

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

Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages

Qing Xu, Tony Mak
Jeff Ko, Raja Sengupta
University of California, Berkeley

California PATH Working Paper
UCB-ITS-PWP-2005-4

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 Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Report for Task Order 5600

November 2005

ISSN 1055-1417

Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages

Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta

Abstract

We propose a Medium Access Control (MAC) protocol design for a vehicle to send safety messages to other vehicles. We develop a QoS model for safety messages consistent with the active safety systems literature. Each message has a range and useful lifetime. The QoS target is to have each message be received with high probability within its specified lifetime by each vehicle within its specified range. The protocol design is based on rapidly re-broadcasting each message multiple times within its lifetime in combination with the 802.11 DCF. This makes the design compatible with the emerging standards for DSRC. Six different design variations are proposed. We derive equations and develop a simulation tool to assess the performance of the designs. Using these we identify the best and most easily implemented of the designs. Design performance depends on the number of re-broadcasts, power, modulation, coding, and vehicular traffic volumes. We show that under certain assumptions on the loss probability tolerated by safety applications, the design is able to transport safety messages in vehicular ad-hoc networks.

I. INTRODUCTION

This paper is about the design of wireless local area networks to enable active vehicle safety systems. For couple of decades automotive engineers have been designing in-vehicle information systems that will detect potential crash situations a second or less in advance and either warn the driver or control the vehicle [33], [16]. These systems are called active safety systems. Some active safety systems provide forward collision warnings, others awareness about vehicles in the blind spot, and yet others about conflicts at intersections. Active safety systems have the potential to prevent many of the crashes that occur today. They target the large class of crashes caused by driver decision errors [34].

Active Safety Systems share a common need. The vehicle needs to know about the locations and motions of its neighboring vehicles. We call this the state of the vehicle neighborhood. Most active safety systems in the literature try to learn the state of the neighborhood by using sensors like radar, laser, or vision. The most promising of these has been radar. Since collision threats come from different directions, the idea has been to equip the vehicles with radars looking forward, to the rear, the right lane and left lane.

This paper is motivated by the idea of enabling active safety systems by learning the locations and motions of neighboring vehicles using GPS and ad-hoc wireless networking technologies like Wi-Fi. A preliminary version appeared in [37]. We call wireless-enabled active safety systems, Cooperative Active Safety Systems (CASS). GPS and Wi-fi are considerably cheaper than the multiple radars that would be required to track all neighboring threats. Thus CASS could replace or complement radar based systems.

The academic community is responding rapidly to these new opportunities. Mobicom instituted its first workshop on Vehicular Ad-hoc Networks (VANET) last year [8]. It continues this year. Government and industry are also moving rapidly on several fronts to promote the penetration of wireless local area networking into road transportation, and its use to enhance the safety of the system. The Federal Communications Commission (FCC) has allocated the Dedicated Short Range Communication (DSRC) spectrum for transportation in the 5.9 GHz band and has ruled that safety messages will have priority access in the spectrum [13]. A USDOT sponsored standard process under ASTM voted to base DSRC on IEEE 802.11a [1]. IEEE has taken up the standardization of DSRC by creating IEEE 802.11p. This process has built priority for safety into its channelization plan. NHTSA and the automotive OEM's created the Vehicle Safety Communication Consortium (VSCC) to promote vehicle-vehicle networking for safety. In their final report [6] they write:

It is not yet certain if vehicle safety applications can be designed to effectively mitigate the effects of potential channel overloading in high traffic environments.

FHWA and three state DOT's created the Intersection Decision Support (IDS) consortium [40]. They demonstrated roadside-vehicle communication to reduce intersection collisions.

This work was supported by California PATH projects TO4224, TO4403, TO5600, and by a gift from Daimler-Chrysler Research and Technology North America, Inc.

Q. Xu is with the Department of Mechanical Engineering, University of California, 1995 University Avenue, Suite 386, Berkeley, CA 94720, U.S.A. qingxu@me.berkeley.edu

Corresponding Author: T. Mak is with the Department of Civil and Environmental Engineering, University of California, Berkeley, CA 04720, U.S.A. tonykm@path.berkeley.edu

J. Ko is with California Partners of Advanced Transits and Highways (PATH), Richmond, CA 94804, U.S.A jko@path.berkeley.edu

R. Sengupta is with the Department of Civil and Environmental Engineering, University of California, Berkeley, CA 04720, U.S.A. raja@path.berkeley.edu

Figure 1 shows a snapshot of the state of the vehicle neighborhood captured from a system we have built. We have three cars with GPS and 802.11a radios. Each vehicle periodically transmits its GPS position, speed, and heading, i.e. the vehicle motion state. Each vehicle receives this information from its neighbors and plots it in a coordinate frame fixed to its own body to produce a map like figure 1. The arrow in the middle is the vehicle itself. The arrowhead points in the forward direction. The other arrows show the relative position and orientation of the other two vehicles. The state of the vehicle neighborhood is then read by higher level safety applications that issue warnings to the driver as necessary.

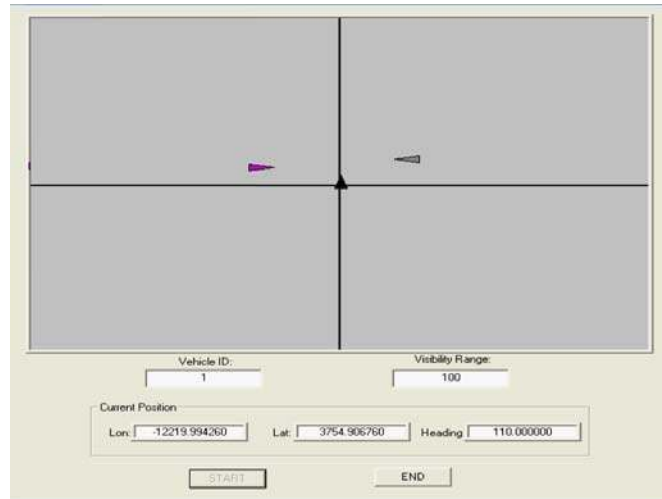


Fig. 1. A Snapshot of Vehicle Neighborhood Map

In this paper we propose a network design for cooperative active safety systems and evaluate it to see if it can do the job. The evaluation focuses on vehicles driving on a 4 to 8 lane freeway using 802.11a radios running over a 20 MHz channel in the DSRC spectrum. This choice of spectrum and technology is motivated by the FCC and USDOT proposal on its use for transportation safety applications [13].

To evaluate designs we need to estimate the amount of data traffic generated by CASS and pick Quality of Service (QoS) measures. This is the content of section II titled Problem Formulation. The section is divided into two subsections. Till communication design is better understood, CASS will not be fully designed and the precise levels of data traffic generated will not be known. Therefore to work on the network design problem we analyze the active safety literature and develop bounds on the amount of data traffic that could be generated by CASS. This is the first subsection.

The second subsection has two QoS measure suitable for networks designed to support CASS. It is argued that the right QoS model for active safety systems is for each message to have a specified lifetime and range. The main QoS measure used to evaluate the network is the probability a safety message is received within its lifetime at a randomly chosen vehicle within its specified range. Range is measured relative to the sender. The second measure we use is channel busy time.

Section III is a review of the related network design literature. Section IV describes our network designs. The designs are based on single hop broadcast overlayed on the 802.11a Distributed Coordination Function (DCF). The focus on single-hop broadcast is motivated by the safety data traffic bounds in section II. If it works, it has the benefit of containing the network design problem in layer 2 and layer 1. The emphasis on 802.11a technology is to keep the design compatible with the rules governing the DSRC spectrum allocated by FCC for transportation.

Our designs try to maximize the reception probability measure by repeatedly broadcasting each message several times within its lifetime in conjunction with DCF. This medium access control (MAC) is ad-hoc and based on the random access literature. We try an ad-hoc solution to make deployment easier by avoiding dependence on coordinating base stations or a roadside infrastructure. We try random access protocols because more sophisticated MAC protocols that schedule nodes in an ad-hoc setting are unproven at freeway traffic volumes and mobility levels. This situation has large numbers of hidden terminals. Related MAC schemes in the literature are discussed in III.

It turns out the QoS measure depends on the number of repetitions, modulation, and coding. These need to be chosen primarily to manage hidden terminals and multiple access interference. Repeating a message more than once raises the probability of reception. Repeating too many times causes too many collisions reducing the probability of reception. There is an optimal repetition number related to the range requirement, total offered load, and vehicular traffic density. We establish this analytically and through simulation.

The QoS relates to modulation and coding because the two determine message transmission time. If the transmission time is increased the message is vulnerable to collision for a longer time. On the other hand, at the smaller constellation sizes or

higher code rates associated with higher transmission rates the required transmission power reduces. This reduces interference power. It turns out there is an optimal transmission time as well related to the specified range, offered load, and vehicular traffic density. Once the modulation and code rate are chosen, our design chooses transmission power to overcome thermal noise at the range specified in the message.

We present mathematical expressions (section V) for the message reception probability and a simulation tool (section VI)). The simulation is done in NS-2 with vehicle motion traces generated by the SHIFT highway traffic simulator. In section VII we use the tools to establish the arguments about optimal operating points and find them at certain nominal vehicular traffic and safety data traffic levels. These arguments are used to select the best protocol design. Section VIII presents the probability of reception over the entire safety data traffic space defined in section II. This is done by computing the optimal repetition number, modulation, and code rate for various points in the safety data traffic space. This results in approximately 600 gigabyte of simulation data. We show how to summarize this data by choosing a target QoS (reception probability). For any given QoS target, we are able to use the simulation data to partition the safety data traffic space into feasible and infeasible parts. In particular, we show the partition for a reception probability of 99/100 and 999/1000

We choose 99/100 because packet loss probabilities of 1/100 or smaller (reception probability of 99/100 or higher) may be acceptable. A loss rate of 1/100 is too high in many networks. However, a safety message reports on the state of motion of the sender vehicle, e.g., its location, speed, heading, etc. The receiver could run a model to compensate for the occasional lost message by extrapolating from motion values received in the past.

It should be noted that the simulations are homogeneous. Each simulation has a particular combination of values in table I, i.e., message rate, packet size, message range, traffic flow, and number of lanes. Each vehicle in the simulation generates messages by a Poisson process with the same rate. The packet size and range of each message is the same. In practice, different safety messages may have different specified ranges, sizes, or arise from streams with different rates. The design accommodates this variation though it does not appear in our evaluation. We leave such variation out of the simulation because without further design of CASS, the statistical distribution of packet sizes, specified ranges, or lifetimes will not be known. If the average of the distribution conforms to the parameters of the homogeneous simulation, this evaluation is at least a first step towards CASS design targets as explained next.

The principal finding is that if CASS is to work within the 20 MHz DSRC channels with 802.11a radios then more research is required to improve application design or communication network design. From the build shown in figure 1 and the requirements in [6] it is known that if every car could broadcast its motion state every 50 to 100 millisecond with enough power to cover 300 meters, CASS would work. With our kind of network design, the loss rate may be above 30%. This is too high.

If CASS is to be enabled by the type of layer 2 protocol design in this paper design targets should be as follows. The application should be designed to tolerate a loss rate of about 1/100. To achieve a QoS target of 1/100 on a highway at maximum flow, the average message rate should be slower than 1/200 millisecond and the average specified range about 150 meters. On a jammed highway the average message range should be about 50 meters. Without the design enhancements in this paper, the loss rate would be 39/100 at this message size, rate, and range. The 39% loss rate is computed by the same simulation models used for all the QoS numbers in this paper. There is only one difference. The MAC protocol associated with the 39% rate is 802.11 DCF instead of our design.

These findings define a future research agenda. The CASS application should choose message range adaptively, leading to a reduction in the average message range as vehicular traffic gets denser. Fortunately, the active safety literature indicates this reduction may be acceptable. When traffic gets denser, average vehicular speeds get lower implying oncoming vehicles have smaller stopping distances. Neighboring vehicles are also closer. Thus lesser power should be safe enough, even though it might fail to reach vehicles that are otherwise reached in high speed traffic. Likewise, a motion state broadcast once every 200 milliseconds is too slow under certain circumstances, e.g., hard braking (see [12]). However, it may be possible to adhere to this rate on average by sometimes broadcasting faster than this rate and sometimes slower. For example, if the vehicle is cruising at even speed there may be no need to broadcast frequently. On the other hand, if it is braking rapidly, it may broadcast once every 50 milliseconds. This means adapting the message rate to the motion state. Further research is required to design a CASS application with such range or rate adaptation.

The other research direction is to try to improve network efficiency. Repeating messages is simple, but results in many collisions. It might be best to focus on improving medium access control. One may try this with the assistance of an infrastructure or stick to the ad-hoc setting as in this paper. For a scheme with infrastructure assistance see [21]. As mentioned before, ad-hoc MAC design to time separate contending nodes is difficult at such high vehicular traffic volumes. Some such schemes are discussed in section III.

II. PROBLEM FORMULATION

This section is divided into two subsections. Subsection II-A bounds the amount of data that could be generated by CASS. Subsection II-B describes the QoS model.

A. Bounding CASS Data Traffic

Table I summarizes this subsection. The numbers are based on estimates in [6], [40], and the following analysis.

Message rate Interval (messages/msec)	1/50 - 1/500	
Packet Size (Bytes)	100 - 400	
Message Range (meter)	50-300	
Average Inter-Vehicle Distance (meters/vehicle)	10 (jammed)	30 (maximum flow)
Lane Number	4, 8	

TABLE I
CASS DATA TRAFFIC BOUNDS

Safety messages are expected to encode content like position, speed, heading, turn signal status, electronic brake lights, “I am stopped in the middle of the road”, etc. For further details see [6], [40], [12]. Liability considerations suggest that one vehicle will probably not send commands to another.

The offered load depends on the safety message rate, message size, and vehicular traffic density. Since communication is wireless, the load also depends on the distance the message has to be propagated since this will determine transmission and interference power.

The message rate numbers are estimated from our own experimental build and the rate numbers in [6]. The rate estimates in [6] lie between 1 and 10 Hz. The experimental data from our own CASS build shows that if a vehicle transmits its motion state (position, speed, and heading data) every 50 msec the receiving vehicles are able to track the motion of the sender smoothly. At 90 mph (40 meters/sec) a vehicle moves 2 meters in 50 msec in the longitudinal direction. This level of precision is adequate for collision warning applications. Thus a receiving rate greater than 1/50 msec is not required. On the other hand, broadcasting once every 500 msec is probably too slow because driver reaction time can be as small as 500 msec [25]. Thus if information is delayed 500 msec, the driver may see the threat before the on-board active safety system. Thus our analyses assume messages are generated by each vehicle with a rate between 1/50 and 1/500 msec.

In our analyses we model the message generation process at each vehicle as Poisson with a rate as above. It is also assumed the message generation processes at different vehicles are independent. Thus the overall message generation process is also Poisson. For the reasons stated in the introduction, the safety message generation process at each vehicle may or may not be periodic. The Poisson process is a good approximation for the superposition of large number of independent periodic processes with the same interval and random starting time [14].

The independence may not be exactly true. For example, if a vehicle brakes hard and transmits a message, following vehicles might brake hard and transmit similar messages. However, these correlations will occur on the timescales of vehicle motion, i.e., in hundreds of milliseconds, making them insignificant on the timescales of communication where short safety messages are transmitted in microseconds. Thus we use the independence assumption. To actually figure out any correlations we would have to design and model the active safety applications. This would involve making more assumptions than made in this section to proceed with an analysis of the networking problem. Since CASS is still an early concept, these assumptions may or may not survive future developments in this area.

The SAE J1746 standard encodes vehicle location and class 2 bus data in less than a hundred bytes [5]. The NTCIP hazard codes encode vehicle hazard information in 5 bytes [24]. Our CASS build encodes vehicle motion data in a total of 160 bytes. Based on these documents it should be possible to keep messages sizes between 100 and 400 bytes, including about 80 bytes for standard network protocol headers. The lower limit of 100 bytes would require header and data compression. We do not know if this is possible. As a nominal value we pick 250 bytes. This would provide 170 bytes for the location and motion information of the sending vehicle and 80 bytes for its network headers. To be conservative the upper limit is chosen to be 400 bytes. These limits are consistent with those derived by VSCC [6] and other efforts [40].

Broadcast ranges should lie between 50 and 300 meters. When a vehicle transmits its safety message it does so to inform oncoming vehicles of its state of motion. Oncoming vehicles that are close need to be told immediately. To make data transport economical, oncoming vehicles that are far away should be told when they are closer. The distinction between near and far can be made precise by thinking of the message as having a critical range. A vehicle should receive the message before it reaches the critical range. For example if a vehicle is stopped, it would like its message to reach oncoming vehicles at freeway speeds before they hit 250 meters to give them ample time to take evasive action. Hence we assume that a stopped vehicle message would be presented to the data transport service with a specified range of 300 meters. In general, the critical range number would depend on the content of the message and the message range would be a value greater than the critical range. For critical range numbers for other active safety applications targeting vehicles in the blind spot, conflicts at intersections, freeway merges, etc., see [6], [12], [23]. The 50 meter lower bound is derived from the vehicle density in a jammed lane. This is about 217 vehicles/lane/mile. It corresponds to about 5 meters between cars. A car itself is about 5 meters in length. This adds up to 10 meters. To cover the width of a multi-lane highway with its merge ramps, etc., we assume the minimum communication range will be 50 meters. The range numbers in [6] lie between 50 and 300 meters. We analyze the same interval. If the technology is 802.11a or DSRC, this kind of range could be covered in one hop. Hence our focus on single-hop design.

Finally, the total offered traffic level depends on the density of the vehicles generating the traffic. We have done our analysis

in a freeway setting. When a freeway lane is jammed there is a vehicle every 10 meters on average. This is the densest network. At maximum flow there is a vehicle every 30 meters on average in each lane. Evaluation is done at the jammed and maximum flow conditions. At other flow levels the vehicular density is less and the QoS will be better. The total number of vehicles depends on the number of lanes as well. The 4 to 8 lane range in the table spans the usual to larger freeways.

B. Quality of Service Measures

We recommend the application present each safety message to the network with a specified range. The network will then determine how to send the message, i.e., power, modulation, coding, timing, etc. The range specification will tell the network it should make a best effort to deliver the message to all vehicles within the message range and not expend resources trying to deliver the message beyond its specified range. As explained in the prior subsection, this is consistent with the way information is thought of in the active safety systems literature. Most safety messages have a critical range derived from safety considerations.

We also recommend the application present each safety message to the network with a specified lifetime. The lifetime specification will tell the network to make a best effort to deliver the message within its lifetime and direct resources away from the message once its lifetime expires. This is also consistent with the nature of information consumed by active safety systems. Since a safety message informs on the state of motion of its sender, it becomes obsolete. After some time the receiver needs to be updated with the new state of motion. In this sense, most messages belong to a stream with each message in the stream being obsoleted by its next message. Once a message is obsolete, the data transport service should not expend resources trying to deliver it.

The primary QoS measure is then the probability of reception or reception failure (loss). We define the probability of reception failure (PRF) as the probability a randomly chosen receiver at the message range fails to receive the message within the message lifetime.

We focus on PRF at the message range rather than within the message range because the interference experienced by a receiver is larger when it is further from the transmitter. Since we are only trying to transport the message to receivers within the message range, the worst case PRF will generally be experienced by the receiver at the message range. In our simulations, we actually compute the PRF at receivers within an annulus of width 10 meters about the message range. This is to get a sample large enough to estimate a probability.

In our evaluations we assume the lifetime is the inverse of the rate. In general these two parameters may be different and our protocol design permits it to be so. We use this simplification to reduce the number of dimensions to be searched when evaluating the design. Table I shows five dimensions. In addition there is the number of repetitions, modulation, and coding making a total of eight dimensions determining PRF. When a message belongs to a periodic message stream, the lifetime should be the inverse of the message rate. The streams in our simulations are Poisson. The exact inter-arrival time between each message and its next one might be the message lifetime. If so, the average of the lifetimes would be the inverse of the rate of the Poisson process. To simplify computation, we give each message a lifetime equal to the inverse of the rate of the process.

We also pay attention to the channel busy time, i.e., if two protocols deliver messages with the same PRF but the channel busy time of one is lower than the other, we consider the one with lower CBT better. For a given time period T in the control channel, let T_{safety} be the total length of the time periods within T that is occupied safety messages. Then we have the following definition:

Definition 1: The channel busy time of a network is defined by:

$$CBT \triangleq \frac{T_{safety}}{T}$$

III. LITERATURE REVIEW AND RELATED TECHNOLOGIES

We do not use TDMA, FDMA, or CDMA because it is difficult to dynamically allocate slots, codes, or channels without centralized control. We base our designs on random access. ALOHA [7] and CSMA [31] are the earliest studied random access protocols. MACA [18], MACAW [10], FAMA and its variants [15] all use the Request-To-Send/Clear-To-Send (RTS/CTS) scheme. Our communication is broadcast. Therefore we cannot use RTS/CTS [38].

In the literature there are more complex protocols that support QoS. HIPERLAN/1 [9], “Black Burst” [29], and the Enhanced Distributed Coordination Function (EDCF) of IEEE 802.11e [36] [32] are all designed to reduce the access delay of time-sensitive communications. The HIPERLAN/1 and Black Burst approaches have no scheme to combat hidden terminals. EDCF-like priority access has been shown to successfully support a small number of vehicles conducting time-critical communication [32]. However, when the number of contending packets of high priority is large the probability of collision is high. This is the case in the CASS scenario. Therefore the authors of [32] point out “the proper design of repetition or multi-hop retransmission strategies represents an important aspect of future work for robustness and network stability of vehicular ad hoc networks”. Our protocols are based on repetitions.

In [19], the authors extend the RTS/CTS scheme to request-to-broadcast/clear-to-broadcast (RTB/CTB), and combine it with the “Black Burst” approach to support reliable broadcast. However, their design objective is to propagate one broadcast message

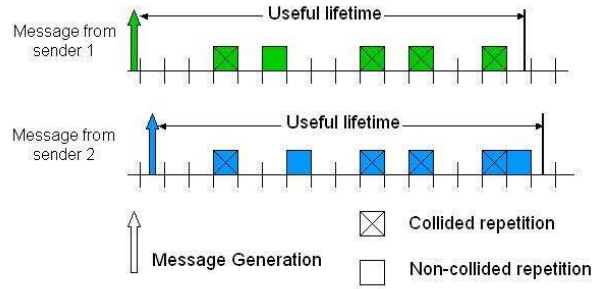


Fig. 2. The Concept of Repetitive Transmission

to a wide area in a short time. Our protocols try to accommodate frequent broadcast within a small area by multiple vehicles efficiently.

The authors of [39] have conducted detailed simulations of the DSRC physical layer and develop a simulation testbed for a DSRC vehicular ad hoc network. Their results reveal that 802.11 DCF will need further enhancement to achieve satisfactory performance on both latency and throughput. This paper proposes one such enhancement.

Reference [27] reviews the existing variants of the 802.11 DCF to support QoS. Its authors conclude the design of a mechanism to provide predictable QoS in an 802.11 network is still an open problem. We use a different definition of QoS. Reference [41] gives an overview of DSRC applications and assesses the characteristics of the IEEE 802.11 MAC and PHY layers in this context. Again, they anticipate that the current 802.11 specifications will need to be suitably enhanced to meet the QoS requirements of DSRC applications.

Cellular networks achieve time sensitive communication to vehicles moving at high speeds. However, this is accomplished with the aid of base stations. Here we stay ad-hoc to enable communications for vehicle safety applications without requiring an extensive infrastructure roll-out.

IV. MAC EXTENSION DESIGN

The objective of MAC extension design is to maximize the probability (minimize the PRF) a safety message is received at all vehicles within the message range within the message lifetime. The strategy explored here is to repeat the message a certain number of times within its lifetime. We choose the transmission power for each repetition to combat thermal noise at a receiver located at the message range.

Intuition suggests that as a message is repeated more than once the PRF may go down. However, if it is repeated too many times, collisions will rise and the PRF will go up. Thus there should be

an optimal number of repetitions. Section V presents a mathematical model to make this intuition precise and section VII shows it by simulation. We explore six variations on the repetition idea. We examine synchronous and

asynchronous designs, repetition with and without carrier sensing, fixed number and p-persistent repetition. Interestingly, enough the performance analysis in section VII shows that one of the asynchronous design with carrier sensing is able to match the PRF of the synchronous protocols. This is convenient because synchronizing MAC clocks across all vehicles would require some sort of infrastructure. The asynchronous designs are more ad-hoc. Moreover the winning design turns out to be the one easily overlaid on the 802.11 DCF.

We eschew reliability by RTS/CTS, or ARQ protocols. These require unicast communication and achieve reliability by receiver feedback. The sender needs to learn the network addresses of its receivers. When there are many receivers or the network is highly mobile, meaning the set of receivers can change a lot, learning identities may itself require significant communication. Therefore we have chosen to evaluate ways to enhance reliability without receiver feedback.

Figure 2 is an illustration of the idea of repetitive transmission. It shows two transmitters within interference range of one receiver each generating a message at the same time. Every repetition of the message is a new packet. At each transmitter the protocol evenly divides the message lifetime (τ) into $n = \lfloor \frac{\tau}{t_{trans}} \rfloor$ slots, where $\lfloor x \rfloor$ is the largest integer not greater than x , τ is the lifetime, and t_{trans} is the time needed to transmit one repetition. It is the slot duration. We randomly pick any k ($1 \leq k \leq n$) slots to repetitively transmit the message. According to the definition of the PRF discussed in section II, if any one or more of the packets corresponding to the message are received by that receiver without collision at a given receiver, the message is received within its useful lifetime and is considered successful. On the other hand, the message fails at the receiver if all its repetitions are lost due to collisions.

Our protocol is an overlay on the standard MAC like ALOHA [7] or Carrier Sensing [31]. We call this overlay the MAC extension layer. It is designed to lie between the Logical Link Control layer (IEEE 802.2) and the standard MAC layer. Its role is to generate and remove repetitions. The state machine of the MAC extension layer is shown in Figure 3. We have implemented it in NS-2. Upon receiving a message from the LLC, the MAC Extension transits from the IDLE to the REPETITION GENERATION state. In this state, the system selects the k repetition slots and creates a Packet Event Queue. Each repetition is an event with a slot number. All these events ordered by slot numbers constitute the Packet Event Queue.

Once the queue is formed, the system transits back to the IDLE state. Whenever a packet event expires, the MAC extension transits to the DISPATCH state and sends the packet down to the MAC. The system then transits back to IDLE. Whenever the MAC Extension receives a packet from the MAC, the system transits from the IDLE to the REPETITION REMOVAL state. If the message ID in this packet has not been seen before, it is from a new message, and the new message is passed up to the LLC. If the message ID in this packet has been seen before, the packet is eliminated.

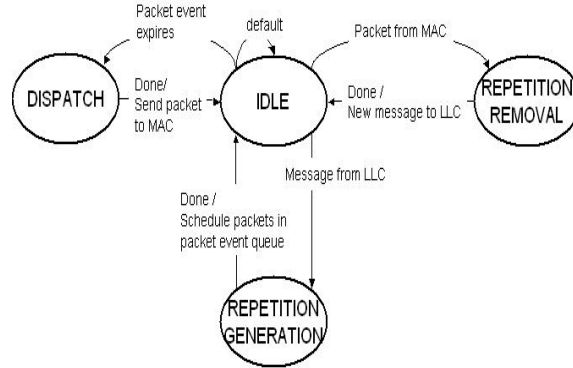


Fig. 3. MAC Extension Layer State Machine

The following are different protocols designed and evaluated by us. They fit the same MAC extension layer basically differing in the algorithm used in the *Repetition Generation State*. We slot the time locally at each radio. All our protocols can be classified as either synchronous or asynchronous. The synchronous protocols slot time to a global clock like in slotted ALOHA [7]. A local slot in each radio starts at the beginning of one global slot of the same size. Our asynchronous protocols do not globally slot time.

1) Asynchronous Fixed Repetition (AFR)

AFR is configured by setting the number of repetitions k . The protocol randomly selects k distinct slots among the total n slots in the lifetime. The radio does not listen to the channel (i.e. perform carrier sensing) before it sends a packet with AFR. The protocol is called “fixed” because the packet is always repeated a fixed number of times, i.e., k .

2) Asynchronous p-persistent Repetition (APR)

The p-persistent repetition protocol determines whether to transmit a packet in each of the n slots in the lifetime with probability $\frac{k}{n}$, where k is again a configuration parameter of the protocol. The average number of repetitions of a message is k . However, for each realization the exact number of repetitions is different. Like 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 slots in all the nodes are synchronized to a global clock.

4) Synchronous p-persistent Repetition (SPR)

The SPR protocol is the same as the APR protocol except that all the slots in all the nodes are synchronized to a global clock.

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

AFR-CS has its own MAC shown in Figure 4. AFR-CS generates repetitions in the same way as the AFR protocol. Whenever a packet is passed down from the MAC Extension, MAC transitions from the IDLE to the CARRIER SENSING state. In the CARRIER SENSING state, the system checks the channel status using carrier sensing [31]. If the channel is busy, the system drops the packet and transits back to the MAC IDLE state. If the channel is idle, the system transits to the MAC TX state, and passes the packet down to the physical layer (PHY). It then transits back to the MAC IDLE state. In MAC IDLE, if PHY sends a packet up, the system transits to the MAC RX state and checks the integrity of the packet. If the packet is corrupted, it is dropped and the system transits back to the MAC IDLE state. Otherwise, the packet is passed up to the MAC Extension layer, and the system transits back to the MAC IDLE state.

6) Asynchronous p-persistent Repetition with Carrier Sensing (APR-CS)

This is similar to AFR-CS except that the slots for message repetitions are selected in the p-persistent manner mimicking APR.

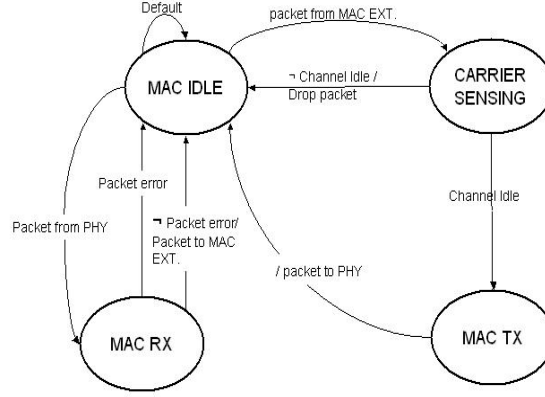


Fig. 4. MAC Layer State Machine of the AFR-CS protocol

V. MATHEMATICAL ANALYSIS

For the SPR and APR protocols we have developed mathematical expressions for the probability of reception failure (PRF). These expressions can be evaluated using Matlab. The expressions provide a simple way of exploring the relationship between PRF and design parameters like modulation, coding, power, and the number of repetitions.

We assume the message generation process is Poisson. We further assume the message generation processes of different vehicles are independent. Then the overall message generation process of all vehicles within interference range of any receiver is also Poisson [14]. However the network traffic is composed of the repetitions of the messages. This is not Poisson. For example, in Figure 2, the process of the arrows is Poisson, but that of the rectangles is not. Hence our analysis is different from others in the literature such as [11] and [31].

Table II lists the notation used in the mathematical analysis. We choose k and n such that $k/n = p$ when modeling a p -persistent protocol.

TABLE II
NOTATIONS IN PROTOCOL ANALYSIS

n	Maximum possible number of repetitions in lifetime, or total number of slots
k	Average number of repetitions for a message
p_j	The j th repetition of a message
S_j	Event that the p_j is successful at a randomly chosen receiver
t_j	The instant that the j th repetition starts
τ	Lifetime of a message
T_j	The event that there is at least one interfering message generated in $(t_j - \tau, t_j]$
λ	The rate of message generation at each individual node
m	Total number of interfering nodes around a receiver
S	The event that at least one of the repetitions succeeds within the lifetime at a randomly chosen receiver at the message range. Probability of $\neg S$ is the PRF.

The main results are Theorem 8 for SPR and Theorem 9 for APR. These give tight upper and lower bounds on PRF.

The number of interferers is critical to the PRF. As depicted in Figure 5, car A is transmitting to all the cars within its communication range, which is represented by the solid circle in the figure. Car B is one of the targeted receivers. Cars within B's interference range can interfere with the reception of A's transmission at B. The interference range is represented by the dashed circle in the figure. For example, when car C and car A transmit at the same time, they will interfere with each other at B. However car D is too far to interfere at B with the message of car A. The interference range depends on the transmitter-receiver distance, the message range, modulation and code rate. The procedure to calculate the interference range is given in Appendix B.

For a given transmitter/receiver pair, once the interference range is obtained, the number of interferers m is calculated by:

$$m = \frac{2 \cdot \text{Interference Range}}{\text{Meters per Vehicle}} \cdot \text{Lane number} \quad (1)$$

where meters per vehicle is the reciprocal of vehicle traffic density. The equation is a good approximation when the interference range is much larger than the lane width.

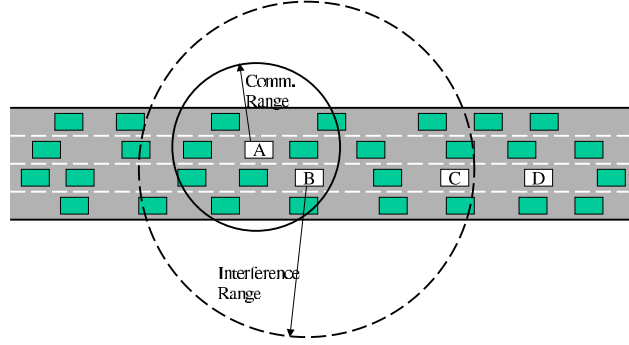


Fig. 5. Interference Range and Communication Range

1) *PRF: SPR protocol*: We prove the main result, Theorem 8, utilizing a series of lemmas. Lemma 2 and Lemma 3 lower bound the PRF.

Lemma 2: PRF for One Single Repetition in the SPR Protocol

For all $1 \leq j \leq k \leq n$, the PRF of p_j at any randomly chosen receiver is given by

$$P(\neg S_j) = 1 - e^{-m\lambda\tau\frac{k}{n}}, \quad (2)$$

Proof: There are two methods to prove this lemma. The first one is as follows.

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 a time period of length τ after the message's generation, these l messages are all the messages whose repetitions could interfere with repetition p_j . The probability that any one of the l messages selects the slot occupied by p_j (to transmit its own repetition) is $\frac{k}{n}$. Repetition 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 messages are independent and the total message generation process is Poisson. Therefore $P(\neg S_j) = 1 - P(S_j) = 1 - e^{-m\lambda\tau\frac{k}{n}}$

We can also prove the lemma 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 messages define 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 the 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. [14]), 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

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

Lemma 3: Lower Bound on the PRF for Multiple Repetitions in the SPR Protocol

Suppose p_1, p_2, \dots, p_r are any r repetitions transmitted for one message, then the probability of failure of all of them is greater than the product of the probability of failure of each one of them. Formally,

$$P(\neg S_1 \wedge \dots \wedge \neg S_r) > \prod_{j=1}^r P(\neg S_j) = (1 - e^{-m\lambda \tau \frac{k}{n}})^r, \forall 1 \leq r \leq k \leq n \quad (3)$$

Proof: We prove using induction, starting with the base case.

For $k = 2$, we need to prove that for any $i, j, 1 \leq i, j \leq n$

$$P(\neg S_i \wedge \neg S_j) > P(\neg S_i)P(\neg S_j)$$

First observe

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

Lemma 2 states

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

Next we analyze $P(S_i \wedge S_j)$.

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 interfere with messages generated in $(t_i - \tau, t_i]$ only, and p_j with 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 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 collide. With the same assumptions as used in the proof of lemma 2, we have

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

where the last equation comes from lemma 2.

Therefore

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

The above inequality holds for all $i, j, 1 \leq i, j \leq n$. Since order does not matter in equation (3), we can arbitrarily let $p_1 = p_i$ and $p_2 = p_j$. The lemma is thus proved for the case of $r = 2$.

Next we prove the induction step.

Assume equation (3) holds for all of j satisfying $1 < j \leq r - 1 \leq n - 1$. Then we have

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

Let t_i be the starting time of repetition p_i for any $1 \leq i \leq r$. Since the order does not matter in equation (3), we can always rearrange the repetitions such that $t_1 < t_2 < \dots < t_{r-1} < t_r$. Therefore we can assume this ordering without loss of generality.

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

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

In the above derivation, the second equation is obtained because the slots are chosen independently. Therefore the 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. $P(B_i | \neg S_r) \geq P(B_i)$ because when packet p_r fails, there are surely some other messages generated in $(t_r - \tau, t_r]$. Therefore it is more probable there are interfering messages in $(t_r - \tau, t_{r-1}]$ and thus in $(t_1 - \tau, t_{r-1}]$.

From the inequality above we have

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

The first inequality holds for the same reasons $P(B_i | \neg S_r) \geq P(B_i)$. Hence equation (3) also holds for r , and the lemma is proved. ■

Lemmas 4 through 7 provide the upper bound on the probability of reception failure. This turns out to be quite close to the lower bound. Plots show the bounds are pretty tight.

Lemma 4: The PRF of a single repetition p_j for the SPR protocol, conditioned on the event T_j , i.e. there is at least one other message generated in $(t_j - \tau, t_j]$, is as follows.

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

Proof: Following the same arguments as in the proof of Lemma 2, 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

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

■

From lemmas 2 and 4 we obtain the following.

Corollary 5:

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

Lemma 6: For all $1 \leq r \leq k \leq n$,

$$P(\neg S_r | \neg S_1 \wedge \dots \wedge \neg S_{r-1}) < P(\neg S_r | T_r) \quad (4)$$

where T_r is the event that there is at least one message generated in $(t_r - \tau, t_r]$.

Proof:

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

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 $(t_j, t_k]$, i.e., the lifetime period shared by the two repetitions.

■

Lemma 7: Upper-Bound on the PRF for Multiple Repetitions in the SPR Protocol

For all $1 \leq r \leq k \leq n$,

$$P(\neg S_1 \wedge \dots \wedge \neg S_r) < \prod_{j=1}^r P(\neg S_j | T_j) = (1 - e^{-m\lambda \tau \frac{k}{n}} + e^{-m\lambda \tau})^r \quad (5)$$

Proof: The inequality follows from the chain rule, Lemma 4, and Lemma 6.

■

Combining the bounds provided by Lemmas 3 and 7, we prove the main theorem as follows.

Theorem 8: Bounds on the PRF of the SPR Protocol

The PRF of the SPR protocol satisfies the following inequality.

$$\left(1 - \frac{k}{n} e^{-m\lambda \tau \frac{k}{n}}\right)^n < P(\neg S) < \left(1 - \frac{k}{n} e^{-m\lambda \tau \frac{k}{n}} + \frac{k}{n} e^{-m\lambda \tau}\right)^n \quad (6)$$

Proof:

Let the random variable K denote the total number of packets transmitted for a randomly chosen message. From lemmas 3 and 7, the PRF for the message conditioned on $K = r$ satisfies the following inequality.

$$\begin{aligned} & (1 - e^{-m\lambda \tau \frac{k}{n}})^r \\ & < P(\neg S | K = r) \end{aligned} \quad (7)$$

$$\begin{aligned} &= P(\neg S_1 \wedge \dots \wedge \neg S_r) \\ & < (1 - e^{-m\lambda \tau \frac{k}{n}} + e^{-m\lambda \tau})^r \end{aligned} \quad (8)$$

Now let p and q be defined as in equations (9) and (10) below.

$$p = (1 - e^{-m\lambda \tau \frac{k}{n}} + e^{-m\lambda \tau}) \quad (9)$$

$$q = (1 - e^{-m\lambda \tau \frac{k}{n}}) \quad (10)$$

Then equation (8) becomes

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

We show below the proof of the left-hand side of the inequality (6) for simplicity of presentation. The proof of right-hand side follows the same steps except for changing the direction of the inequality and replacing q with p .

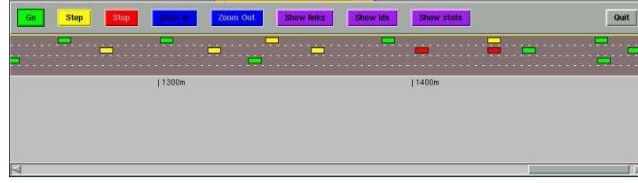


Fig. 6. A Typical Traffic Screen-shot of SHIFT

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

In the above $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. We applied the Binomial Theorem in the proof. The right hand side can be proved in exactly the same way. ■

2) *PRF: APR Protocol*: The analysis for APR protocol is similar to that of the SPR protocol. In APR, if a repetition is transmitted at time t , any other repetitions transmitted in the interval $[t - t_{trans}, t + t_{trans})$ can collide with it. The transmitted repetition is vulnerable in two slots in contrast to one in the SPR protocol. Remember t_{trans} is the time duration of a repetition.

Therefore for the repetition to be successful we require no other repetitions are transmitted in the two-slot interval. We have similar series of lemmas as for the PRF of the SPR protocol. They are listed in Appendix A. Using the lemmas we obtain the following theorem.

Theorem 9: Bounds on the PRF for the APR Protocol

The probability of reception failure at the receiver of one message for APR protocol satisfies the following inequality.

$$\begin{aligned}
 &\left(1 - \frac{k}{n} e^{-m\lambda\tau} \left[2\frac{k}{n} - \frac{k^2}{n^2}\right]\right)^n < P(\neg S) \\
 &< \left(1 - \frac{k}{n} e^{-m\lambda\tau} \left[2\frac{k}{n} - \frac{k^2}{n^2}\right] + \frac{k}{n} e^{-m\lambda\tau}\right)^n \tag{11}
 \end{aligned}$$

For both SPR and APR in the parameter range we are interested in (Table I), the upper and lower bounds are quite tight. This is because when the total transmission rate is high, i.e. $m\lambda \gg 1$,

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

In the rest of the paper we calculate using the right hand sides of (6) and (11). The corresponding plots for the left hand sides are not distinguishable at the scale, for example, of figure 9.

VI. SIMULATOR DEVELOPMENT

We have developed a DSRC simulator to conduct the simulations. The simulator is based on two others, namely SHIFT [26] and NS-2 [3].

We use SHIFT to simulate highway vehicle traffic. SHIFT is a computer language developed by California PATH for simulating dynamic networks of hybrid automata and in particular the vehicle traffic system. It has implemented microscopic models for merging, lane changing, gap acceptance, vehicle following, etc. A detailed description of the vehicle traffic simulation appears in [35]. It uses the COSMODRIVE [30] cognitive model to model the human driver. This includes the Hoffmann model of range-rate perception [17]. Figure 6 is a screenshot of vehicle traffic as output by SHIFT.

We use NS-2 (abbreviation of Network Simulator) to simulate the wireless communication network. NS-2 is a discrete event simulator for networking research, with most popular protocols implemented at various OSI layers. We added our protocol on top of the 802.11 MAC. Our physical layer settings are such that the simulated communication takes place in a 5.9 GHz 802.11a DSRC channel rather than the usual 2.4 GHz 802.11b channel. The reception SINR thresholds for all the data rates supported by the radio are listed in Table III [22]. We use the wireless extension of NS-2 developed by the Monarch project [2]. We use the Friis free-space channel model for short TX/RX distances and the two-ray model for long distances [20]. The

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

TABLE III
SINR THRESHOLDS AND 802.11A TRANSMISSION RATES

Message Rate (messages/mesc)/Lifetime	100
Packet Size (Bytes)	170
Message Range (meter)	80
Average Inter-Vehicles Distance (meters/vehicles)	30
Lane Number	4

TABLE IV
NOMINAL PARAMETER VALUES

parameters in table V are also used in the simulator. They are set according to the IEEE 802.11a standard on the physical and MAC layers [4].

In the DSRC simulator we first simulate the vehicle traffic with SHIFT, then feed the generated trace file as the “node movement file” to NS-2. Thus the DSRC simulator is the standard NS-2 release plus

- SHIFT
- The radio model for 802.11a at 5.9 GHz
- The repetition protocols
- A different data structure that changes the run-time of NS-2 from quadratic to linear in the number of nodes. Figure 7 shows the run-time comparisons. This enhancement has enabled us to simulate networks with up to a thousand vehicles.

We simulate a highway segment of length 1.8 kilometers. The highway is straight and without entrances or exits. The maximum flow per lane is 2200 vehicle/hour. The simulation duration is 1 minute. In the nominal parameter setting summarized in Table IV, there are 240 vehicles on average at any given time on the highway. During a simulation there are $\frac{60}{0.1} \cdot (\frac{2200}{60} \cdot 4 + 240) \cdot \text{number of repetition}$ messages transmitted by the vehicles. For example, when the repetition number is 10, the sample size is 2.32 million messages. Since the highway we simulate has limited length, there is an edge effect, i.e., the nodes at the beginning of the highway have less interferers behind them, while those at the end of the highway have less interferers in front of them. To remove the edge effect, we do not include the edge node receivers when calculating the PRF statistics. When we calculate the PRF of the inner nodes, the interference from the edge nodes is considered. We simulate all the protocols proposed in section IV at all the parameter combinations listed in table I.

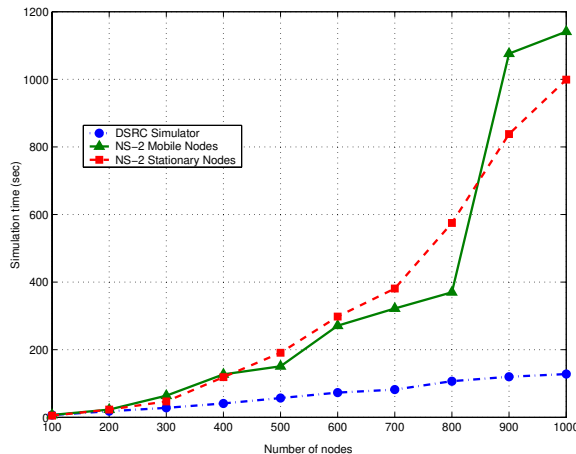


Fig. 7. Improvement on the Scalability of the DSRC Simulator over NS-2

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

TABLE V
OTHER SIMULATION PARAMETERS

VII. OPTIMIZING DESIGN

In this section we use the tools to establish the arguments about optimal operating points and find them at certain nominal vehicular traffic and safety data traffic levels. The optimal points are used to select the best protocol design. Subsection VII-A discusses PRF optimization by varying the number of repetitions. Subsection VII-B discusses minimizing PRF by varying modulation and coding. Subsection VII-C uses the analyses in these two subsections to pick a winning design from amongst the six variations in section IV. Subsection VII-D quantifies the probability of a burst of message losses since these are more detrimental to the receiver tracking the sender.

PRF depends on message rate, range, size, inter-vehicle spacing, number of lanes, number of repetitions, modulation, and code rate. Equations (6) and (11) in section V argue PRF is determined by the number of repetitions, transmission time, and the number of interferers. When the message lifetime is the inverse of the rate the $\lambda\tau$ product in the inequalities is 1. This suggests the eight dimensions determining PRF may be approximated by the three in (6) and (11).

Figure 8 shows a examination of part of this hypothesis by simulation. We keep transmission time fixed and vary the number of interferers and the number of repetitions. The simulations are of a mobile network. The vehicle headways are 10, 15, and 30 meters meaning the curves cover a jammed highway, one at maximum flow, and an intermediate flow level. Each curve in the figure is a plot of our two QoS measures for a particular set of values of the eight parameters. The different points on each curve correspond to different numbers of repetitions. Higher CBT points are higher repetition points. The message rate, size, modulation, and code rate are the same for all the curves in the figure. Message size, modulation and code rate determine transmission time. Thus the curves all have the same transmission time. The message range, number of lanes, and inter-vehicle spacing differ from curve to curve. These parameters together with the modulation and code rate determine the number of interferers. Observe that the curves for 70 and 75 interferers are close together as are the three curves for 113 interferers and the three for 151 interferers. This closeness substantiates our hypothesis that the number of interferers (one of three parameters in equations (6) and (11)) is a good indicator of average network performance along with transmission time and repetition number. This seems to be true even if the network is mobile. We use this reduction of several parameters to the number of interferers in several arguments in the following subsections.

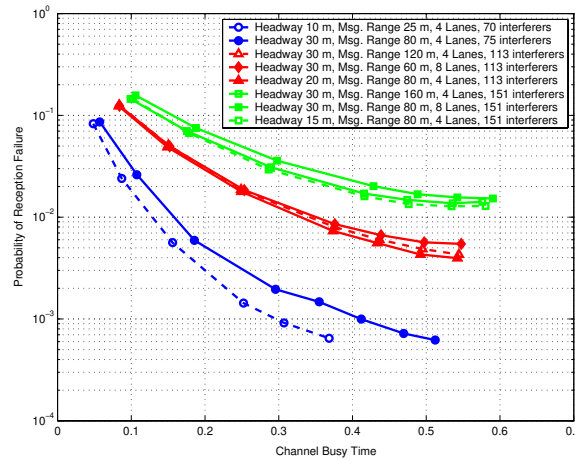


Fig. 8. Performance of AFR-CS Protocol as a Function of Interferer Number

A. Optimizing PRF by Repetition Number

Figure 9¹ is a plot of the PRF for the SPR and APR protocols. The curves labeled Analytical are generated using the right hand sides of inequalities (6) and (11), i.e., by stochastic analysis. The other two curves are obtained by simulation. Parameter values are as in Table IV. The number of interferers is 75.

The simulated PRF is a bit better than the PRF computed from the inequalities. Since the message generation process is Poisson the lifetimes of consecutive messages generated by the same vehicle could overlap. A repetition of a message can thus select the same transmission time slot as a repetition of a later message. The derivations of inequalities (6) and (11) assume the two repetitions will collide. On the other hand, in simulation the repetition of the latest message overwrites any contending repetitions from earlier messages, since this is more realistic. Therefore the PRF computed by simulation is better than the PRF computed using the inequalities. The close match between the two curves has been our way of validating the simulator.

The shape of the curves illustrates the intuition described in the introduction. As the number of repetitions is increased the PRF gets better up to a point. Thereafter there are too many collisions and the PRF gets worse. The shape of the curve is similar for other parameter values. There is an optimal number of repetitions.

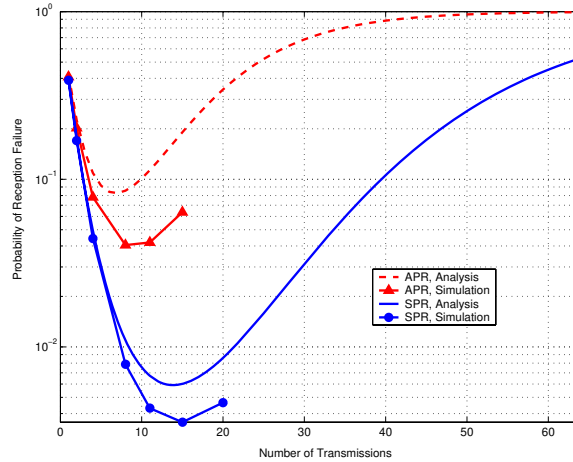


Fig. 9. Optimizing PRF by Repetition Number

Figures 13 and 14 show the other protocol designs exhibit similar behavior. The plots are obtained by simulation. Parameter values for figure 13 are as in table IV. Parameter values for figure 14 are in table X. This setting has a larger number of interferers.

The optimal number of repetitions depends on the message rate, range, vehicular traffic density, and packet transmission time. Figure 13 shows the optimal number of repetitions for the AFR-CS protocol is above 20 repetitions while figure 14 shows the optimal number to be about 15.

This suggests it may be worth designing to pick the number of repetitions adaptively in response to the offered load or other parameters. However, if one is willing to forgo a best effort and be satisfied with a specified level of performance it may be possible to pick one repetition number. We present data in section VIII showing how to pick one repetition number.

B. Optimizing Modulation and Coding

Here we examine the dependence of PRF on modulation and coding. The IEEE 802.11a standard uses Orthogonal Frequency Division Modulation. The channel is partitioned into 54 sub-channels, and data is coded, modulated and transmitted at 48 of the 54 sub-carriers. Error coding is convolutional. A given 802.11 transmission data rate corresponds to a modulation scheme and convolutional code rate. The 802.11a combinations and corresponding data rates are in table VI.

A modulation and code rate choice determine a data rate. Figure 10 shows the variation of PRF with data rate for the SFR protocol. The curves are obtained by plotting the right hand side of inequality (6) for the various data rates supported by 802.11. All other parameters are at the nominal setting in Table IV. A choice of data rate and message size determines transmission time. The ability to receive at a data rate is related to the Signal to Noise Ratio (SNR) at the receiver (see table III). Thus a data rate and message range determine transmission power. Transmission power and message range determine interference range and the number of interferers. Higher data rates reduce transmission time tending to improve PRF. Given a message range, a higher data rate means a higher transmission power. This implies higher interference range and a larger number of interferers. This reduces PRF. This suggests the existence of an optimal modulation and code rate given a message rate, range, size, and vehicular traffic density. The trade-off is more precisely captured by inequalities (6) and (11).

¹Read Number of Repetitions for Number of Transmissions in the following figures.

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 VI
TRANSMISSION RATE, MODULATION, AND CODING IN IEEE 802.11A

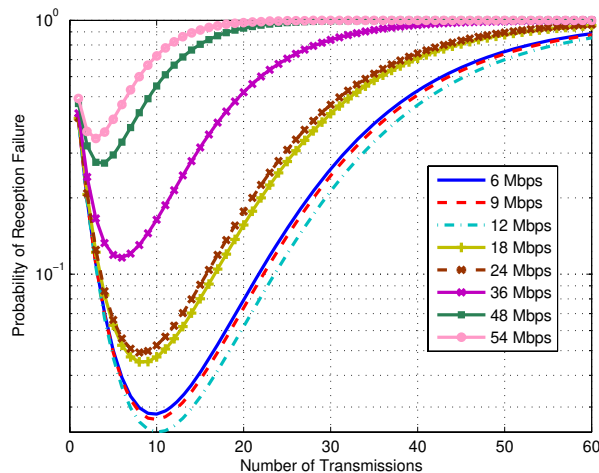


Fig. 10. PRF of SFR Protocol at Various Data Rates in the Nominal Setting: Analytical

The 12 Mbps data rate achieves a PRF near 1/100 at 10 repetitions (see figure 10). This is the best PRF. Through 6, 9, and 12, Mbps the PRF gets better. From 18 through 54 Mbps it gets worse. We also observe that the optimal repetition numbers are different at different data rates. Thus PRF should be jointly optimized over the repetition number and data rate dimensions.

Figure 11 shows the AFR-CS protocol also has an optimal data rate. This result is obtained by simulation. Parameter values are as in tables IV and V. The PRF shown for each data rate is that obtained after optimizing over the number of repetitions. The best data rate is 18 Mbps. Table VII shows the best data rate for the other protocol designs. This table is computed by simulation. For each protocol and each data rate we have run several simulations to find the optimal repetition number.

Table VIII shows the optimal data rate of the AFR-CS protocol at various communication ranges. The numbers are derived by simulation. Parameter values are as in tables IV and V.

Though PRF can vary over an order of magnitude with data rate, the optimal data rate appears quite insensitive to communication range. This is a surprising and useful fact. To ensure our finding is not a simulation error, we cross-checked it using our stochastic analysis. Table IX shows the optimal data rates as a function of the average number of interferers derived using the right hand side of inequality (6). Once again, the optimal data rate is quite insensitive to the average number of interferers. We are not sure how to explain this intuitively.

The insensitivity of the optimal data rate to interferer number may be useful. The optimal data rate might still be related

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

TABLE VII
OPTIMAL DATA RATE FOR VARIOUS PROTOCOLS IN THE NOMINAL SETTING

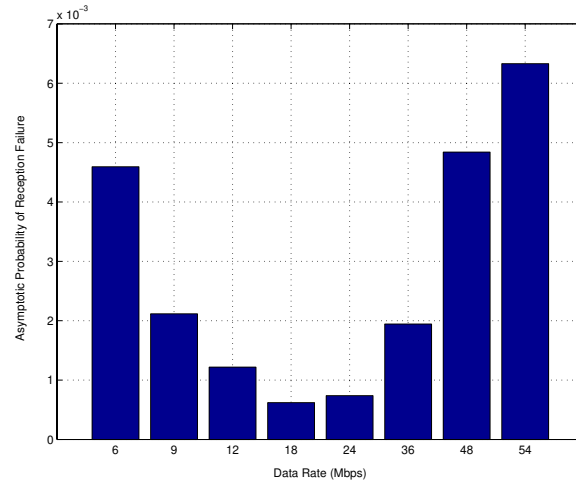


Fig. 11. PRF of AFR-CS Protocol at Various Data Rates in the Nominal Setting: Simulation

Communication Range (m)	Interferer Number	Optimal Data Rate (Mbps)
30	11	12
60	27	18
80	59	18
120	87	18
150	111	18
180	131	18
210	155	18
240	179	18

TABLE VIII

OPTIMAL DATA RATE OF AFR-CS AT VARIOUS COMMUNICATION RANGES: SIMULATION

to the message rate and average message size per vehicle. However, if it is not related to the number of interferers, it will not be related to the density of vehicular traffic. Thus one might choose the modulation and coding at which to execute CASS communications by estimating the average message rate and size per vehicle. There may be no need to adapt the rate dynamically to changing vehicular traffic conditions. At small numbers of interferers the optimal rate is different. However, in this regime the network is lightly loaded rendering the PRF acceptable even at a non-optimal data rate.

C. Choosing the Optimal Protocol

Figure 12 is a plot of CBT versus repetition number for some of the protocol designs for the parameter values in table IV. It shows CBT increases with the number of repetitions. Not surprisingly, the 802.11 DCF has small CBT since it does not repeat.

Figure 13 shows the performance of the protocols as a function of the number of repetitions. The curves are based on outputs from the simulator. CSMA parameters (e.g., DIFS) have been kept fixed at their 802.11 values. As discussed in subsection VII-B, there is an optimal data rate for each protocol given a particular set of message rate, range, or size values. The figure shows the PRF of each protocol at its optimal rate for the nominal parameter values.

Interferer Number	Optimal Data Rate (Mbps)
11	6
27	6
59	12
87	12
111	12
131	12
155	12
179	12

TABLE IX

OPTIMAL DATA RATE OF SFR AT VARIOUS INTERFERER NUMBERS: ANALYTICAL

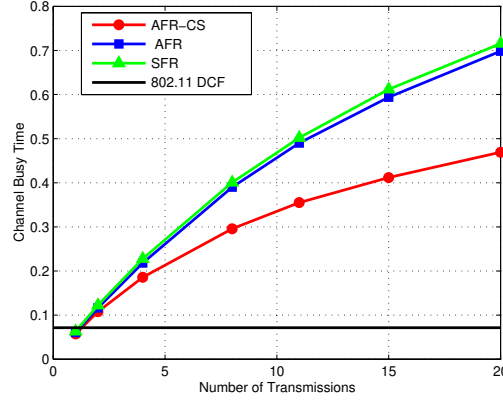


Fig. 12. Channel Busy Time for Fixed Repetition Protocols

Message Rate (messages/msec)	1/200
Packet Size (Bytes)	170
Message Range (meter)	150
Average Inter-Vehicular Distance (meters/vehicle)	30
Lane Number	4
Number of Interferers	150

TABLE X
PARAMETER VALUES CORRESPONDING TO A LARGER COMMUNICATION RANGE

The best protocols in terms of PRF are AFR-CS and SFR. SFR would require a clock synchronization infrastructure. Therefore we prefer the AFR-CS protocol. The AFR-CS protocol also improves PRF relative to 802.11a DCF by one order of magnitude. This shows optimizing repetition, modulation and coding, significantly improves network performance.

Figure 14 shows the simulation performance of all the protocols for another parameter combination within the ranges in table I. Parameters values are as in table X. The communication range is twice the nominal value. This increases the number of interferers. On the other hand the message generation rate is lower. The performance numbers in Figure 14 indicate the same protocol preferences as figure 13. The advantage of the AFR-CS and SFR protocols over 802.11 DCF remains. We have repeated this exercise for other parameter combinations consistent table I and have confirmed the superior PRF of the AFR-CS protocol.

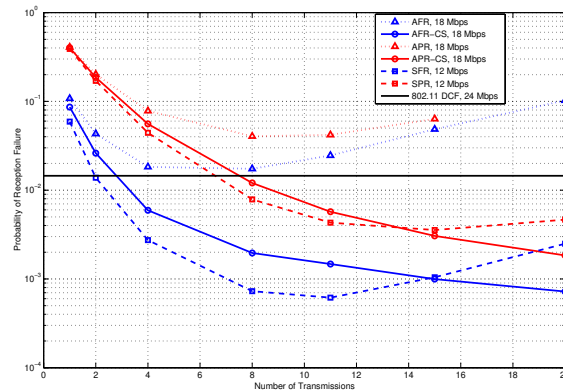


Fig. 13. PRF for Various Protocols with Nominal Parameter Values

From figures like 13 and 14 we conclude that for the same repetition methods (i.e. fixed repetition or p-persistent repetition), the synchronous protocols outperform the asynchronous protocols. The synchronous protocols eliminate the partial overlap of packets transmitted by different nodes. This observation is consistent with prior results on slotted and non-slotted ALOHA [28]. For the same repetition method, a CSMA protocol is better than a non-CSMA protocol. CSMA nodes listen before transmitting. Therefore many potential collisions are avoided. The reception failures for CSMA protocols are mostly due to hidden terminals.

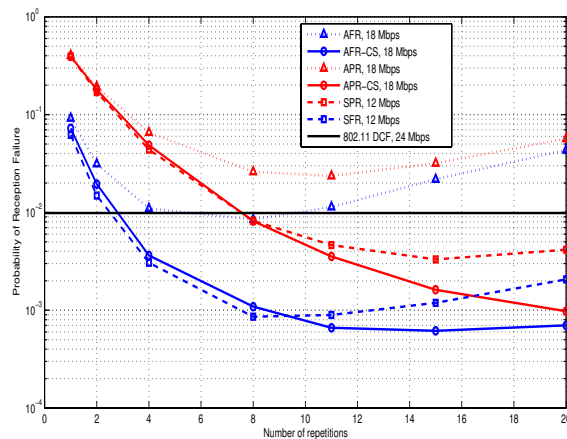


Fig. 14. PRF for Various Protocols with More Interfering Vehicles (table X)

The fixed repetition protocols outperform the corresponding p-persistent protocols. The fixed repetition protocols are better at maintaining the number of repetitions for each message, i.e. there is less variation between the actual number of repetitions of each message and the expected number of repetitions. In figures 13 And 14 one might wonder why the PRF of AFR-CS keeps decreasing as the number of repetitions increases. We have checked that as we keep increasing the number of repetitions the PRF of the AFR-CS protocol does eventually increase as observed for other protocols, though at very large numbers of repetitions.

The Channel Busy Time could be viewed as a measure of the fraction of channel capacity left over for messages generated by non-safety applications. As the repetition number goes up so should CBT. Thus there should be an inverse relationship between PRF and CBT up to the optimal repetition number. The curves in figure 15 show this inverse relationship. The number of repetitions increases from left to right for each curve. As the QoS to safety messages goes up, that of other non-safety applications would come down. Therefore these curves are a good way of evaluating the performance of our protocols. Some of the participants in the DSRC standards process have proposed safety message share the DSRC control channel with other non-safety messages. These people would prefer designs with low CBT as determined by the safety message traffic alone.

Figure 15 compares the two best protocols, i.e., SFR and AFR-CS. Parameter values are as in the nominal case. The figure indicates that up to a CBT of 50% the performance of AFR-CS and SFR are indeed quite close. As expected, at the same PRF the SFR protocol has better CBT than the AFR-CS protocol. Since SFR and AFR-CS outperform other protocols in both PRF and CBT, and AFR-CS should be easier to deploy than SFR , our design choice is AFR-CS.

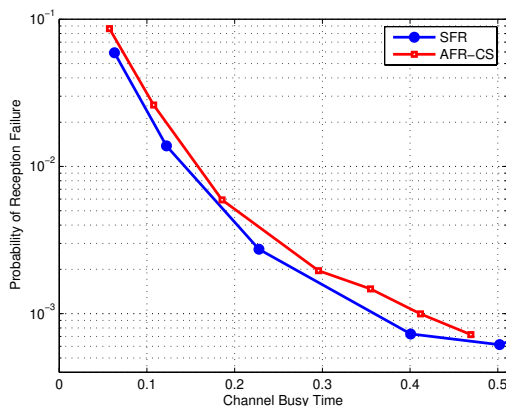


Fig. 15. Comparison of AFR-CS and SFR Protocols with Nominal Parameter Values

Figures 16, 17 and 18 respectively show the sensitivity of PRF and CBT to message range, rate, and packet sizes. In each figure, all parameter values other than the one being varied, are as in table IV. The protocol is AFR-CS.

Not surprisingly, figure 16 shows an increase in communication range degrades the performance of the protocol. 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 IV and data rate being 18 Mbps, the maximum allowed communication range should lie between 120 m and

180 m. Observing Figure 17 and 18, we see smaller message interval and larger packet size degrade the protocol performance. These results are also as expected.

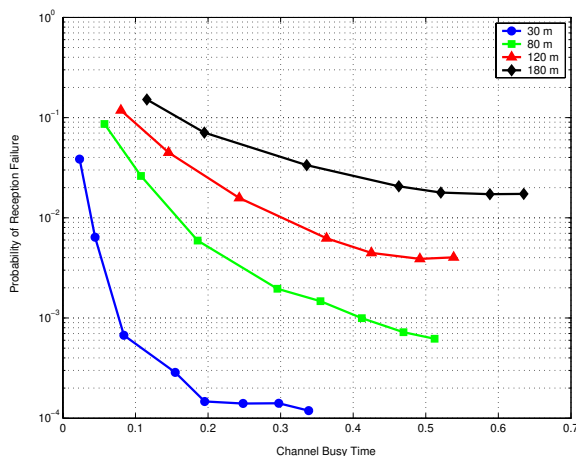


Fig. 16. AFR-CS PRF for Various Communication Ranges

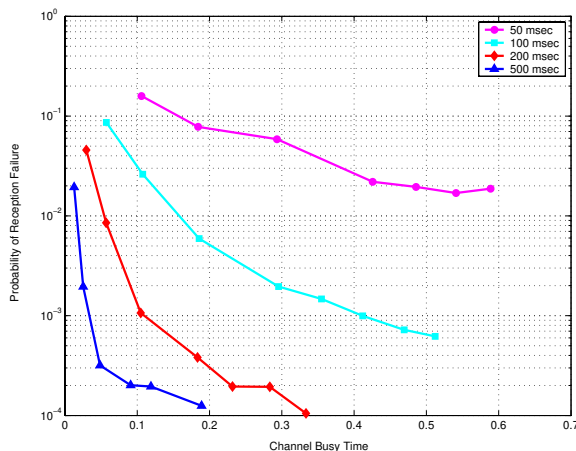


Fig. 17. AFR-CS PRF for Various Message Generation Intervals

D. Bursts of Reception Failures

Figure 19 shows the probabilities of bursts of lost packets of different lengths. Parameter values are nominal (table IV). The burst probabilities are small. This is partly due to the memoryless feature of the channel in simulation. The probability for a receiver seeing two or more consecutive failures is smaller than 0.001. This is good for a receiver tracking a sender.

VIII. FEASIBILITY ANALYSIS

In this section we use the simulation data to assess the feasibility of the communications component of CASS using 802.11a technology in the DSRC spectrum.

The communication load is determined by the parameters in table I, i.e., message rate, size, range, inter-vehicle spacing, and number of lanes. To assess feasibility we sample the parameter space in the table. For each sample, we run several simulations with the AFR-CS design but different numbers of repetitions and transmission data rate. We record the PRF and CBT number for each simulation. This results in 600 gigabyte of data.

Given a PRF and CBT requirement we can partition the parameter space into a feasible part, i.e., one that meets the requirement, and an infeasible part, i.e., one that does not. To visualize this partition effectively, we reduce message range, inter-vehicle spacing, and number of lanes, to the corresponding number of interferers.

Figure 20 is a feasibility figure. This partition is based on requiring PRF to be less than 1/100 and CBT to be less than 50%. One can see, the 200 msec message rate, 250 byte message, with 140 interferers is feasible. This corresponds to a 4 lane highway at capacity (2200 vehicles/hour/lane) with a message range of 150 meters. Likewise the 10 meter headway (jammed road), 4 lanes, and 50 meter message range is also feasible since it has the same interferer number.

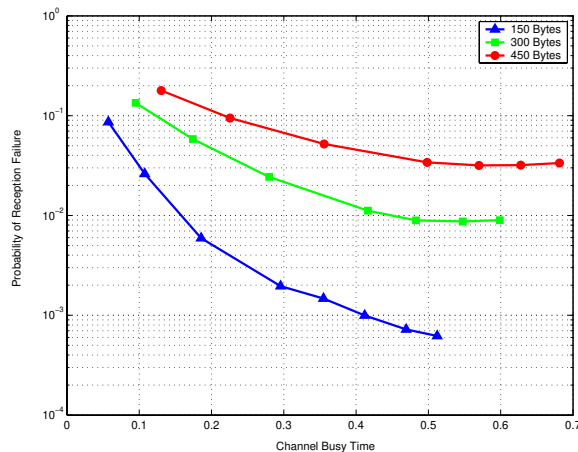


Fig. 18. AFR-CS PRF for Various Packet Sizes

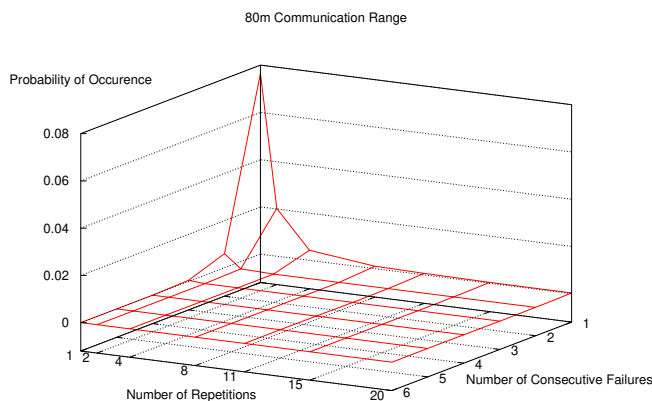


Fig. 19. Probability of Message Failure Bursts: AFR-CS

Figure 21 shows the feasibility regions when the PRF is required to be lower than 0.001, and the CBT lower than 50%. The higher PRF requirement makes feasibility regions smaller than in Figure 20. For example, in Figure 20, the 200 msec message rate, 250 byte message is feasible at 140 interferers, however in figure 21 the same message rate and message size combination is feasible only when there are less than 30 interferers.

Table XI shows the minimum number of repetitions required along the lines separating the feasible and infeasible regions in figure 20. For example, the first line of table XI asserts that for 100 byte packets, sent every 200 msec, with 198 interferers, at least 4 repetitions are required of each message to achieve a PRF less than or equal to 1/100. One can see the minimum number of repetitions required to maintain a PRF lesser than or equal to 1/100 varies between 4 and 11. This is not a large range. Moreover we have confirmed that the optimal number of repetitions in each case is greater than the number of repetitions in table XI. The optimal number is greater than or equal to 11 in each case. Thus if we were to set the number of repetitions at 11 for each combination of message size, rate, and number of interferers, the PRF would still be 1/100 or better. This suggests it may not be necessary to adaptively set the number of repetitions. Recall we showed in subsection VII-B that the optimal data rate is also not sensitive to the number of interferers and may not have to be set adaptively either.

IX. CONCLUSION

Our work has been motivated by FCCs allocation of spectrum for DSRC and the growing interest in using it for active safety systems, i.e. CASS. We have investigated the communications component of Cooperative Active Safety Systems. By investigating the active safety systems literature, we characterized its communication requirements and proposed a QoS model. Based on this analysis we formulated the communication problem as a single-hop broadcast problem to be solved in an ad-hoc fashion.

Based on a survey of the literature on wireless ad-hoc medium access protocols and our understanding of the mobility and volume of freeway vehicular traffic, we thought it best to try a simple, robust strategy based on random access protocols. The

Packet Size	No. of interferers	1/Message rate	Min. No. of Repetitions
100	198	200	4
100	141	100	11
100	114	100	8
100	57	50	8
250	198	400	4
250	170	200	8
250	141	200	8
250	76	100	11
250	57	100	8
250	29	50	8
400	114	200	11
400	29	100	4

TABLE XI
MINIMUM NUMBER OF REPETITIONS FOR PRF 1/100

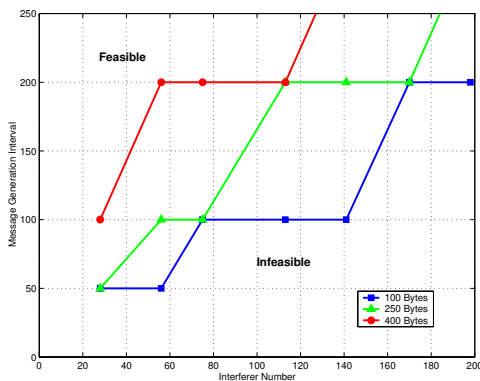


Fig. 20. Feasibility Regions for < 0.01 Probability of Reception Failure and $< 50\%$ CBT

strategy is to repeat each message within its lifetime with enough power to overcome thermal noise at its range at the chosen transmission data rate. We specified our design as a state machine that can be overlaid on IEEE 802.11 DCF.

We then developed a stochastic model and a simulator to evaluate the QoS delivered by our design. The evaluation is set in the context of the DSRC spectrum. The findings indicate a need for further research. If the community is to stick with the simple networking design in this paper, CASS has to be designed to work with a message loss rate between $1/100$ and $1/1000$. Even at this loss rate, if message sizes are about 250 bytes and the highway is at maximum flow, the average message rate should be less than $1/200$ msec, and the average message range 150 meters or below. This rate is too slow in some settings, e.g., in a hard braking situation. We show in [12] the delay in this situation should be 50 msec or less. Likewise this range is also too small in some situations, e.g., braking to avoid a stopped vehicle on a freeway. However, since these are rare events, further design of CASS might show it is possible to cover these hazardous situations while keeping average rates and ranges below these limits.

We also showed when the highway is jammed the average range needs to be 50 meters or less. Thus the same message

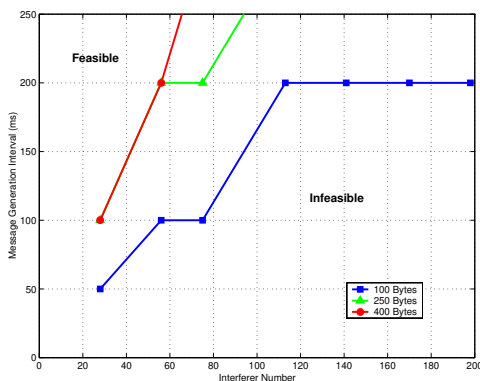


Fig. 21. Feasibility Regions for < 0.001 Probability of Reception Failure and $< 50\%$ CBT

range and transmission power will not work across all traffic conditions. Fortunately on jammed highways vehicles are closer and slower suggesting the CASS application may not need to sent its messages too far. Clearly, research is required to develop some kind of traffic adaptive power or range control scheme.

It is also worth doing further research on communication designs that might utilize the channel more efficiently. This suggests schemes that time-separate contending nodes better than CSMA. This is a well established problem in the literature. Better schemes are known for static or quasi-static networks. For vehicular traffic networks one might be able to do better by using infrastructure support or some new technology like GPS clocks that is not conventionally used in wireless medium access control.

A PRF of 1/100 is a higher loss rate than accepted in many networks. Since CASS is a safety application research is needed to verify such a loss rate is not unacceptably high.

ACKNOWLEDGMENT

The authors thank Dr. Ken Laberteaux of Toyota Technical Center U.S.A., Inc., Mr. Daniel Jiang of Daimler Chrysler RTNA and Dr. Hariharan Krishnan of General Motors Research and Development for valuable discussions. We thank Mr. Joel VanderWerf for help on vehicle traffic simulations, and Mr. Marc Torrent Moreno for help on NS-2 simulations.

REFERENCES

- [1] Dedicated Short Range Communications (DSRC) home. <http://www.learmstrong.com/dsrc/dsrchomeset.htm>.
- [2] Monarch project. <http://www.monarch.cs.cmu.edu/cmu-ns.html>.
- [3] The network simulator: NS-2. <http://www.isi.edu/nsnam/ns>.
- [4] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. *IEEE Standard 802.11a-1999*, 1999.
- [5] ISP-vehicle location referencing standard. *SAE Standard J1746*, July 2001.
- [6] Vehicle safety communications project: Final report. submitted to nhtsa and fhwa in response to cooperative agreement number dtfh61-01-x-001. January 2005.
- [7] N. Abramson. The throughput of packet broadcasting channels. *IEEE Trans. Comm.*, COM-25:117–128, January 1977.
- [8] ACM. Proceedings of the 1st acm workshop on vehicular ad-hoc networks. October 2004.
- [9] G. Anastasi, L. Lanzini, and E. Mingozzi. HIPERLAN/1 MAC protocol: stability and performance analysis. *IEEE Journal on Selected Areas in Communications*, 18(9):1787–1798, September 2000.
- [10] 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.
- [11] 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.
- [12] J. Carbaugh, D.N. Godbole, and R. Sengupta. Safety and capacity analysis of automated and manual highway systems. *Transportation Research Part C (Emerging Technologies)*, 6C:69–99, February 1998.
- [13] Federal Communications Commission. FCC 03-024. FCC Report and Order, February 2004.
- [14] W. Feller. *An introduction to Probability Theory and its Applications*, volume 1. John Wiley and Sons, 1968.
- [15] J. Garcia-Luna-Aceves and C. Fullmer. Floor acquisition multiple access (FAMA) in single channel wireless networks. *ACM Mobile networks and applications*, 4:157–174, 1999.
- [16] D.N. Godbole, R. Sengupta, J. Misener, N. Kourjanskaia, and J.B. Michael. Benefit evaluation of crash avoidance systems. *Transportation Research Record*, (1621), January 1998.
- [17] E. Hoffmann and R. Mortimer. Scaling of relative velocity between vehicles. *Accident Analysis and Prevention*, 28(4):415–421, 1996.
- [18] P. Karn. MACA—a new channel access method for packet radio. *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140, 1990.
- [19] G. Korkmaz, E. Ekici, F. Özgüer, and Ü. Özgüner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. *Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks*, pages 76–85, October 2004.
- [20] W. C. Y. Lee. *Mobile Communications Design Fundamentals*. John Wiley & Sons, 2 edition, 1993.
- [21] T. Mak, K. Laberteaux, and R. Sengupta. A multi-channel vanet providing concurrent safety and commercial services. *Proc. of the 2nd ACM Workshop on Vehicular Ad-hoc Networks*, September 2005.
- [22] Bill McFraland. Private Communication.
- [23] J.B. Michael, D.N. Godbole, J. Lygeros, and R. Sengupta. Capacity analysis of traffic flow over a single-lane automated highway system. *ITS Journal*, 4:49–80, August 1998.
- [24] Institute of Transportation Engineers. Traffic management data dictionary (TMDD) and message sets for external traffic management center communications (MS/ETMCC). <http://www.ite.org/tmdd>, 2004.
- [25] P. Olson. Perception-response time to unexpected roadway hazards. *Human Factors*, 28(1):91–96, January 1986.
- [26] California PATH. SHIFT: The hybrid system simulation programming language. <http://www.path.berkeley.edu/shift/>.
- [27] W. Pattra-Atikom, P. Krishnamurthy, and S. Banerjee. Distributed mechanisms for quality of service in wireless LAN. *IEEE Wireless Communications*, pages 26–34, June 2003.
- [28] L. Roberts. Aloha packet system with and without slots and capture. *Computer Communication Review*, 5(2):28–42, 1975.
- [29] 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.
- [30] 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.
- [31] F. Tobagi and L. Kleinrock. Packet switching in radio channels: Part I- carrier sense multiple-access modes and their throughput/delay characteristics. *IEEE Trans. Comm.*, COM-23:1400–1416, December 1975.
- [32] M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. *Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks*, pages 10–18, October 2004.
- [33] USDOT. Report to congress on the national highway traffic safety administration its program progress during 1992 1996 and strategic plan for 1997 2002. January 1997.
- [34] USDOT. Analysis of light vehicle crashes and pre-crash scenarios based on the 2000 general estimates system. *IEEE Intelligent Vehicle Symposium*, (DOT-VNTSC-NHTSA-02-04 DOT HS 809 573), February 2003.

- [35] 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.
- [36] Y. Xiao. Enhanced DCF of IEEE 802.11e to support Qos. *Proceedings of IEEE WCNC*, pages 1291–1296, 2003.
- [37] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-vehicle safety messaging in dsrc. *Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks*, October 2004.
- [38] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-vehicle safety messaging in dsrc. *Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks*, pages 19–28, October 2004.
- [39] J. Yin, T. El Batt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty. Performance evaluation of safety applications over DSRC vehicular ad-hoc networks. *Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks*, pages 1–9, October 2004.
- [40] M. Zennaro and J. Misener. A state-map architecture for safe intelligent intersection. *ITSA, Minneapolis*, 2003.
- [41] J. Zhu and S. Roy. MAC for Dedicated Short Range Communications in Intelligent Transportation System. *IEEE Communications Magazine*, pages 60–67, December 2003.

APPENDIX

A. Lemmas for the PRF of the APR protocol

In this subsection we list the lemmas of the APR protocol leading to Theorem 9 bounding the PRF of APR. The lemmas are similar to lemmas 2—7. The proofs are also similar and are neglected here.

Lemma 10: PRF for One Single Repetition in the APR Protocol

For all $1 \leq j \leq k \leq n$, the PRF of p_j at any randomly chosen receiver is given by

$$P(\neg S_j) = 1 - e^{-m\lambda\tau\left[2\frac{k}{n} - \frac{k^2}{n^2}\right]}, \quad (12)$$

Lemma 11: Lower Bound on the PRF for Multiple Repetitions in the APR Protocol

Suppose p_1, p_2, \dots, p_r are any r repetitions transmitted for one message, then the probability of failure of all of them is greater than the product of the probability of failure of each one of them. Formally,

$$P(\neg S_1 \wedge \dots \wedge \neg S_r) > \prod_{j=1}^r P(\neg S_j) = (1 - e^{-m\lambda\tau\frac{k}{n}})^r, \forall 1 \leq r \leq k \leq n \quad (13)$$

Lemma 12: The PRF of a single repetition p_j for the APR protocol, conditioned on the event T_j , i.e. there is at least one other message generated in $(t_j - \tau, t_j]$, is as follows.

$$P(\neg S_j | T_j) = 1 - e^{-m\lambda\tau\left[2\frac{k}{n} - \frac{k^2}{n^2}\right]} + e^{-m\lambda\tau}$$

Lemma 13: For all $1 \leq r \leq k \leq n$,

$$P(\neg S_r | \neg S_1 \wedge \dots \wedge \neg S_{r-1}) < P(\neg S_r | T_r) \quad (14)$$

where T_r is the event that there is at least one message generated in $(t_r - \tau, t_r]$.

Lemma 14: Upper-Bound on the PRF for Multiple Repetitions in the APR Protocol

For all $1 \leq r \leq k \leq n$,

$$\begin{aligned} P(\neg S_1 \wedge \dots \wedge \neg S_r) &< \prod_{j=1}^r P(\neg S_j | T_j) \\ &= (1 - e^{-m\lambda\tau\left[2\frac{k}{n} - \frac{k^2}{n^2}\right]} + e^{-m\lambda\tau})^r \end{aligned}$$

B. Calculation of the Interference Range

The procedure to calculate the interference range r_i , given the distance between transmitter and receiver r , the message range R , and the data rate, is as follows. We need to first calculate the transmission power P_t required of R , and then the interference range r_i for r .

There is a Signal to Interference+Noise Ratio (SINR) threshold for a radio to receive data at a given data rate. The higher the data rate, the higher the threshold. Specific values of the thresholds depend on the radio design. In our simulation we use the SINR threshold values of a commercial off-the-self 802.11a radio product.

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

1) Find the SINR threshold β corresponding to the data rate.

The ratio between the reception power P_r and thermal noise N is β in dB.

2) Calculate the reception power

$$P_r = N \cdot 10^{\frac{\beta}{10}}.$$

3) Calculate the transmission power

Use the path-loss channel model, P_r , and R to calculate P_t . If the free-space model is used, $P_t = P_r \cdot \frac{R^2}{A}$, with A being some constant depending on the signal wavelength and the gains of transmit and receive antennas.

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.

1) **Find the SINR threshold β corresponding to the data rate.**

2) **Calculate the power of the signal at the receiver P_r**

If the free-space model is used, $P_r = P_t \cdot \frac{A}{r^2}$.

3) **Calculate the minimum power required to interfere**

The ratio between P_r and the interference power P_i is equal to or lower than β in dB, hence, $P_i = 10^{\frac{\beta}{10}} P_r$.

4) **Calculate r_i**

Use the channel model, P_t , and P_i to calculate r_i . If the free-space mode is used, $r_i = \sqrt{\frac{A P_i}{P_t}}$. All nodes closer than r_i from the receiver can interfere.

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

$$r_i = 10^{\frac{\beta}{20}} \cdot r \quad (15)$$

Hence, the interference range as well as the number of interferers of a receiver is a linearly increasing function of its distance to the transmitter². All the PRF results are for the cases where the distance between the transmitter and receiver is the message range. This is the worst case.

²Although the communication region increases quadratically with the transmitter-receiver distance, the number of the interference only increases linearly because the network topology is constrained by road paths