information are currently being developed. Examples of such systems include: intersection decision systems (IDS) [51], cooperative adaptive cruise control (CACC) systems [46] [49] [50], and automated highway systems (AHS) [25].

Being aware of the great benefits such a communication system could bring, the FCC has recently allocated a Dedicated Short Range Communications (DSRC) spectrum of 75MHz width at 5.9GHz specifically for national ground transportation safety and productivity. DSRC provides a short to medium range communications service that supports both public safety and private operations in R-V and V-V communication environments. It is intended to provide very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important. The North America DSRC standard program was formed jointly under ASTM and IEEE to develop a set of standards that will support full interoperatability throughout North America while satisfying all of the application requirements [2].

We work on the design of an ad-hoc Medium Access Control (MAC) V-V/R-V communication protocol that is optimized for a vehicle or the roadside to send safety messages to other vehicles. Such a protocol is needed by Advanced Vehicle Safety Systems (AVSS) and the DSRC architecture. The DSRC spectrum is allocated with a mandate that it is to be used to en-

hance public safety, while supporting other transportation interests. DSRC has a multi-channel operation model where safety messages have priority on the control channel, the default channel listened to by the DSRC radio of a moving vehicle. All other non-safety related services announce themselves on the control channel and then execute the service on separate service channels. This makes reliable, un-congested operation of the control channel critical for the operation of the entire multi-channel system. The basic challenge is to develop a protocol that can meet the latency and/or reliability requirements of safety messages in a fast changing network of vehicles, while being economical enough in the utilization of the control channel for the multi-channel operation scheme to work effectively.

In this project, we propose several ah-hoc protocols, all based on the repetition coding and carrier sensing principles. Analytical bounds of the protocols' performance are derived. We conduct simulations to compare the performance of the protocols in satisfying the above-mentioned requirements. The best protocol among proposed is found to significantly outperform IEEE 802.11 MAC protocol in broadcast mode. We obtain the optimal relation between the performance and protocol design. We test the sensitivity of the protocol performance under various communication conditions and vehicle traffic conditions. Feasible combinations of the communication and highway traffic parameters are found to meet specific performance requirements on communication.

We consider *broadcast, single-hop, single channel* communications only. We assume there is no centralized control or global clock, therefore our system is ad hoc by nature. We also assume each moving vehicle is outfitted with a single omni-directional antenna and a single wireless radio that can transmit and receive, but cannot do both simultaneously. The ASTM DSRC standards committee has decided to base DSRC on 802.11a technology at 5.9 GHz. We aim to design our V-V/R-V MAC protocol to maximize compatibility with such requirements. The protocol should work within the control channel allocated by ASTM [2]. Implementation of the protocol can be accomplished by being included as part of the national DSRC standard by manufacturers of future DSRC radios or by vehicle OEM's to enhance vehicle safety based on communications. The protocol may also be installed by highway management public agents on roadside transmitters to send public safety messages.

The rest part of the report is structured as follows. Chapter 2 reviews previous work on the design and analysis of ad hoc random access MAC protocols, and on the communication requirements of highway safety applications.

Chapter 3 formulates the MAC protocol design problem in the V-V/R-V communication environment under the DSRC architecture. In Chapter 4 we propose several protocols based on repetition coding. The analysis of selected protocols is also presented in the section. Chapter 5 reports the numerical results based respectively on the analytical model and simulation under various vehicle traffic conditions and communication system parameters. Chapter 6 concludes the paper and proposes future work.

Chapter 2

Previous Work

In this chapter we review previous work on relevant topics. It can be categorized into two sets: ad-hoc random access MAC protocol design and safety application communication requirements. We review them respectively in 2.1 and 2.2.

2.1 Ad-hoc Random Access MAC Protocol Design and Analysis

Our aim is to design an ad-hoc MAC protocol. A protocol is ad-hoc when all participating radios have the same role in network control, and centralized control is unavailable. We mainly review work on MAC protocol design and touch upon some work done at the physical layer that affects the MAC layer. Since our protocol is ad hoc, we do not review literature on infrastructure-based communication systems, e.g. cellular systems. Also since we only consider one-hop communication, the vast literature on wireless routing is not discussed.

Design of an ad-hoc network poses difficult problems due to the time-variant network topology, lack of centralized control, stochastic characteristics of wireless channels, transmission power constraints, anonymity of nodes, and potentially large number of participating nodes. Difficulties exist at the network layer, MAC layer, as well as physical layer. These types of problems are of interest to both information theorists and communication engineers. The former attempt to solve Shannon-type problems for a multi-user communication channel; this field is commonly referred to as "network information

theory". The latter attack the engineering design of an actual system. Gallager presents in [22] an extensive review on the work of both sides. More results regarding network information theory can be found in corresponding chapters in [20]. A good reference on communication engineering theory and applications as well as information theory is [11], a collection of papers on multiple access in wireless networks that appeared in IEEE publications up to 1993. Historical materials on packet radio network can be found in [31].

The difficult design problems for an ad hoc network in the MAC layer exist due to hidden terminals and the absence of centralized control. Gupta and Kumar [24] describe the difficulties with options like TDMA, CDMA, and FDMA. Random access seems to be the current favorite. We will mainly review work on random access MAC protocol design.

The ALOHA system, one of the earliest random access systems, is studied in many papers such as [9] [10] and [36]. These papers contain the throughput analysis of both slotted and un-slotted Aloha protocols. In the slotted version, all nodes are synchronized to a global clock and only allowed to start transmitting at the beginning of common time slots. On the other hand, in the un-slotted Aloha protocol, nodes transmit at any instant when it has a new packet to transmit or a previously failed packet scheduled to retransmit. It is derived that the throughput of un-slotted ALOHA is $1/2e$ while that of slotted ALOHA is $1/e$. With the capture ability of the wireless radio, i.e. the radio's ability to pick up the packet with the strongest signal among multiple overlapping packets, the throughput of the system can be increased over that of the "collision model". The increase depends on the capture ratio parameter, which is the signal to interference+noise ratio (SINR) threshold required for capture. For a perfect capture case where the capture ratio is 0 dB, the throughput can reach 1. As will be described later in 4.1, both slotted and un-slotted protocols are studied in our paper, which we call synchronous and asynchronous protocols respectively. We also consider the capture ability of the radios. The capture ratio values we use are those of an off-the-shelf commercial radio product.

A simple enhancement to the ALOHA protocol is Carrier Sense Multiple Access (CSMA). The seminal analysis of CSMA protocols appear in [43]. CSMA protocols differ from Aloha by listening to the channel before transmitting, and transmitting only when the channel is sensed to be idle. The performance of a CSMA protocol is limited by the existence of hidden terminals. Hidden terminals are the nodes whose signal cannot be heard by the sender but can interfere with the packet from the sender at the receiver.

Without hidden terminals, [43] shows that it is possible for CSMA protocols to achieve a throughput of 1 provided that the propagation delay in the network is much smaller than the packet duration. We study Aloha type protocols as well as CSMA protocols. We will show the superior performance of CSMA protocols in comparison to ALOHA-type protocols.

In [44] Kleinrock and Togabi show that hidden terminals have negative impacts on the capacity of CSMA systems and can reduce it to that of pure ALOHA systems. They propose Busy Tone Multiple Access (BTMA) as a solution to the hidden terminal problem. The receiver transmits a busy tone in a separate channel whenever it is receiving a packet, making all other nodes defer their transmission when hearing a busy tone. A disadvantage of the busy tone approach is the requirement of a separate busy tone channel and the complicated radio design. Use of Request-To-Send (RTS)/Clear-To-Send (CTS) packets is an alternative approach without these difficulties. The original idea appears in [45] with SRMA (Split-channel Reservation Multiple Access), although the splitting of a channel is not necessary. MACA (Multiple Access Collision Avoidance) [27] and MACAW (MACA for Wireless LAN) [14] are examples of a RTS/CTS scheme in a single channel. In such a scheme, nodes use a three-way handshake to reduce the severity of the hidden terminal problem. The transmitter first sends a Request-To-Send packet to the receiver. The receiver replies with a Clear-To-Send packet upon successfully hearing the RTS packet. The transmitter then sends the data packet after receiving the CTS. All other nodes which hear either RTS or CTS defer transmission. RTS/CTS cannot fully solve the hidden terminal problem, partially due to the collisions of RTS/CTS packets themselves. Garcia-Luna-Aceves and Fullmer propose FAMA (Floor Acquisition Multiple Access) [23]. They prove that one of the variants, FAMA-NCS can eliminate hidden terminals by applying non-persistent CSMA when exchanging RTS/CTS packets and by properly designing the length of the RTS and CTS packets. We are primarily interested in broadcast communications, therefore a RTS/CTS approach is not directly applicable in our work. We will show that a "repetition" approach helps reduce the effect of hidden terminals.

The IEEE 802.11 MAC protocol [8] uses CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) for wireless LAN. Nodes have an option to be in RTS/CTS mode or in basic mode. RTS/CTS is not used when the data packet length is shorter than a threshold, since in this case the overhead makes the scheme inefficient. In the 802.11 MAC protocol, if nodes hear that the channel is idle for a sufficient amount of time, it transmits (data packet

or RTS) immediately. On the other hand if a node hears a busy channel, it waits until the channel is idle for a while, then back-offs for a random number of slots ranging between 1 and Contention Window (CW), a design parameter. A timer is used to count down the back-off time slots left before transmitting. The timer is suspended if the channel is sensed busy and reactivated when the channel is idle again. Whenever the timer reaches zero, the node transmits. A node doubles its CW with every failure experienced until a maximum value of CW. The CW drops back to the minimum value after one successful transmission. There are numerous analytical as well as simulation studies of 802.11 system in the literature, among them [15] [16] [19]and [42]. The results of Bianchi [15] [16] and those of Tay and Chua [42] show that the performance of the 802.11 protocol is most sensitive to the number of competing nodes in the network and the minimum Contention Window size, which is set to be 16 in the standard. They also show that basic mode is more sensitive to these parameters than RTS/CTS mode. They assume no hidden terminals in the analyses. Cali et. al. [17] [18] derive a theoretical upper bound on the throughput of the 802.11 protocol and propose a way to dynamically adjust the CW such that the upper bound can be achieved. Li, et. al. [32] study ad-hoc network capacity for a 802.11 system with ad-hoc routing using simulation and analysis methods. One main difference between all above works and ours is that they do not have delay requirements on the data. Our safety messages have a useful lifetime within which they must be delivered. Once the lifetime has expired, the message should be dropped. Therefore their results are not directly applicable.

The MAC protocol design problem for real-time applications such as multi-media communications was studied in [39]. The authors propose that real-time nodes use "Black Bursts", short bursts of high power, to contend for the channel. The length of the black burst is proportional to the delay the node experienced. Essentially all real-time nodes transmit in a round-robin manner while normal nodes transmit with best effort. The difference between their work and ours is that they attempt to guarantee successful transmission of all real-time packets within a certain delay. We on the other hand aim to achieve a high (but not 1) probability of such success for all nodes. With this change in requirements, our protocol can support a larger number of real-time nodes in the same environment.

Recently, ASTM E17.51 Committee endorsed 802.11a Roadside Application (R/A), a variant of the IEEE wireless LAN standard, as the platform of DSRC link and data link layer. Reference [52] gives a tutorial overview of

DSRC applications and assesses the characteristics of IEEE 802.11 MAC and PHY layer in this context. It is anticipated that current 802.11 specifications will need to be suitably altered to meet requirements of DSRC applications with varieties of QoS for which the original design was not intended. The article captures the current state of art of 802.11-based multiple access protocols and highlights open questions. Our work is one of the first attempts of overcoming the challenges presented in the paper.

At the physical layer, transmission power of nodes has to be high enough to reach the intended node while causing minimal interference at others. Power control in the physical layer can impact the design of the MAC layer, which is a property of wireless networks that is non-existent in wired systems. Results in [24] suggest there is a tradeoff between transmission power and the capacity. As transmission power goes up, capacity goes down. They analyze long distance transmission in a multi-hop network. Takagi and Kleinrock [41] also consider multi-hop communication, and derived the optimal number of nodes to cover in one transmission in order to balance the coverage and interference. Their objective is to minimize the time to reach the destination node without sacrificing throughput. Wu et. al. in [48] propose combining dual busy tone and RTS/CTS to avoid hidden terminal as well as exposed terminal problems in ad hoc MAC protocol design. Their solution is to transmit RTS and "transmitting busy tone" at the normal power, while transmit CTS and "receiving busy tone" at power just high enough to cover the distance, which is estimated from the signal strength of the received RTS. Our communications are local-area, broadcast, and one hop, where all above results are not directly applicable. However, we will study the impact of transmission power for given system design and network configuration in vehicle safety communication.

2.2 Communication requirements of Highway Safety Application

The primary goal of our communication protocol is to support vehicle safety applications, therefore the first step of design is to understand the communication requirements of these applications. Results on communication requirements studies provide us with the performance measures that are important to vehicle safety applications, and tell us the range of these measures

that should be supported by communication systems. The first communication requirements for safety messages sent by vehicles for vehicles were provided by Sengupta and Shladover to the ASTM DSRC committee in April 2001. Report [4] is the first comprehensive identification of the types of safety messages that might be transmitted by roadside transmitters to vehicles. Another set of communication requirements for IDS safety messages appears in [51]. The first comprehensive summary of communications for vehicle-vehicle safety messages appears in [29]. Further requirements work is ongoing under the aegis of the Vehicle Safety Communications Consortium (VSCC).

The requirements literature is inspired by the communication needs of AVSS. Some examples of AVSS are adaptive cruise control, forward collision warning systems, and lane-keeping systems [13]. These are on-board systems being designed to enhance the driver's ability to safely manage interactions with the road and neighboring vehicles. AVSS require information about the surrounding vehicles and roadway.

Therefore vehicles transmit information such as their position, velocity, or intent (e.g. abnormally stopped in the middle of the lane, changing lanes now, etc.) [29]. Roadside transmitters may send messages about events like "work zone coming up", "oil spill on the road", "advised curve speed is 35 mph", "light turning red", or "stop sign coming up" [4].

The following is an example of safety application and its communication requirements from [29].

Cooperative Collision Warning:

1. Definition

   Use vehicle-to-vehicle communication to collect surrounding vehicle locations and dynamics and warn the driver when a collision is likely.

2. Application needs

   (a) Vehicle to vehicle communication

   (b) Two-way communication

   (c) Point-to-multipoint communication

   (d) Allowable latency $\sim$ 20–200 msec

   (e) Frequency (update rate) $\sim$ 10 Hz

(f) Data to be transmitted and/or received - position, velocity, acceleration, heading, yaw-rate

(g) Range of communication $\sim$ 50–300 m

The study of vehicle safety applications' communication requirements is a developing field and many new results are expected. A highly correlated field is the design of control/estimation system with information conveyed over a wireless communication link [37] [38]. A review of these studies is beyond the scope of this paper.

Chapter 3

The MAC Protocol design problem in DSRC V-V/R-V communication

Our aim is to design a Medium Access Control protocol for V-V and R-V communications with emphasis on safety messages.

The problem of adequate performance is formulated in the following manner. There are two performance measures, i.e., *reception probability* and *channel busy time*. The performance of a protocol is adequate if its reception probability and channel busy time are acceptable for expected safety data traffic patterns in the channels allocated by the DSRC architecture. We discuss the two measures in detail in this chapter.

Our protocol is ad-hoc, i.e., there is no centralized control in the network. All vehicles and roadside transmitters play the same role. Roadside transmitters act merely as stationary nodes. Thus, the system design is kept simple and V-V communication can penetrate the market without being crucially dependent on the penetration of a roadside infrastructure. This will facilitate deployment.

Since each node in our vehicle communication network represents an onboard radio of a vehicle, in our discussion below we use words "vehicle" and "node" interchangeably. The meaning should be clear from the context.

3.1 Probability of Reception

Reception with a specified probability has the following meaning. Each message has a *intended range* and *useful lifetime* associated with it. Our performance requirement is that vehicles within the specified range receive the message within its specified lifetime with a specified probability. For example if the range is 100 meters, the useful lifetime is 50 msec, and reception probability is 0.999, then each vehicle within 100 meters of the sending vehicle should receive the message within 50 msec with probability 0.999. The motivation for such a performance definition is because each safety-related message has a lifetime in which it is useful to the receiving vehicles. Typically, at the end of the lifetime the next message (e.g. new position or velocity update) becomes available for transmission. At this point it is better to stop retransmitting the old message and transmit the new one. The platoon network [12] [30] [38], IDS network [4] [51] are designed not to retransmit obsolete messages even if they have not been received.

By requiring the high probability reception at all vehicles within a range associated with the message, we actually assume the safety applications are implemented on top of geographic multi-cast, or *geo-cast* [28]. Our MAC protocol is designed to support geo-cast at higher layers. In geo-cast, the set of targeted receivers is specified as a geographic region relative to the transmitter (see Figure 3.1). The geographic region is called the geo-cast zone of the message. A sender broadcasts messages to all the receivers in its communication range. It is the receiver's responsibility to determine if it is in the geo-cast zone, and thus the relevance of the message and the proper response. The decision is made on the basis of the relative position of the sender (e.g. in front, behind, left lane, distance, etc.), the content of the message (e.g. brake warning, lane change warning, accident reporting, congestion obesrvation/prediction, etc.), as well as the highway traffic environment. To use geo-cast, wireless communication techniques must be integrated with other techniques such as Global Positioning System, Inertial Navigation System, digital map, radar/lidar, and sensor fusion.

Though our MAC protocol is not designed for a unicast system, the results obtained here are still relevant. The realization of any unicast V-V/R-V communication requires the assistance of geo-cast. In unicast communication, Location Based Addressing is needed to build (in all involved vehicles) the map between the physical location of neighboring vehicles and their communication addresses. This map basically answers the question "What is the

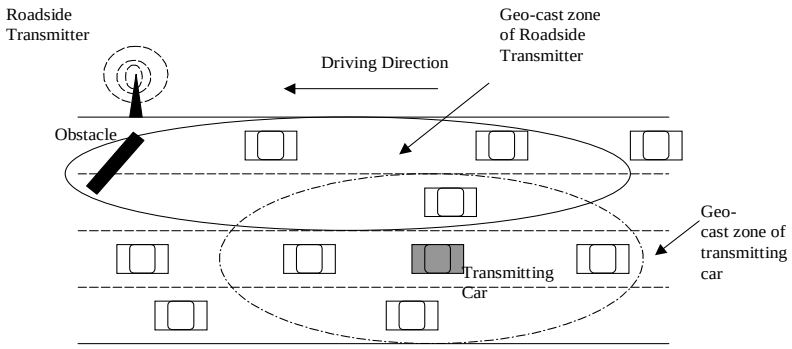

Figure 3.1: The geo-cast concept

communication address(es) of the vehicle(s) at given position(s)?". Geo-cast is critical in the establishment and update of this map, since unicast is unavailable in these processes.

3.2 Channel Busy Time

Channel busy time (CBT) is an important performance measure when operating in the DSRC control channel. We define CBT as the fraction of time that the channel is occupied by either a successful packet or collided packets within a specific region. CBT represents the fraction of time when the channel cannot be used by other non-safety applications.

DSRC would support critical safety application, such as vehicle collision avoidance, as well as other valuable non-safety related ITS applications, such as Electronic Toll Collecting (ETC), digital map update, etc. The versatility of DSRC greatly enhances the likelihood of its deployment by various industries and adaptation by the consumers. DSRC achieves its versatility by introducing an explicit multi-channel operation model. Safety messages, whether from other vehicles or infrastructure devices on the roadside, are sent in the control channel and monitored by all vehicles. In the meantime, a licensed roadside unit could use the control channel to inform approaching vehicles of its services (often non-safety applications) and conduct the actual application in one of several service channels. For example, a roadside unit could announce a local digital map update in the control channel and transfer this data to interested vehicles in a service channel. Therefore congestion in

the control channel would endanger the safety of the relevant vehicles depending on the safety applications; at the same time, it would also jeopardize the operation of all service channels and, thus, disrupt the whole multi-channel architecture. Our protocol should use the control channel economically.

Besides these two performance measures, we are also interested in the probability of a burst of message failures. Not only do we require the probability of message reception failure to be low, we also require that large number of consecutive failures (bursts) not be likely. In safety applications such as neighborhood map building and cooperative collision warning, updates of the state of neighboring vehicles must be received in a periodic sense. Bursts of missing messages more severely degrades a vehicle's estimation of its neighborhood than failures evenly distributed in time. Our MAC protocol should not cause bursts of failures. However, notice that the wireless V-V/R-V communication channel's slow fading could also cause this problem. In this paper we only study the impact of MAC design on the production of bursty data loss. Statistical study of the characteristics of V-V/R-V communication channel is an on-going work [1].

Chapter 4

Protocols and Analysis

We describe the proposed protocols in 4.1. The analysis of selected protocols are reported in 4.2.

4.1 Description of Protocols

We make the following assumptions in the design of the protocols.

- Vehicle safety applications generate a message to be transmitted to other vehicles when an event (e.g. on-board sensor measurement update, hard braking, emergency) occurs. We denote the useful lifetime as τ. The message is passed down to the MAC layer. The MAC protocol attempts to transmit the packet only within the message's lifetime and discards the packet when the message expires.

- The information in the *message* is encapsulated in a *packet* to be transmitted to other vehicles. The size of packets is time invariant and is the same across nodes. The packet could contain the location of the sender, the targeted vehicle's location (e.g. the first following vehicle, all vehicles in the adjacent lane), the nature of the event (e.g. hard braking, accident, severe road condition), etc. The time taken to transmit one packet is a function of the packet size and the data rate of the radio. We denote this time period as t_{trans}.

- Channel fading is neglected. The signal power attenuation is determined by the path loss only. Therefore every packet transmitted in the

communication range without collision is received successfully. And the potential interferers are within the interference range of the receiver.

We will discuss later in 5.1 the parameters that influence the performance of the protocol and their possible values. One fact is that generally τ is much larger than t_{trans}, hence a node could repetitively transmit the packet many times in the useful lifetime of the message. By definition the vehicle traffic environment does not change dramatically within the useful lifetime (otherwise the message cannot be useful any more), therefore the successful reception of any one of the repeated packets at any time within the lifetime is considered as the success of the message. This observation motivates us to consider repetition protocols.

Figure 4.1 is a illustration of the repetition idea. Two transmitters within interference range of one receiver have messages generated at same time, and the protocol commands them to randomly choose multiple slots to repetitively transmit a packet in each. If any one or more *packets* are received without being collided, the *message* is received by the targeted receiver, and the delay is smaller than the useful lifetime of the message. On the other hand, the message transmission fails if all of its transmitted packets are lost due to collisions. Both vehicles in Figure 4.1 succeed if there are no other interfering vehicles.

The whole lifetime is evenly divided into $n = \lfloor \frac{\tau}{t_{trans}} \rfloor$ slots, where $\lfloor x \rfloor$ is the maximum integer not greater than x. The fraction of τ that is not used is quite small since in general $\tau \gg t_{trans}$ (See discussions in 5.1). We can randomly pick any 1 to n slots to transmit the packets. We only study homogeneous systems, assuming all nodes repeat the packet for k times. Intuitively, repetition increases the probability for at least one packet to get through. However excessive repetitions add burden to the channel and degrade the performance, as we will see later in analytical and simulation results. Therefore the optimal number of transmissions k_{opt} must be found.

Based on the random repetition idea, we have two classes of repetition protocols, "fixed repetition" and "p-persistent repetition" protocols. They each correspond to a way to perform repetition in packet transmission. In addition to the repetition, we have two other ways to further enhance the performance of the protocol. The first is synchronizing the transmission of all vehicles to a global clock such that transmissions start only at the beginning of a common slot. The idea is the same as in slotted ALOHA [36]. The other is carrier sensing before the transmission of each repeated packet. The well

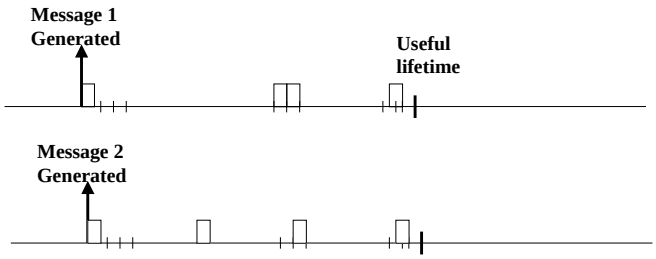

Figure 4.1: The Concept of Repetitive Transmission

known idea is the same as in CSMA [43]. With the combination of these options, we have the following six protocols.

1. *Asynchronous Fixed Repetition (AFR)*

   In AFR, as well as all other fixed repetition protocols, the design parameter is the number of repetition k. The protocol randomly in uniform selects k distinct slots among the total n slots in the lifetime. The protocol is so called since the repetition number is fixed. The radio does not listen to the channel before it sends a packet with AFR.

2. *Asynchronous P-persistent Repetition (APR)*

   P-persistent repetition protocol determines whether to transmit a packet in each of n slots in lifetime by flipping an independent unfair coin with $P(H) = \frac{k}{n}$ and $P(T) = 1 - \frac{k}{n}$. A packet is transmitted if the result is head, where positive integer $k \leq n$ is the design parameter of the protocol. We can see that in average there are k transmissions (repetitions+1) in the lifetime of a message; however, for each realization the exact number of repetitions varies. Later we compare the performance of p-persistent protocol, with average number of transmissions k, to that of corresponding fixed repetition protocols, with constant k transmissions. The relation between the two classes of protocols is analogous to that of standard 802.11 and p-persistent 802.11 proposed in [17]. The reason to introduce p-persistent protocols is because they are mathematically tractable [17]. Like with AFR, the radio does not listen to the channel before it sends a packet.

3. *Synchronous Fixed Repetition (SFR)*

This protocol is the same as AFR except that all the nodes are synchronized to a global clock as in slotted ALOHA, and all message generations as well as transmissions happen at the beginning of a slot. With this protocol, partial overlapping between packets is avoided. However, the synchronization may be hard to realize.

4. *Synchronous P-persistent Repetition (SPR)*

   The SPR protocol is the same as APR protocol except for the synchronization of message generations and transmissions from different nodes.

5. *Asynchronous Fixed Repetition with Carrier Sensing(AFR-CS)*

   In AFR-CS, we partition the lifetime with larger time slots called *extended slots*. Each extended slot is composed of a contention period followed by a packet transmission period. The contention period is the sum of propagation delay, transmission/reception turnaround time, and other processing delay. The length of packet transmission period is the packet duration. Like in AFR, The protocol selects randomly in uniform k extended slots to transmit. The difference is that in each selected slot, the radio first listens to the channel during the contention period. If the channel is idle, a packet is transmitted afterwards, otherwise the slot will be discarded.

6. *Asynchronous P-persistent Repetition with Carrier Sensing (APR-CS)*

   It is similar to AFR-CS except that the extended slots are selected in the p-persistent manner.

Our protocols are essentially based on repetition coding. More efficient coding scheme such as erasure coding [47] will improve the communication quality at the cost of more complex coding/decoding computation at both the transmitter and the receiver.

4.2 Analysis of the protocols

In this section we present analysis of two of the protocols we proposed: SPR and APR. We use these analytical results to validate our simulation results, and to obtain insights into the design of all of the proposed repetition protocols.

We make the following two assumptions in our analysis.

- The message generation process of each individual vehicle is a Poisson process.
- The message generation processes of different vehicles are identically independent.

With these two assumptions, we know immediately that the generation process of all interfering messages is also Poisson with the rate equal to the sum of the rates of all interferers. Assume that the rate of the Poisson process for each node is λ and the number of interfering nodes is m, then the rate of message generation process of all these nodes is $m \cdot \lambda$. Actually, the above assumptions can be replaced by the following weaker assumption, which does not require independence of messages generations among vehicles.

- The aggregate message generation process of any (reasonably large) number of vehicles is Poisson with rate proportional to the vehicle number.

We present only homogeneous analysis here. As stated above, the protocol design is the same for all the transmitters, and all packets of all transmitters are of the same size. Furthermore, all nodes apply the same transmission power to all packets, hence the communication ranges of all packets are the same.

The notations listed in Table 4.1 are used in the mathematical analysis.

We present analytical results in terms of probability of reception failure (PRF), which can be easily interpreted to equivalent results regarding reception success. We show the results of SPR protocol in subsection 4.2.1, and those of APR protocol in subsection 4.2.2. The main results are in Theorems 7 and 8 respectively, which give tight upper and lower bounds of the PRF of one message at one particular receiver.

4.2.1 Probability of Reception Failure: SPR protocol

We prove the main result, Theorem 7, utilizing a series of lemmas. The lemmas and main theorem are listed below. The proof of the main theorem is presented in this section, while proofs of lemmas are in the appendix.

Lemmas 1- 2 lower bounds PRF.

Table 4.1: Notations in Protocol Analysis

n	Maximum possible number of repetitions in lifetime, total slots number
k	Average number of repetitions for a message
S_j	Event that the jth repetition is successful
S	Event that at least one of the repetitions succeeds
p_j	The jth repeated packet sent by a transmitter for a message
t_j	The instant that the jth repetition starts
τ	Useful lifetime of a message
T_j	Event that there is at least one interfering message generated in $(t_j - \tau, t_j]$
λ	The rate of message generation of each individual node
m	Total number of interfering nodes around a receiver

Lemma 1. ***The Probability of Reception Failure for One Single Packet in SPR***

Let a packet p_j be the j^{th} repeated packet sent by one transmitter. Then the probability of reception failure of p_j by any a receiver with m interferers obeys the following equation

$$P(\neg S_j) = 1 - e^{-m\lambda\tau\frac{k}{n}}, \forall 1 \leq j \leq k \leq n \tag{4.1}$$

Proof. See Appendix 7.1 □

Lemma 2. ***Lower Bound of the Probability of Reception Failure for Multiple Packets in SPR***

Suppose p_1,p_2,...,p_r are any r repeated packets sent for one message, then the probability of failure of all of them at a receiver with m interferers is greater than the product of the probability of failure of each one of them. Formally,

$$P(\neg S_1 \wedge \ldots \wedge \neg S_r) > \prod_{j=1}^{r} P(\neg S_j) = (1 - e^{-m\lambda\tau\frac{k}{n}})^r, \forall 1 \leq r \leq k \leq n \tag{4.2}$$

Proof. See Appendix 7.2 □

Lemmas 3- 6 provide the upper bound of the probability of reception failure, which comes out to be quite close to the lower bound.

Lemma 3. *The probability of failure of a single packet p_j at a receiver with m interferers, conditioned on the event that there is at least one interfering message generated in $(t_j - \tau, t_j]$, obeys the following equation.*

$$P(\neg S_j|T_j) = 1 - e^{-m\lambda\tau\frac{k}{n}} + e^{-m\lambda\tau}, \forall 1 \leq j \leq k \leq n$$

Proof. See Appendix 7.3 □

From lemmas 1 and 3 we can easily see the following.

Corollary 4. *1.*

$$P(\neg S_j) < P(\neg S_j|T_j)$$

.

2. When the total interfering transmission rate is high, i.e. $m\lambda \gg 1$,

$$P(\neg S_j) \approx P(\neg S_j|T_j)$$

.

Lemma 5.

$$P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) < P(\neg S_r|T_r) \tag{4.3}$$

where T_r is the event that there is at least one interfering message generated in $(t_r - \tau, t_r]$, $\forall 1 \leq r \leq k \leq n$.

Proof. See Appendix 7.4 □

Lemma 6. ***Upper-Bound of Probability of Reception Failure for Multiple Packets in SPR***

$$P(\neg S_1 \wedge \ldots \wedge \neg S_r) < \prod_{j=1}^{r} P(\neg S_j|T_j) = (1 - e^{-m\lambda\tau\frac{k}{n}} + e^{-m\lambda\tau})^r, \forall 1 \leq r \leq k \leq n \tag{4.4}$$

Proof. The inequality is obvious from chain rule and lemmas 3 and 5. □

Combining the bounds provided by Lemmas 2 and 6, we can now prove the main theorem.

Theorem 7. ***Bounds on the Probability of Reception Failure for One Message in SPR***

The probability of reception failure of one message at a receiver with m interferers satisfies the following inequality.

$$\left(1-\frac{k}{n}e^{-m\lambda\tau\frac{k}{n}}\right)^n < P(\neg S) < \left(1-\frac{k}{n}e^{-m\lambda\tau\frac{k}{n}}+\frac{k}{n}e^{-m\lambda\tau}\right)^n \tag{4.5}$$

Proof. Let random variable K be the total number of packets transmitted for one message. From lemmas 2 and 6, the probability of success for the message conditional on $K = r$ satisfies the following inequality.

$$(1-e^{-m\lambda\tau\frac{k}{n}})^r < P(\neg S|K=r) = P(\neg S_1 \wedge \ldots \wedge \neg S_r) < (1-e^{-m\lambda\tau\frac{k}{n}}+e^{-\lambda\tau})^r \tag{4.6}$$

Now let p and q be defined as in equations 4.7 and 4.8 respectively.

$$p = (1-e^{-m\lambda\tau\frac{k}{n}}+e^{-m\lambda\tau}) \tag{4.7}$$

$$q = (1-e^{-m\lambda\tau\frac{k}{n}}) \tag{4.8}$$

Then equation 4.6 becomes

$$q^r < P(\neg S|K=r) < p^r$$

We show below the proof of the left-hand side of the inequality 4.5 for simplicity of presentation. The proof of right-hand side follows the exact steps except for the changing of direction of inequality and replacing q with p.

$$
\begin{aligned}
P(\neg S) &= \sum_{r=0}^{n} P(\neg S|K=r)P(K=r) \\
&> \sum_{r=0}^{n} q^r P(K=r) \\
&= \sum_{r=0}^{n} q^r \binom{n}{r} \left(\frac{k}{n}\right)^r \left(1-\frac{k}{n}\right)^{n-r} \\
&= \sum_{r=0}^{n} \binom{n}{r} \left(q\frac{k}{n}\right)^r \left(1-\frac{k}{n}\right)^{n-r} \\
&= \left(1-\frac{k}{n}+q\frac{k}{n}\right)^n \\
&= \left(1-\frac{k}{n}e^{-m\lambda\tau\frac{k}{n}}\right)^n
\end{aligned}
$$

In above proof $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. We applied Binomial Theorem in the proof. We can prove the LHS of inequality in exactly the same way, therefore the theorem is proved.

□

4.2.2 Probability of Reception Failure: APR Protocol

The analysis for APR protocol is similar to that of the SPR protocol. In APR, if a packet is transmitted at time t, any interfering packets transmitted in the interval $[t - t_{trans}, t + t_{trans})$ can collide with it, i.e. the transmitted packet is vulnerable in two slots in contrast to one as in SPR. Remember that t_{trans} is the time duration of a packet. Therefore for this packet to be successful we require none of the interferers transmits in the two-slot interval. We have similar series of lemmas as listed in subsection 4.2.1. To save space we only present the main result in the following theorem.

Theorem 8. ***Bounds on the Probability of Reception Failure for One Message in APR***

The probability of reception failure of one message at a receiver with m

interferers satisfies the following inequality.

$$\left(1-\frac{k}{n}e^{-m\lambda\tau\left[2\frac{k}{n}-\frac{k^2}{n^2}\right]}\right)^n < P(\neg S) < \left(1-\frac{k}{n}e^{-m\lambda\tau\left[2\frac{k}{n}-\frac{k^2}{n^2}\right]}+\frac{k}{n}e^{-m\lambda\tau}\right)^n \tag{4.9}$$

The bounds of reception probability as shown in Theorems 7 and 8 are quite tight when the interfering vehicle number is large, which is true for all the cases we study. Thus we can use one of the bounds to represent the real value of the probability of reception failure.

Once we know the PRF for a particular vehicle with m interferers and the spatial distribution of the nodes, the PRF of all the vehicles within the communication range of a safety message can be calculated. Let's consider a simplified one-lane case. Let the intended communication range be R. Let r denote the distance between the transmitter and the receiver, which takes values in $(0, R]$. The linear vehicle density of the lane is $\rho(r)$ vehicles/meter, a function of r. As indicated in Theorems 7 and 8, the PRF of a potential receiver is a function of the number of interferers $m(r)$, also a function of r. As we will discuss later, $m(r)$ can be a linearly increasing function of r if the vehicle density is invariant in r. The probability of reception failure for all the vehicles within the communication zone of the safety message can then be calculated with the following equation.

$$PRF_{msg} = \frac{\int_0^R PRF(m(r))\rho(r)dr}{\int_0^R \rho(r)dr} \tag{4.10}$$

The actual calculation is more complicated, since vehicles' spatial distribution is discrete rather than continuous. When there are multiple lanes, care must be taken to the edge effects, i.e. vehicles on border of the road in general experience less interference than those in the center lanes. But essentially we apply variants of equation 4.10 to calculate the probability of reception failure of messages, both analytically and in simulations.

Chapter 5

Numerical Results and Discussions

In this chapter we present and discuss numerical results of the performance of the protocols. We first discuss in 5.1 the parameters that influence the protocol performance in vehicle safety communications. The implementations of the simulations are presented in 5.2. In section 5.3 we validate the simulation with analytical results. We compare the performance of all the candidate protocols in the nominal setting in 5.4. Among them, the AFR-CS protocol is found to best meet the communication requirements of vehicle safety applications. We discuss our finding of an optimal transmission data rate in 5.5. We discuss in 5.6 the sensitivity of the performance of the AFR-CS protocol on design parameters. Finally we show the performance of the protocol on generating message failure bursts in 5.7.

5.1 Determining Parameters of the V-V/R-V Safety Communication Performance

The performance of V-V/R-V safety communication protocol is determined by many factors. It depends on how many resources (e.g. channel utilization) each competing node consumes, and how many such nodes are competing with a particular transmitting node. The former is determined by the vehicle safety application while the latter can be derived from the topology of the highway network and the vehicle traffic conditions. Specifically, the parameters determining the performance of our MAC protocol are the

following:

1. *Message Generation Rate/Interval*

   They parameterize the frequency at which a safety communication message is generated. The message generation rate is the reciprocal of message generation interval. Generally a safety message is generated once every a few hundred milliseconds. This is due to the highly dynamic property of highway traffic, and the task of vehicle safety communication to provide vehicles with the most recent information about traffic environment.

2. *Packet Size*

   For vehicle safety applications the packet size is generally on the order of a few hundred bytes [2]. In most cases the information that needs to be transmitted is: vehicle position, velocity, acceleration, yaw rate, intents, etc. All of these could be represented by a few real numbers. We assume the size of packets is time-invariant and is the same across nodes. Although the packet is small, its size impacts the performance of the protocol due to the potentially large number of interfering vehicles and the high message generation rate.

3. *Data Rate*

   The data rate (or channel bit rate) together with the packet size determines the time taken to transmit one packet. The data rate values we use here are those specified in the 802.11a physical layer standard [8]. The DSRC draft standard gives a radio the options to use a 20MHz wide channel or a 10MHz wide channel. The purpose of the latter option is to reduce the inter-symbol interference when necessary. We assume channel width to be 20MHz in this paper, the same as in the 802.11a physical layer standard. If a 10MHz channel is used, the data rates will be half of the corresponding values in 802.11. Considering the message lifetime and packet size discussed above, we can see that there could be many repetitions of a packet in the useful lifetime of a message. The message useful lifetime is in the order of hundreds of milliseconds, while the packet duration is in the order of hundreds of micro-seconds. We generally have hundreds of slots (maximum possible repetitions) in a useful lifetime.

4. *Desired Communication Range*

   This is the range a vehicle intends to transmit its safety message to. Given other conditions, it determines the transmission power and therefore interference range. We use omni-directional antennae and deterministic path-loss channel model in this paper, therefore the communication zone of a transmitter is a circle centered at the position of its antenna with the communication range as radius. Similarly, the interference zone of a receiver is a circle centered at the position of its antenna, but with the interference range being the radius. We do not consider cumulative interference in our simulation, hence only the nodes within the interfering range of the receiver can potentially interfere.

   In our simulation, we use the Friis free-space channel model for short TX/RX distances and the Two-ray model for long distances. The channel model is switched at the TX/RX distance when the two model give the same reception power for same transmission power. We implement the model of Atheros' 802.11a radio [7]. The reception SINR thresholds of this radio model at all data rates supported in IEEE 802.11a physical layer standard are listed in Table 5.1. The thermal noise floor is at -96 dBm when channel width is 20 MHz.

   The procedure to calculate transmission power P_t of a message to reach a intended communication range R at a given data rate is the following.

   (a) Find the SINR threshold β corresponding to the data rate in Table 5.1.

   (b) The ratio between the reception power P_r and thermal noise is β in dB. Reception power P_r is obtained.

   (c) Use the path-loss channel model, P_r, and R to calculate P_t.

   Given the transmission power P_t, the TX/RX distance $r \leq R$, and the data rate, the procedure to calculate the interference range r_i of the receiver is the following.

   (a) Find the SINR threshold β corresponding to the data rate in Table 5.1.

   (b) Use the channel model, P_t, and r to calculate the power of the signal, P_r, at the receiver.

(c) The ratio between P_r and the interference power P_i is β in dB.

(d) Use the channel model, P_t, and P_i to calculate r_i. All nodes closer than r_i from the receiver can potentially interfere.

The interference range depends on the TX/RX distance. If free-space channel model is used, we have the following relation.

$$r_i = 10^{\frac{\beta}{2}} \cdot r \tag{5.1}$$

Hence, the interference range of a receiver is a linearly increasing function of its distance to the transmitter. When the density of vehicles is unchanged in space, then the average number of interferers around this receiver is also a linearly increasing function of its distance to the transmitter.

The followings are obvious from Equation 5.1 and Table 5.1:

- r_i is proportional to r. The further away the receiver is from the transmitter, the more vulnerable it is to interference. The worst case is when r is equal to the communication range R, i.e., the furthest it can be that we are still interested in.
- r_i is greater than r for all the data rates supported in 802.11a.
- The higher the data rate the larger the ratio between r_i and r, i.e. the message is more vulnerable to interference for higher data rate.
- At the lowest data rate, 6 Mbps, $r_i = 2r$.

When TX/RX distance is large (> 150m), Two-ray model is used to calculate interference range. The relation between TX/RX distance and the interference range is then more complicated than in equation 5.1, but the above observations hold except for the last one.

Finally, in our simulation we transmit packets at slightly higher power than needed to cover the communication range. This is to ensure that vehicles driving at the edge of communication zone can receive the message.

5. *Vehicle Density/Distance*

Table 5.1: SINR Thresholds for 802.11-supported Data Rate in Simulated Radio Model

Data Rate (Mbps)	Reception SINR Threshold (dB)
6	6
9	8
12	9
18	11
24	14
36	18
48	23
54	25

The vehicle density is the reciprocal of the distance between two neighboring vehicles in the same lane. Once we know the density, the lane number, and the interference range we could calculate the total number of interfering vehicles for an individual vehicle. In mathematical analysis we assume homogeneous traffic in which all the vehicles have equal and time-invariant distance from its neighboring vehicles in the same lane. Whereas in simulations we set the simulation parameters such that the average vehicle distance equals our desired value.

6. *Lane Number*

   The lane number influences the number of interfering vehicles in the interference zone. We only consider a straight-lane highway without overpasses in this paper. The lane width we use is 3.6 meters from California Highway Design Manual [33].

Table 5.2 lists the parameters of the "nominal setting" of our simulations as well as analysis. This setting reflects the typical situation for vehicle safety communication and is of most interest to us. Throughout Chapter 5, without explicit specification, the parameters of a simulation take the values in Table 5.2 by default. We study the sensitivity of the protocols with broader range of the parameters in Section 5.6. Table 5.3 summarizes the range of parameter values we study. These parameters come from literature on the communication requirement of vehicle safety applications as discussed in 2.2.

Table 5.2: Nominal Setting Parameters

Message Generation Interval (msec)	100
Useful Life Time (msec)	100
Packet Payload Size (Bytes)	100
Desired Communication Range (m)	80
Average Distance Between Vehicles (m)	30
Lane Number	4

Table 5.3: Range of Parameters Studied

Message Generation Interval (msec)	50, 100, 200	
Packet Payload Size (Bytes)	100, 250, 400	
Data Rate (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	
Average Distance Between Vehicles (m)	10 (jammed)	30 (smooth)
Desired Communication Range(m)	10-100	30-300
Lane Number	4, 8	

Table 5.4: Other Simulation Parameters

MAC header	24 Bytes
FCS	4 Bytes
PLCP header + tail	46 Bytes
Preamble Duration	16 μs
Antenna Gain	4 dB
Channel Frequency	5.9 GHz
Channel Width	20 MHz
Thermal Noise Level	-96 dBm
Antenna Height	1.5 m

5.2 Simulation Implementations

We implement our simulation with NS [6] and SHIFT [34].

We use NS (Network Simulator) to simulate a wireless communication network. NS is a discrete event simulator targeted at networking research. It is a free, open source software downloadable from the Internet [6], with most popular protocols implemented in various OSI layers. We use the wireless extension of NS developed by the Monarch project [5]. We implement our protocols on top of 802.11 MAC in broadcast mode. We change the physical layer settings such that the simulated communication takes place in 5.9 GHz DSRC channel rather than the original 2.4 GHz 802.11b channel. Besides the parameters already discussed in 5.1, parameters in Table 5.4 are used in implementations, which are common to all settings listed in Table 5.3. Whenever applicable they are set according to the IEEE 802.11a standard on physical and MAC layers.

We use SHIFT to simulate highway vehicle traffic. SHIFT is a programming language developed by California PATH for simulating dynamic networks of hybrid automata, in particular the vehicle traffic system. It is open-source and can be downloaded from the Internet. We implemented microscopic models for merging, lane changing, gap acceptance, vehicle following, etc. The detailed description of the vehicle traffic simulation is in [46]. We use COSMODRIVE [40] cognitive model for human driver modelling which includes the Hoffmann model of range-rate perception [26].

We first simulate the vehicle traffic with SHIFT, then feed the generated

trace file as the "node movement file" to the wireless communication simulation of NS. In the future it is possible to extend our "piped" simulation by implementing vehicle safety applications and feeding back the output of the V-V communication simulation to the vehicle traffic simulation. The simulation system then will become a closed-loop system, with the vehicle traffic component and wireless communication component influencing each other and vehicle safety application being the bridge between them.

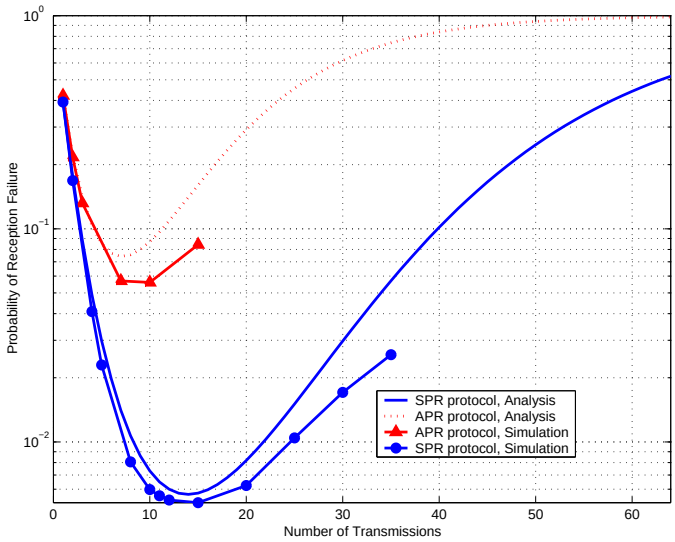

Figure 5.1: Validation of Simulation Results with Analytical Model

5.3 Validation of Simulation

Figure 5.1 shows the analytical and simulated probability of reception failure (PRF) of APR and SPR protocols in the nominal setting summarized in Table 5.2. The analytical results come from equations 4.5, 4.9, and 4.10. The channel data rate is 6 Mbps, the lowest supported data rate in 802.11a. For both APR and SPR, the upper and lower bounds are too close to be distinguished, thus we only plot one of them as the true value of PRF. The analytical and simulation results match well. In both analysis and simulation results, we see there is an optimal average number of repetitions (or equivalently, probability of persistence in each slot) for both of the protocols.

Repetitively transmitting packets beyond this number will congest the channel and degrade the performance of the protocol. This observation confirms our prediction in 4.2. The optimal number of transmissions, k_{opt}, is 15 for SPR protocol (or optimal probability of persistence is $15 \cdot \lfloor \frac{t_{trans}}{\tau} \rfloor$), and 7 for APR (or optimal probability of persistence is $7 \cdot \lfloor \frac{t_{trans}}{\tau} \rfloor$). Not surprisingly, since synchronous protocol eliminates the partial overlap between packets from different nodes, SPR's performance is superior to that of APR. This observation agrees with the previous results on the slotted and non-slotted ALOHA [36]. The relatively good match validates the simulation model we implement.

5.4 Comparison of Protocols in the Nominal Setting

Figure 5.2 shows the PRF of all proposed protocols in the nominal setting. The solid black horizontal line in the middle represents the simulation result of 802.11 broadcast mode in the same setting for comparison. Clearly, for the same repetition methods (i.e. fixed repetition or p-persistent repetition), synchronous protocol outperforms asynchronous protocol, identical to what we have observed and explained in Figure 5.1. Also it is obvious that for the same repetition method, a CSMA protocol is better than a non-CSMA protocol. This result is expected since in CSMA each node listens before transmission, therefore many potential collisions are avoided. The reception failures for CSMA protocols are mostly due to hidden terminals. Fixed repetition protocols outperform corresponding p-persistent protocols. The reason is that the fixed repetition protocols are better at maintaining the number of repetitions for each message, i.e. there is less fluctuation between the actual number of repetition of each message and the expected number of repetitions.

As we will discuss in the next subsection, there is an optimal data rate for each protocol under a given set of parameters. In Figure 5.2 all of the protocols are simulated with their respective optimal data rate under the nominal setting.

Among the six candidate protocols, four yield lower probability of reception failure than 802.11. The best two are AFR-CS and SFR. They both achieve minimum (or asymptotic) probability of failure of 0.0004, which is one order of magnitude lower than that of 802.11. This shows that repetition

helps combat interference by giving a transmitter more chances to transmit, and making interfering nodes transmit at different time. The better performance of the AFR-CS protocol over that of 802.11 indicates that repetition reduces the hidden terminal effects without using RTS/CTS. Synchronizing the transmissions among nodes and adding CSMA to the protocol bring about the same level of benefit. However, it is in general much easier for the radios to listen to the channel before transmitting than synchronizing all the transmissions of all nodes to a global clock. Therefore we prefer AFR-CS to SFR for deployment simplicity. In Figure 5.2, the PRF of AFR-CS keeps decreasing with number of transmissions. However, the PRF shown in the plot already levels off. In another test, we keep increasing the number of repetitions and observe that the PRF of the AFR-CS protocol does increase as observed in other protocols, though at very large repetition numbers. The result is not shown here to save space. This observation together with the CBT results to be discussed below indicate that we should not blindly repeat large number of packets in the AFR-CS protocol in order to obtain good performance.

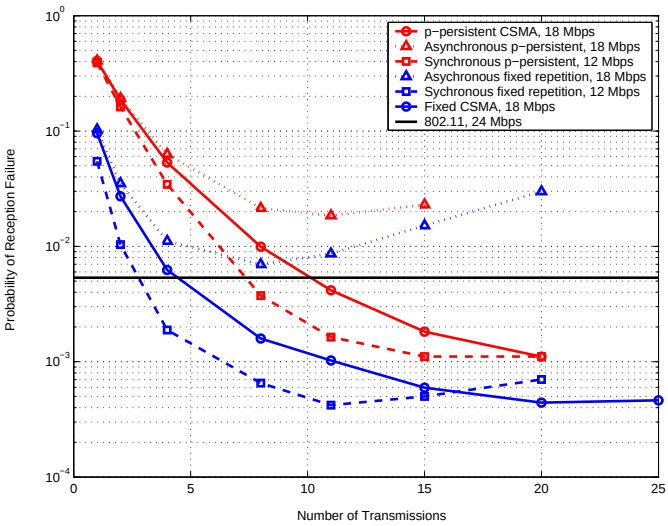

Figure 5.2: Probability of Reception Failure for Proposed Protocols in the Nominal Setting

Figure 5.3 shows the CBT of the three fixed repetition protocols and 802.11 under the nominal setting. Results for p-persistent protocols turn out to be quite close to those of corresponding fixed-repetition protocols. By this

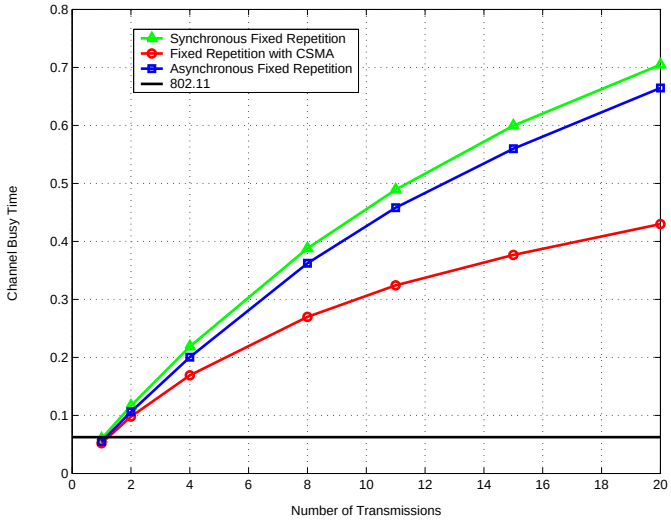

Figure 5.3: Channel Busy Time for Fixed Repetition Protocols in the Nominal Setting

we mean with the same number of repetitions, APR and AFR yield about equal CBT. The same relation holds between SPR and SFR, and between APR-CS and AFR-CS. For clarity we do not show the CBT of p-persistent protocols in Figure 5.3. As we expected, the CBT increases with the number of repetitions. Neglecting the collisions between packets, the CBT can be estimated with the following equation.

$$CBT \sim m \cdot \lambda \cdot k \cdot t_{trans} \tag{5.2}$$

where as defined above m is the total number of nodes within the interference range of a receiver, λ is the message generation rate of each node, k is the average number of transmitted packets for each message, and t_{trans} is the time taken to transmit one packet.

Obviously, equation 5.2 is merely the sum of the transmission time of all packets from all interfering nodes in one second in average, assuming none of them collide with another. It is a upper-bound of the real CBT. In the equation, the estimated CBT increases linearly with the number of repetitions. But as repetition increases, packets have more chances to collide, occupying less channel time than when they are completely separated. Therefore the actual CBT is a sub-linear function of repetition number below the bound

indicated in equation 5.2. Among the candidate protocols, AFR-CS has the lowest CBT at the same number of repetitions. With this protocol, less than half of channel time is occupied by vehicle safety applications, leaving time for non-safety communications, such as announcements for services in other channels. Since there is no repetitions in 802.11 MAC protocol, its CBT is much lower than repetition protocols as expected. Combining the observations of Figures 5.2 and 5.3, we conclude that in the nominal setting AFR-CS is the best protocol among simulated. It produces probability of reception failure as low as 0.0004 while occupying the channel for less than 44% of time. We conduct further analysis of this protocol in the later part of the paper.

5.5 Optimal Data Rate

IEEE 802.11a standard applies Orthogonal Frequency Division Modulation (OFDM) technique at physical layer. The channel is partitioned into 54 sub-channels, and data is coded, modulated and transmitted at 48 of the 54 sub-carriers. A given transmission data rate corresponds to a combination of modulation scheme and coding rate in each sub-carrier. The supported data rates and corresponding combinations are listed in Table 5.5. From communication theory we know the reception SINR threshold increases with the data rate [35]. In this project we use the reception SINR threshold specifications of Atheros' 802.11a radio shown in Table 5.1. The reception threshold (in dB) is almost a linear function of data rate.

Thus, there is a tradeoff in applying higher data rate in transmission. On one hand, higher data rate decreases the transmission time for each packet, t_{trans}. There are more slots available for repetition in the lifetime of a message and packets of interfering messages are less likely to collide. On the other hand, higher data rate requires higher reception SINR threshold, thus each node has to transmit at higher power. Higher transmission power causes larger interference range and more interferers for each receiver. Figure 5.4 shows this mixed impact of data rate on the asymptotic probability of reception failure for AFR-CS in the nominal setting. Clearly, for this case, 18 Mbps is the optimal data rate to transmit.

The optimal data rate is dependent on the protocol design and the simulation parameter setting. Table 5.6 shows the optimal data rates of all the protocols we simulate in the nominal setting, as they are labeled in Fig-

Table 5.5: Rate Dependent Parameters in IEEE 802.11a PHY Specifications

Data Rate (Mbps)	Modulation	Coding Rate
6	BPSK	1/2
9	BPSK	3/4
12	QPSK	1/2
18	QPSK	3/4
24	16-QAM	1/2
36	16-QAM	3/4
48	64-QAM	2/3
54	64-QAM	3/4

Table 5.6: Optimal Data Rate for Simulated Protocols in the Nominal Setting

Protocol	Optimal Data Rate (Mbps)
SFR	12
AFR	18
SPR	12
APR	18
APR-CS	18
AFR-CS	18
802.11	24

ure 5.2. In Table 5.7 we show the optimal data rate of AFR-CS with different communication range. The other parameters are the same as in the nominal setting. Amazingly, we see that the optimal data rate is 18 Mbps for all the communication range values studied except for 30 m. We cannot make any further conclusions since we do not yet have analytical expression for optimal data rate. Currently the optimal data rate can only be found by simulation, and we only consider the data rates supported by 802.11a. In all the following results we show the simulation results of the protocols at the optimal data rate we find for the design parameters.

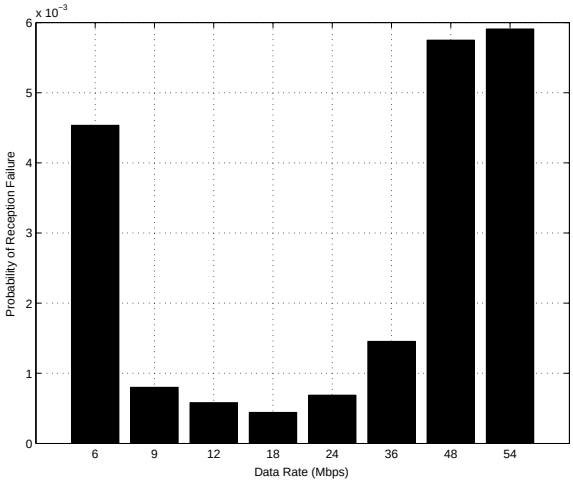

Figure 5.4: Probability of Reception Failure for Various Data Rate Under Nominal Setting: AFR-CS Protocol

Table 5.7: Optimal Data Rate of AFR-CS Protocol for Various Communication Ranges

Communication Range (m)	Available Time Slots	Optimal Data Rate (Mbps)
30	1027	12
60	1541	18
80	1541	18
120	1541	18
150	1541	18
180	1541	18
210	1541	18
240	1541	18

5.6 Sensitivity of AFR-CS Protocol on Design Parameters

5.6.1 Dependence on Communication Range and Network Topology

When one node transmits to another, nodes within the interference range of the receiver impact the quality of the communication. The severity of the impact depends on the number of interfering nodes, which is a function of the interference range and the network topology.

The interference range r_i of a receiver that is r meters away from the transmitter comes from equation 5.1. For a certain data rate, β in equation 5.1 is constant, therefore the interference range is proportional to TX/RX distance. The worst case is when the transmitter-receiver distance is the desired communication range, i.e. the furthest as it can be. On the other hand, the best case is when the receiver is the vehicle next to the transmitter in the same lane, with their average distance known.

The topology of vehicle communication network is determined by the road configuration and the vehicle traffic condition, which are respectively parameterized by lane number and vehicle distance/density in this paper. Thanks to the advances in transportation studies, such information of real highway traffic is readily available , e.g. from the PeMS system [3]. The average number of interferers of a given receiver is proportional to the ratio between the interference range and the vehicle distance. Since in all the cases we study the interference range is much larger than the road width, i.e. total width of lanes, the lane number merely acts as a multiplier. Neglecting the edge effects, when the ratio between the communication range and the average vehicle distance is the same, the topology of the vehicles within the communication zone, as well as the topology of the vehicles in the interference zones of each of the potential receiver, are the same. Therefore the performance of the protocol should also be the same. A larger such ratio means either all vehicles are transmitting at a higher power, or that the highway traffic is more congested. In either case, the performance of the protocol should degrade due to more interference.

Therefore, the performance of the protocol (both on PRF and CBT) depends on the communication range, the vehicle distance, and the lane number in the following manner.

$$Interferer\ Number \propto \frac{Communication\ Range}{Vehicle\ Distance} * (Lane\ Number) \quad (5.3)$$

We define the right hand side of the equation as the "Interference Indicator" for a transmitted message. It parameterizes the interference the potential receivers face when the communication range and network topology are given. The larger this indicator is, the more interference the receivers experience.

Figure 5.5 illustrates above discussions. Here we plot PRF vs. CBT, without explicitly showing repetition number. The performance of a protocol is bad if it has high PRF for given CBT, or if it requires high CBT to achieve a given PRF. Curves representing superior performance are located to the lower-left of the plot. There are three groups of curves where interference indicators are equal for curves in the same group and unequal across groups. Clearly, larger interference indicator means more interference and worse protocol performance. Also notice that there are many combination of parameters which can produce same interference indicator values. For example, the interference indicator of the middle group of curves is 16. By equation 5.6.1, all the four cases yield this value, although they are different in communication range, vehicle headway (average distance), or lane number.

We cannot distinguish scenarios with same interference indicator when observing the protocol performance. Thus, although we cannot study all possible combinations of parameters, the results reported in this paper actually represent a much broader scope in vehicle communication environment than those shown in Table 5.3. For example, although only 4-lane and 8-lane cases are studied in the paper, some results for 10-lane scenarios are obtained with vehicle density or communication range combinations that produce same interference indicators.

5.6.2 Sensitivity on All Parameters

We further study the sensitivity of the performance of AFR-CS protocol on parameters listed in 5.1. Figures 5.6-5.9 show the sensitivity results for various communication ranges, message generation intervals, and packet sizes. As stated above, except for the varying parameters we study the sensitivity for, all other parameters take values in Table 5.2. In Figure 5.9, the packet

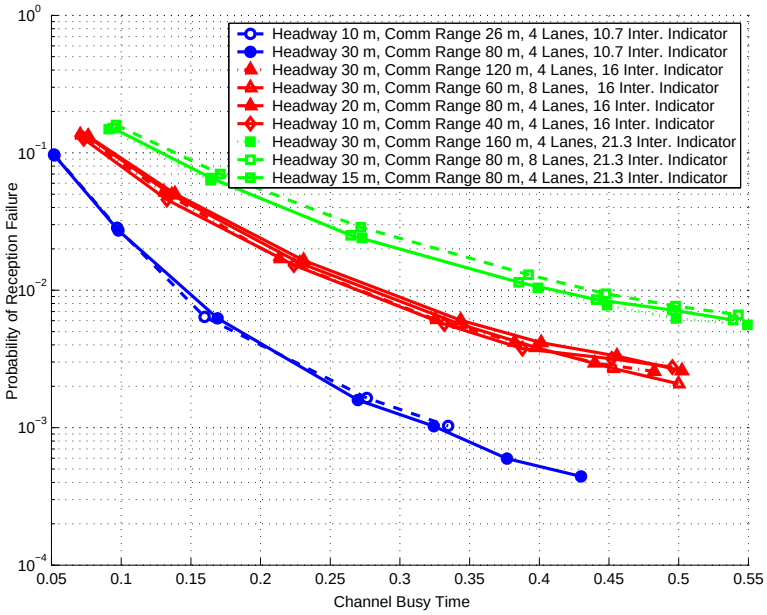

Figure 5.5: Performance of AFR-CS Protocol as a Function of Interference Indicator

size values only account for payload size, and headers and preamble are added according to Table 5.4.

Not surprisingly, Figures 5.6 indicates that an increase in communication range degrades the performance of the protocol. Larger communication range requires higher transmission power from each vehicle, therefore in the same network topology, more vehicles are interfering with each other. For the same CBT, probability of reception decreases with communication range, and CBT increases with communication range when the probability of failure is kept constant. If we require the probability of reception failure be lower than 0.01 and CBT be lower than 50%, with all other parameters taking values in Table 5.2 and data rate being 18 Mbps, the maximum allowed communication range lies between 180 m and 240 m.

Figure 5.7 compares the asymptotic PRF of AFR-CS protocol with that of 802.11 MAC in broadcast mode. We can see that in nominal setting when the communication range is 80 meters, AFR-CS is one order of magnitude better than 802.11, as has been shown in Figure 5.2. But as communication range increases, the benefit of repetition is lessened. When the communication

range is over 200 meters, the PRF of the two protocol converges. Clearly, when the nodes transmit at higher power to achieve larger communication range, the interference experienced by each node increases. At the same time, there are more hidden terminals around each nodes. The capability of repetition in combating hidden terminals is reduced when there are too many.

Observing Figure 5.8 and 5.9 in the same way, we conclude that smaller message interval and larger packet size degrade the protocol performance. These also agree with engineering intuition.

We conduct sensitivity analysis for all the parameter combinations in Table 5.3. From the result one can find the feasibility region of the parameters that achieves given communication requirements. We set the communication requirements to be:

- Probability of reception failure < 0.01
- Channel busy time $< 50\%$

Figure 5.10 shows the feasibility regions in parameter space. The three curves represent three cases with different packet sizes, where again only payload sizes are shown. The region below each curve is feasible, while the region above is infeasible. We use the interference indicator in horizontal axis with in mind the results in 5.6.1. We can achieve these interference indicator values with proper arrangement of communication range, vehicle density, and lane number. The figure shows that as interference increases, each node has to generate messages less frequently in order to meet the communication requirements. At the same time, larger packet size has a negative impact on the performance by decreasing the feasibility region. The feasibility results provide us with constraints in design. The larger the feasible region, the easier it is to design the protocol. For example, when the packet payload is 100 bytes, if the interference indicator is 20 (e.g. 5 lanes, vehicle distance = 30 meters, communication range = 120 meters), the nodes cannot transmit messages more than 10 times per second; while if the interference indicator is only 5 (e.g. 5 lanes, vehicle distance = 20 meters communication range = 20 meters), the nodes can transmit as many as 20 messages per second without violating the communication requirements. For 400 bytes case, when the interference indicator is larger than 20, no message interval values we simulate can satisfy the communication requirements. With another

set of communication requirements, our method can easily find the feasible parameter combinations in the same way.

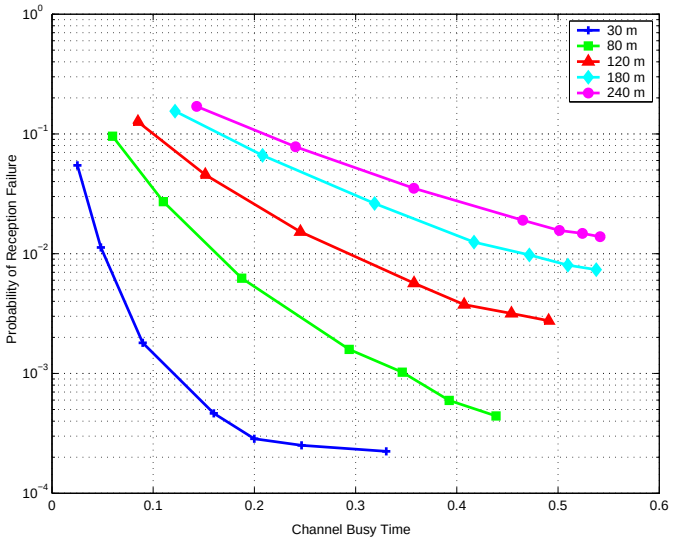

Figure 5.6: Probability of Reception Failure for Various Communication Ranges: AFR-CS Protocol

5.7 Bursts of Reception Failures

As discussed in Chapter 3, vehicle safety applications require small likelihood of bursts of reception failures in vehicle communication. We check if the AFR-CS protocol satisfies such requirements and show the results in Figures 5.11 and 5.12.

In Figure 5.11, we study the probability of message failure bursts conditioned on one message failure occurrence, i.e. given that a message has failed, the probability that there are more consecutive message failures following it. Clearly, the conditional probability of message failure bursts decreases with the number of repetitions and eventually levels off. It increases with the communication range. In all cases we study, as the packet being repeated many time, the conditional probability of message failure bursts stabilizes to values lower than 0.05.

Figure 5.12 shows the probability of message failure bursts versus repetition number. The communication range is 240 meters, and all other param-

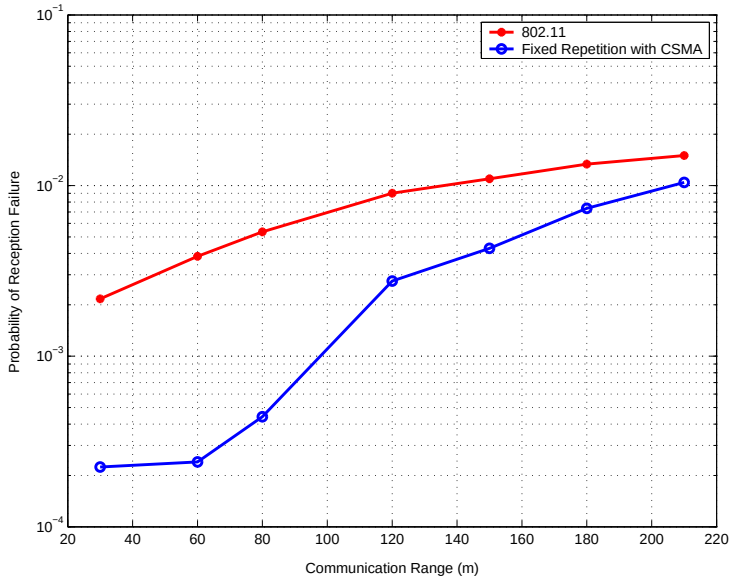

Figure 5.7: Comparison of AFR-CS and 802.11 for Various Communication Range

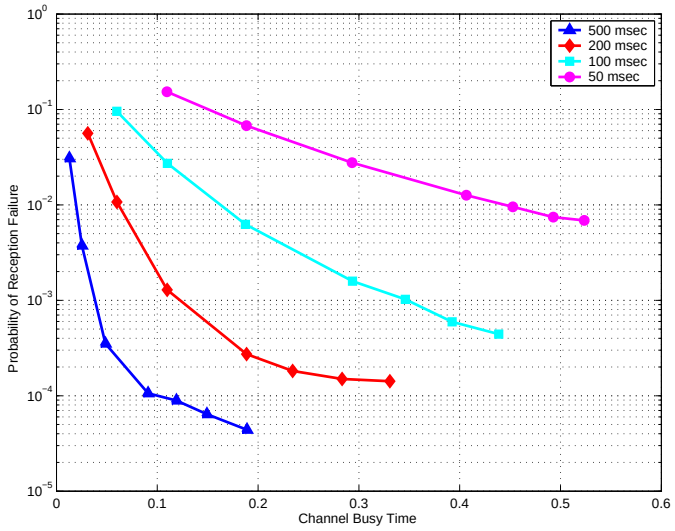

Figure 5.8: Probability of Reception Failure for Various Message Generation Intervals: AFR-CS Protocol

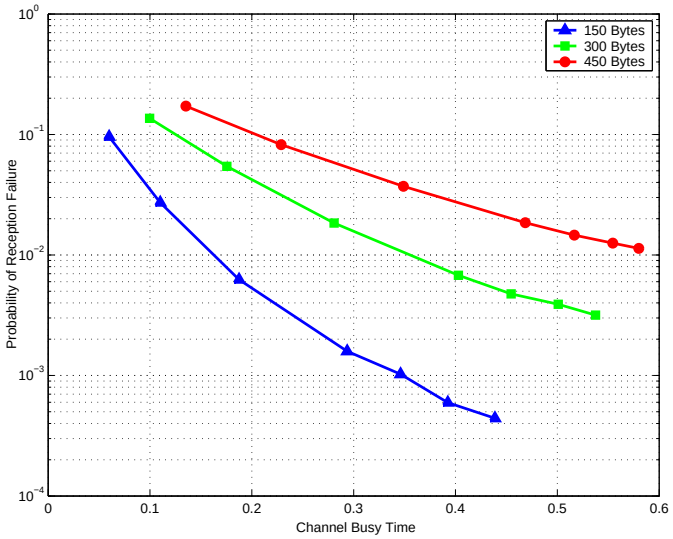

Figure 5.9: Probability of Reception Failure for Various Packet Sizes: AFR-CS Protocol

eters are from Table 5.2. The more the packets of a message are repeated, the less probable it is for the failure bursts of the message to occur. For the same repetition number, longer bursts are less likely than shorter ones. As we repeat reasonably many times, the probability of reception failure of single messages as well as that of consecutive messages both approach zero. We show here only the result of 240 meters communication range, which is worse than the results of any shorter communication range. We conclude that AFR-CS protocol rarely causes bursts of message failures.

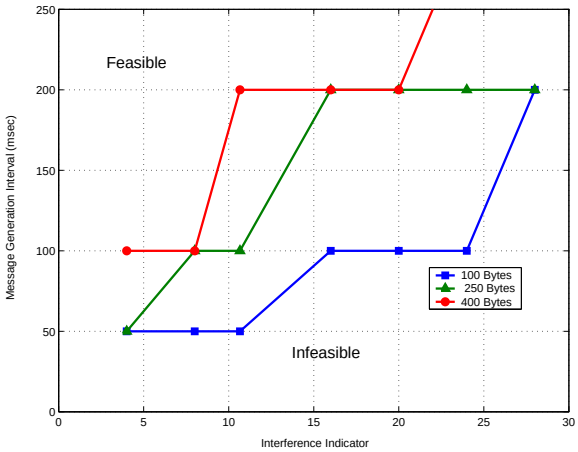

Figure 5.10: Feasibility Regions for Probability of Reception Failure < 0.01 and CBT $< 50\%$

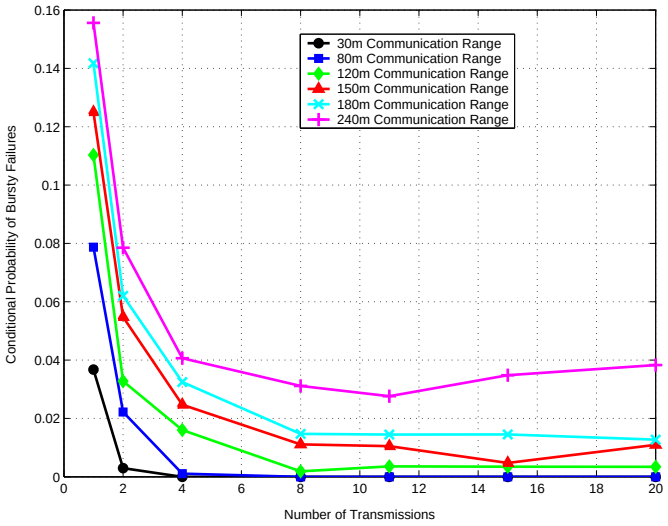

Figure 5.11: Probability of message failure bursts conditioned on one message failure: AFR-CS protocol

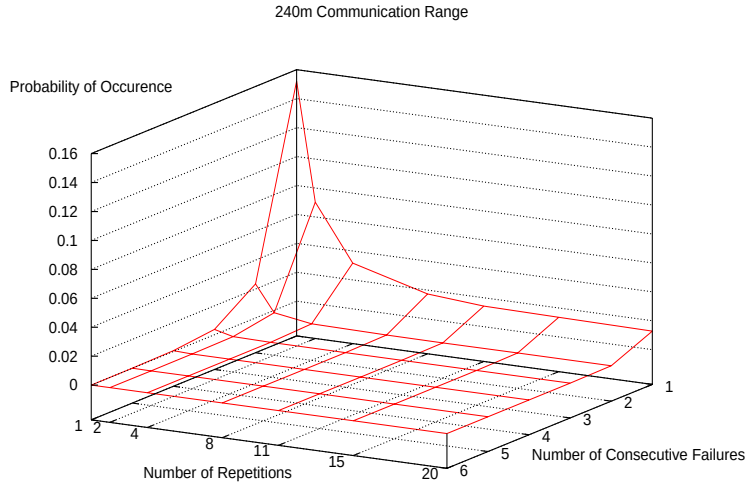

Figure 5.12: Probability of message failure bursts vs. repetition number: AFR-CS Protocol, Communication Range = 240 m

Chapter 6

Conclusion and future work

Issues concerning the design of MAC protocol for vehicle safety communications in 5.9 GHz DSRC spectrum were studied. The communication requirements of vehicle safety applications were discussed. Several protocols based on repetition coding were proposed. We analytically studied two of the protocols. We simulated all of the proposed protocols in a vehicle communication environment. The analytical results match well with the simulation results. From among the proposed protocols, we found that AFR-CS performed the best. Some highlights of the performance of this protocol under nominal setting are:

1. The probability of reception failure approaches 0.0004 asymptotically. This is an order of magnitude lower than that of IEEE 802.11 MAC protocol in broadcast mode.

2. The channel busy time is lower than 50% to achieve the desired probability of reception failure.

3. Message failure bursts are rarely caused by the MAC protocol.

4. The optimal 802.11-supported data rate to transmit is 18 Mbps.

We studied the sensitivity of AFR-CS to a wide range of design parameters and found the feasibility regions of the protocol with probability of reception failure lower than 0.01 and CBT lower than 50%. We found that the communication range, vehicle density, and lane number affect the performance only in determining the interference indicator.

The environment faced by vehicle safety communication is heterogeneous. We believe in such settings transmission power and data rate need to be adapted within the environment. For example, when traffic density is high, vehicles should transmit at a lower power to reduce the interference to neighboring vehicles. At the same time since the density is high, packets transmitted at low power can reach enough neighboring vehicles for safety. On the other hand when the density is low, the transmission power should be increased to reach the same number of vehicles. This is also necessary because, generally speaking for vehicles on highway, when the density is low, the velocity is high and louder communication is needed to ensure safety. Such an adaptive system can be designed based on current homogeneous results. Applying more efficient coding schemes than repetition coding is another potential direction of study. We need to design the system with consideration to both the communication and computation components. In the simulation, we used a deterministic channel model. Wireless V-V communication channel should be better understood and modelled. The impact of a stochastic channel model on the simulation should be studied.

Chapter 7

Appendix

7.1 Proof of Lemma 1

Proof. There are two methods to prove this lemma.

1. $P(\neg S_j) = 1 - P(S_j)$

   Let E_l be the event that there are l messages generated by all transmitters within interference range of the receiver in $(t_j - \tau, t_j]$. Since one message can only affect time period of length τ after the message's generation, these l messages are all the messages whose packets potentially interfere with packet p_j. The probability for any one of the l messages to select the slot occupied by p_j (to transmit its own packet) is $\frac{k}{n}$. And p_j is received successfully if and only if none of the l messages selects p_j's time slot. Formally we have

$$\begin{aligned} P(S_j) &= \sum_{l=0}^{\infty} P(S_j|E_l)P(E_l) \\ &= \sum_{l=0}^{\infty} \left(1 - \frac{k}{n}\right)^l \cdot e^{-m\lambda\tau} \frac{(m\lambda\tau)^l}{l!} \\ &= e^{-m\lambda\tau} \sum_{l=0}^{\infty} \frac{[m\lambda\tau(1 - \frac{k}{n})]^l}{l!} \\ &= e^{-m\lambda\tau} e^{m\lambda\tau(1-\frac{k}{n})} \\ &= e^{-m\lambda\tau\frac{k}{n}} \end{aligned}$$

In above derivation we used the fact that the repetitions of different message are independent and the total message generation process is a Poisson process.

Therefore $P(\neg S_j) = 1 - P(S_j) = 1 - e^{-m\lambda\tau\frac{k}{n}}$

2. Prove using the theory of compound Poisson distribution. Let l be the total number of message generated in the interference range of the receiver in $(t_j - \tau, t_j]$. For each of these message there is a Bernoulli variable X_i corresponding to the time slot occupied by p_j, where $X_i = 1$ means that there is a repetition of the i-th message in the time slot and $X_i = 0$ means the time slot is not selected by this message. We then have $P(X_i = 1) = \frac{k}{n}$ and $P(X_i = 0) = 1 - \frac{k}{n}$. Since all $X_i's$ are i.i.d from the design of protocol, $X = \sum_{i=1}^{L} X_i$ is the sum of L random variables, where L itself is a Poisson distributed random variable with $P(L = l) = e^{-m\lambda\tau}\frac{(m\lambda\tau)^l}{l!}$. According to the theory of compound Poisson distribution (see e.g. [21]), X also has a Poisson distribution with $P(X = l) = e^{-m\lambda\tau\frac{k}{n}}\frac{(m\lambda\tau\frac{k}{n})^l}{l!}$. Therefore

$$\begin{aligned} P(\neg S_j) &= 1 - P(S_j) \\ &= 1 - P(X = 0) \\ &= 1 - e^{-m\lambda\tau\frac{k}{n}} \end{aligned}$$

□

7.2 Proof of Lemma 2

Proof. We prove using induction.

1. For $k = 2$, we need to prove

$$P(\neg S_i \wedge \neg S_j) > P(\neg S_i)P(\neg S_j), \forall 1 \leq i, j \leq n$$

First we notice

$$\begin{aligned} P(\neg S_i \wedge \neg S_j) &= 1 - P(S_i \cup S_j) \\ &= 1 - P(S_i) - P(S_j) + P(S_i \wedge S_j) \end{aligned}$$

From Lemma 1 we have known that

$$P(S_i) = P(S_j) = e^{-m\lambda\tau\frac{k}{n}}$$

Now we need to figure out $P(S_i \wedge S_j)$.

Suppose that p_i starts at t_i and p_j starts at t_j, and assume $t_j > t_i$ without loss of generality. Then p_i can potentially be interfered by messages generated in $(t_i - \tau, t_i]$ only, and p_j by messages generated in $(t_j - \tau, t_j]$ only.

Since p_i and p_j are known to be selected by the same one message, we have

$$t_i - \tau < t_j - \tau < t_i < t_j.$$

Let $\tau_1 = t_i - (t_j - \tau) = \tau - (t_j - t_i)$, and $\tau_0 = \tau - \tau_1 = t_j - t_i$. Then the time period $(t_i - \tau, t_j]$ is divided into three time intervals, $I_1 = (t_i - \tau, t_j - \tau]$, $I_2 = (t_j - \tau, t_i]$, and $I_3 = (t_i, t_j]$. I_1 and I_3 both have length τ_0 while the length of the I_2 is τ_1. Messages generated in I_1 can only interfere with p_i, and messages generated in I_3 can only interfere with p_j. However messages generated in I_2 can interfere with both p_i and p_j. We also observe that the behavior of messages generated in different intervals is independent. $P(S_i \wedge S_j)$ is the probability that neither p_i nor p_j are collided. With the same assumptions as used in the proof of lemma 1, we have

$$\begin{aligned}
P(S_i \wedge S_j) = &\left(\sum_{l_1=0}^{\infty}\left(1-\frac{k}{n}\right)^{l_1}\cdot e^{-m\lambda\tau_0}\frac{(m\lambda\tau_0)^{l_1}}{l_1!}\right)\cdot \\
&\left(\sum_{l_2=0}^{\infty}\left(1-\frac{k}{n}\right)^{2l_2}\cdot e^{-m\lambda\tau_1}\frac{(m\lambda\tau_1)^{l_2}}{l_2!}\right)\cdot \\
&\left(\sum_{l_3=0}^{\infty}\left(1-\frac{k}{n}\right)^{l_3}\cdot e^{-m\lambda\tau_0}\frac{(m\lambda\tau_0)^{l_3}}{l_3!}\right) \\
&= e^{-m\lambda\tau_0\frac{k}{n}}\cdot e^{m\lambda\tau_1[\left(1-\frac{k}{n}\right)^2-1]}\cdot e^{-m\lambda\tau_0\frac{k}{n}} \\
&= e^{-2m\lambda\tau\frac{k}{n}+m\lambda\tau_1\frac{k^2}{n^2}} \\
&> e^{-2m\lambda\tau\frac{k}{n}} \\
&= P(S_i)P(S_j)
\end{aligned}$$

where the last equation comes from lemma 1.

Therefore

$$\begin{aligned} P(\neg S_i \wedge \neg S_j) &= 1 - P(S_i \cup S_j) \\ &= 1 - P(S_i) - P(S_j) + P(S_i \wedge S_j) \\ &> 1 - P(S_i) - P(S_j) + P(S_i)P(S_j) \\ &= [1 - P(S_i)][1 - P(S_j)] \\ &= P(\neg S_i)P(\neg S_j) \end{aligned}$$

The above inequality holds $\forall 1 \leq i, j \leq n$. Since order does not matter in equation 4.2, we can arbitrarily let $p_1 = p_i$ and $p_2 = p_j$. The lemma is thus proved for the case of $r = 2$.

2. Assume equation 4.2 holds for all of j satisfying $1 < j \leq r - 1 \leq n - 1$, then we have

$$P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) > (\prod_{j=1}^{r-1} P(\neg S_j))$$

Let t_i be the starting time of packet p_i for any $1 \leq i \leq r$. Since the order does not matter in equation 4.2, we can always rearrange the packets such that $t_1 < t_2 < \ldots < t_{r-1} < t_r$. Therefore we will assume so without loss of generality.

Now let B_i be the event that there are i other messages generated in the time period $(t_1 - \tau, t_{r-1}]$.

$$\begin{aligned} P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} | \neg S_r) &= \sum_{i=0}^{\infty} P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} | B_i, \neg S_r) P(B_i | \neg S_r) \\ &= \sum_{i=0}^{\infty} P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} | B_i) P(B_i | \neg S_r) \\ &\geq \sum_{i=0}^{\infty} P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} | B_i) P(B_i) \\ &= P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) \end{aligned}$$

In above derivation, the second equation comes from the fact that the decision on whether to select a slot to transmit is independent from that of another. Therefore event that p_r fails affects the probability of failure of another packet only by saying that there might be other interfering messages for the second packet. If all the interfering messages are known, the failure of one packet says nothing more about the failure of the other. The inequality above comes since when packet p_r fails, there are surely some other messages generated in $(t_r - \tau, t_r]$. Therefore it is more likely to have some interfering messages in $(t_r - \tau, t_{r-1}]$ which is a subset of $(t_1 - \tau, t_{r-1}]$.

From above inequality we have

$$\begin{aligned} P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} \wedge \neg S_r) &= P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1} | \neg S_r) P(\neg S_r) \\ &\geq P(\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) P(\neg S_r) \\ &> (\prod_{j=1}^{r-1} P(\neg S_j)) P(\neg S_r) \\ &= \prod_{j=1}^{r} P(\neg S_j) \end{aligned}$$

Hence equation 4.2 also holds for r, and the lemma is proved.

□

7.3 Proof of Lemma 3

Proof. Following the same arguments as in the proof of 1, let E_l be the event that there are l messages generated by all transmitters in $(t_j - \tau, t_j]$, then $l \geq 1$ since T_j has occurred. Thus

$$
\begin{aligned}
P(S_j|T_j) &= \sum_{l=1}^{\infty} P(S_j|E_l)P(E_l) \\
&= \sum_{l=1}^{\infty} \left(1 - \frac{k}{n}\right)^l \cdot e^{-m\lambda\tau} \frac{(m\lambda\tau)^l}{l!} \\
&= e^{-m\lambda\tau} \sum_{l=1}^{\infty} \frac{[m\lambda\tau(1-\frac{k}{n})]^l}{l!} \\
&= e^{-m\lambda\tau}(e^{m\lambda\tau(1-\frac{k}{n})} - 1) \\
&= e^{-m\lambda\tau\frac{k}{n}} - e^{-m\lambda\tau}
\end{aligned}
$$

Therefore

$$
P(\neg S_j|T_j) = 1 - P(S_j|T_j) = 1 - e^{-m\lambda\tau\frac{k}{n}} + e^{-m\lambda\tau}
$$

□

7.4 Proof of Lemma 5

Proof.

$$
\begin{aligned}
P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) &= P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1} \wedge T_r)P(T_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) \\
&\quad + P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1} \wedge \neg T_r)P(\neg T_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) \\
&= P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1} \wedge T_r)P(T_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1}) + 0 \\
&\leq P(\neg S_r|\neg S_1 \wedge \ldots \wedge \neg S_{r-1} \wedge T_r) \\
&= P(\neg S_r|T_r)
\end{aligned}
$$

The last equation comes from the fact that a message selects different time slots in its lifetime to transmit packets independently. Therefore the failure of p_j says nothing about p_k for $k \neq j$ other than that there may be messages from other transmitters in $(t_j, t_k]$, the lifetime period shared by the two packets.

□

Bibliography

[1] http://path.berkeley.edu/DSRC.

[2] Dedicated Short Range Communications (DSRC) home. http://www.leearmstrong.com/dsrc/dsrchomeset.htm.

[3] Freeway performance measurement system (PeMS). http://pems.eecs.berkeley.edu.

[4] Intersection collision avoidance using its countermeasures, final report: Performance guidelines. Technical Report DOT HS 809 171, U.S. Department of Transportation, National Highway Traffic Safety Administration.

[5] Monarch project. http://www.monarch.cs.cmu.edu/cmu-ns.html.

[6] The netowrk simulator: NS-2. http://www.isi.edu/nsnam/ns.

[7] Atheros, Inc. http://www.atheros.com.

[8] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. *IEEE Standard 802.11a-1999*, 1999.

[9] N. Abramson. The ALOHA system-another alternative for computer communications. *1970 Fall Joint Comput. Conf., AFIPS Conf. Proc.*, 37:281–285, 1970.

[10] N. Abramson. The throughput of packet broadcasting channels. *IEEE Trans. Comm.*, COM-25:117–128, January 1977.

[11] N. Abramson, editor. *Multiple Access Communications: Foundations for Emerging Technologies*. IEEE Press, 1993.

[12] R. Attias, D. Lee, A. Puri, S. Tripakis, R. Sengupta, and P. Varaiya. A token-ring medium-access-control protocol with quality of service guarantees for wireless ad-hoc networks. Technical Report UCB-ITS-PRR-2001-07, California PATH, March 2001.

[13] L. Barr and W. Najm. Crash problem characteristics for the intelligent vehicle initiative. *80th National Research Council (U.S.). Transportation Research Board Meeting*, 2001.

[14] V. Bharghavan, A. Demers, S. Shanker, and L. Zhang. MACAW: A media access protocol for wireless LANs. *ACM SIGCOMM'94*, pages 212–225, August 1994.

[15] G. Bianchi. IEEE 802.11-saturation throughput analysis. *Communications Letters*, 2(12):318–320, December 1998.

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

[17] F. Cali, M. Conti, and E. Gregori. Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput. *IEEE/ACM Transactions on Networking*, 8(6):785–799, December 2000.

[18] F. Cali, M. Conti, and E. Gregori. IEEE 802.11 protocol: design and performance evaluation of an adaptive backoff mechanism. *IEEE Journal on Selected Areas in Communications*, 18(9):1774–1786, September 2000.

[19] H. Chhaya and S. Gupta. Performance modling of asynchronous data transfer methods of IEEE 802.11 MAC protocol. *Wireless Networks*, 3:217–234, 1997.

[20] T. Cover and J. Thomas. *Elements of Information Theory*. New York: Wiley-Interscience, 1991.

[21] W. Feller. *An introduction to Probability Theory and its Applications*, volume 1. John Wiley and Sons, 1968.

[22] R. Gallager. A perspective on multi-access channels. *IEEE Trans. Information Theory*, IT-31, March 1985. Special issue on random access communications.

[23] J. Garcia-Luna-Aceves and C. Fullmer. Floor aquisition multiple access (FAMA) in single channel wireless networks. *ACM Mobile networks and applications*, 4:157–174, 1999.

[24] P. Gupta and P. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, IT-46(2):388–404, March 2000.

[25] K. Hedrick, Q. Xu, and M. Uchanski. Enhanced AHS safety through the integration of vehicle control and communication. Technical Report UCS-ITS-PRR-2001-28, California PATH, 2001.

[26] E. Hoffmann and R. Mortimer. Scaling of relative velocity between vehicles. *Accident Analysis and Prevention*, 28(4):415–421, 1996.

[27] P. Karn. MACA-a new channel access method for packet radio. *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140, 1990.

[28] Y. Ko and N. Vaidya. Geocasting in mobile ad hoc networks: location-based multicast algorithms. *Second IEEE Workshop on Mobile Computer Systems and Applications*, Feb. 1999.

[29] H. Krishnan and C. Kellum. Use of communication in vehicle safety application. Internal Report of General Motors Company, 2002.

[30] D. Lee, A. Attias, A. Puri, R. Sengupta, S. Tripakis, and P. Varaiya. A wireless token ring protocol for intelligent transportation systems. *IEEE 4th International Conference on Intelligent Transportation Systems, Oakland, CA*, 2001.

[31] B. Leiner, D. Nielson, and F. Tobagi (Guest Eds.). Special Issue on Packet Radio Networks. *Proceedings of IEEE*, 75(1), January 1987.

[32] J. Li, C. Blake, D. De Couto, H. Lee, and R. Morris. Capacity of wireless ad hoc networks. *MobiCom '01*, July 2001.

[33] Department of Transportation of California. California highway design manual. 1995.

[34] California PATH. Shift: The hybrid system simulation programming language. http://www.path.berkeley.edu/shift/.

[35] J. Proakis. *Digital Communications*. WCB/McGraw Hill, third edition, 1995.

[36] L. Roberts. Aloha packet system with and without slots and capture. *Computer Communication Review*, 5(2):28–42, 1975.

[37] P. Seiler. *Coordinated Control of Unmanned Aeiral Vehicles*. PhD thesis, University of California, Berkeley, 2001.

[38] P. Seiler and R. Sengupta. Analysis of communication losses in vehicle control problems. *American Control Conference*, June 2001.

[39] J. Sobrinho and A. Krishnakumar. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *IEEE Journal on Selected Areas in Communications*, 17(8):1353–1368, August 1999.

[40] B. Song and D. Delorme. Human driver model for smartAHS based on cognitive and control approaches. *Tenth Annual Meeting of the Intelligent Transportation Society of America*, May 2000.

[41] H. Takagi and L. Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. *IEEE Transactions on Communications*, COM-32(3):246–257, March 1984.

[42] Y. Tay and K. Chua. A capacity analysis for the IEEE 802.11 MAC protocol. *Wireless Networks*, 7(2):159–171, 2001.

[43] F. Tobagi and L. Kleinrock. Packet switching in radio channels: Part I-carrier sense multiple-access modes and their throughput/delay characteristics. *IEEE Tans. Comm.*, COM-23:1400–1416, December 1975.

[44] F. Tobagi and L. Kleinrock. Packet switching in radio channels: Part II-the hidden terminal problem in carrier sensing multiple access models and the busy tone solution. *IEEE Tans. Comm.*, COM-23:1417–1433, December 1975.

[45] F. Tobagi and L. Kleinrock. Packet switching in radio channels: Part III-polling and (dynamic) split-channel reservation multiple access. *IEEE Tans. Comm.*, COM-24(8):832–845, August 1976.

[46] J. VanderWerf, N. Kourjanskaia, S. Shladover, H. Krishnan, and M. Miller. Modeling the effects of driver control assistance systems on traffic. *National Research Council Transportation Research Board 80th Annual Meeting*, January 2001.

[47] H. Weatherspoon and J. Kubiatowicz. Erasure coding vs. replication: A quantitative comparison. *The First International Workshop on Peer-to-Peer Systems*, March 2002.

[48] S. Wu, Y. Tseng, and J. Sheu. Intelligent medium access for mobile ad hoc networks with busy tones and power control. *IEEE Journal on Selected Areas in Communications*, 18(9):1647–1657, September 2000.

[49] Q. Xu, K. Hedrick, R. Sengupta, and J. VanderWerf. Effects of vehicle-vehicle/roadside-vehicle communication on adaptive cruise controlled highway systems. *IEEE Vehicular Technology Conference*, October 2002.

[50] Q. Xu and R. Sengupta. Simulation, analysis, and comparison of ACC/CACC in highway merging control. *IEEE Intelligent Vehicles Symposium*, June 2003.

[51] M. Zennaro and J. Misener. A state-map architecture for safe intelligent intersection. *ITSA, Minneapolis*, 2003.

[52] J. Zhu and S. Roy. MAC for Dedicated Short Range Communications in Intelligent Transporation System. *IEEE Communications Magazine*, pages 60–67, December 2003.