Vehicle-to-Vehicle Safety Messaging in DSRC

Qing Xu
Department of Mechanical Engineering
University of California
Berkeley, CA 94720-1740
qingxu@me.berkeley.edu

Tony Mak
Jeff Ko
California PATH
Richmond, CA 94804-4603
{tonykm, jko}@path.berkeley.edu

Raja Sengupta
Department of Civil and Environmental Engineering
University of California
Berkeley, CA 94720-1740
raja@path.berkeley.edu

ABSTRACT

This paper studies the design of layer-2 protocols for a vehicle to send safety messages to other vehicles. The target is to send vehicle safety messages with high reliability and low delay. The communication is one-to-many, local, and geo-significant. The vehicular communication network is ad-hoc, highly mobile, and with large numbers of contending nodes. The messages are very short, have a brief useful lifetime, but must be received with high probability. For this environment, this paper explores the efficacy of rapid repetition of broadcast messages. This paper proposes several random access protocols for medium access control. The protocols are compatible with the Dedicated Short Range Communications (DSRC) multi-channel architecture. Analytical bounds on performance of the proposed protocols are derived. Simulations are conducted to assess the reception reliability and channel usage of the protocols. The sensitivity of the protocol performance is evaluated under various offered traffic and vehicular traffic flows. The results show our approach is feasible for vehicle safety messages in DSRC.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless Communication

General Terms

Algorithm, Design, Performance, Reliability

Keywords

ad-hoc wireless networks, dedicated short range communications (DSRC), medium access control, vehicle safety systems

1. INTRODUCTION

Dedicated Short-Range Communications (DSRC) is 75 MHz of spectrum at 5.9 GHz allocated by the Federal Communications Commission (FCC) to "increase traveller safety, reduce fuel consumption and pollution, and continue to advance the nation's economy [9]." This promising development is designed to support vehicle-to-vehicle and vehicle-to-infrastructure communication using a variant of the IEEE 802.11a technology [1]. DSRC will support safety-critical communications, such as collision warnings, as well as other valuable Intelligent Transportation System applications, such as Electronic Toll Collection (ETC), real-time traffic advisories, digital map update, etc. The versatility of DSRC greatly enhances the likelihood of its deployment by various industries and adoption by consumers.

The 2004 FCC ruling [10] specifies DSRC will have six service channels and one control channel. The control channel is to be regularly monitored by all vehicles. The FCC has recognized safety messages and "safety of life" messages. Safety of life is to have the highest priority, whether originated by vehicles or roadside transmitters. The non-safety data transfers have the lowest priority. Given these requirements, this paper adopts the reasonable assumption that safety communications take place in the control channel[1]. Further, a licensed roadside unit could use the control channel to inform approaching vehicles of its services (often non-safety applications) and conduct the actual application in one of the service channels. For example, a roadside unit could announce a local digital map update in the control channel and transfer this data to interested vehicles in a service channel.

This paper explores the feasibility of sending safety messages from vehicle to vehicle in the DSRC control channel (hereafter simply channel). We reason about safety applications and estimate the range of data traffic they might produce. We develop Quality of Service (QoS) measures appropriate for safety applications. Finally, we build network models analytically and in simulation to assess the feasibility of supporting safety applications relying on vehicle-vehicle communication over 802.11a radios within the spectral resources allocated by DSRC.

In both simulation and analysis we use the simple collision model. Packets are lost if two nodes within interference range of each other transmit packets overlapping in time. The interference range is derived by assuming the Friis and two-ray models. The collision model is widely-used for network analysis, e.g. in [8], [12], and [22]. It is simple enough for large-scale simulation. We simulate networks with up to 1000 moving vehicles. It is the model implemented in the network simulator NS-2 [2]. The DSRC simulator used here is based on NS-2.

The rest of the paper is structured as follows. Section 2 reviews the relevant literature and technologies.Section 3 is the problem for-

VANET'04, October 1, 2004, Philadelphia, Pennsylvania, USA.

[1]However, the techniques described in this paper could be applied to service channel monitored by all vehicles.

mulation, 4 discusses the protocol design, 5 explains our evaluation methods, and 6 shows the evaluation results. Section 7 concludes the paper.

2. LITERATURE REVIEW AND RELATED TECHNOLOGIES

In ad hoc vehicular networks, TDMA, FDMA, or CDMA are difficult due the need to dynamically allocate slots, codes, or channels without centralized control. We base our designs on random access [22]. ALOHA [5] and CSMA [22] are the earliest studied random access protocols. MACA [14], MACAW [7], FAMA and its variants [12] all use the RTS/CTS scheme. Our communication is broadcast (see Section 3) therefore cannot use RTS/CTS.

In literature there are more complex protocols that support QoS. But none of them are suitable for vehicle safety messaging. HIPERLAN/1 [6], "Black Burst" [21], and the Enhanced Distributed Coordination Function (EDCF) of IEEE 802.11e [25] are all designed to reduce access delay of time-sensitive communications. The HIPERLAN/1 and Black Burst approaches have no scheme to combat hidden terminals. In EDCF, when the number of contending packets of equal priority is large the probability of collision is high. This is the case for vehicle safety communications (Section 3).

Reference [19] reviews the existing variants of the 802.11 DCF to support QoS. Its authors conclude that 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 (Section 3). Reference [27] gives an overview of DSRC applications and assesses the characteristics of the IEEE 802.11 MAC and PHY layers in this context. It is anticipated that the current 802.11 specifications will need to be suitably altered 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. Cellular base stations are significantly more expensive than their supposed DSRC equivalent, i.e., 802.11 access points. Moreover, cellular handles only infrastructure to mobile communication.

3. PROBLEM FORMULATION

We clarify certain design assumptions and then estimate data traffic levels offered by safety applications and develop our QoS measures in two sub-sections respectively.

Most safety messages produced by a vehicle are useful to many vehicles. For example, a stopped vehicle warning is useful to all approaching vehicles. Therefore we assume a broadcast communication service.

We have restricted design to a communication service able to execute the vehicle-vehicle communication without any roadside or base station infrastructure, i.e, an ad-hoc service. This would ease deployment.

802.11a radios are designed to transmit over distances of 200 to 300 meters. This is the upper end of the message range in Table 1. Hence we propose a single hop communication service.

In summary, we propose a single-hop service to broadcast messages while meeting QoS requirements in vehicular ad-hoc local-area networks.

3.1 The DSRC Safety Environment

Table 1 summarizes this section. It gives ranges for the parameters determining the offered traffic. Our evaluation is based on these ranges.

Table 1: Offered Traffic Parameter Ranges

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

When the offered traffic is large, reliability, latency, and channel efficiency deteriorate. In wired networks offered traffic is measured by the total bits/second produced by all the senders. However, in wireless networks, a more appropriate measure of offered traffic is bit-meters/second [13], i.e., a network able to transmit a bit 100 meters, may not be able to transmit the same bit 200 meters. Therefore the offered traffic depends on the safety message rate (messages/sec), size (bytes/message), message range (meters), and the density of vehicles producing these messages.

The reasoning behind table 1 is as follows. A vehicle at high freeway speeds (90 mph) moves 2 meters within its lane in 50 msec. This is usually not a significant movement at high speed. Thus messages repeating faster than once every 50 msec are unlikely to provide significantly new information. On the other hand an update slower than once every 500 msec is probably too slow. Driver reaction time to stimuli like brake lights can be of the order of 0.7 seconds and higher. [17] Thus if updates come in slower than every 500 msec, the driver may realize something is wrong before the safety system. This would make the driver think the safety system is not effective. The message sizes in table 1 are chosen to permit sender or receiver location as per the SAE J1746 standard [4], GPS, NTCIP hazard codes [16], and standard protocol headers [3]. Safety messages are usually short. Communication is more difficult at high vehicle densities. The 10 meters per vehicle represents the jammed highway. The 30 meters per vehicle represents the highway at capacity. Likewise, the 4 to 8 lane range spans the usual to large roads.

The message range is the maximum distance at which a message should be received. For example, a stopped vehicle warning may have a message range of 300 meters, meaning that any vehicle within 300 meters of the sender should receive it with high probability. Safety application designers would prefer large message ranges to smaller ones. On the other hand large message ranges make network design more difficult. The 300-meter message range corresponds to the comfortable stopping distance of a high speed car. When the road is jammed, neighboring cars will be much closer. Therefore it should not be necessary to send safety messages over the same distance. We assume a top range of 100 meters for jammed roadways, or approximately 10 inter-vehicle distances.

3.2 Quality of Service Metrics for DSRC Safety Messages

Reliable communication in networks has typically meant retransmitting a message till it is acknowledged by the recipient(s). This is appropriate for file transfers since even one missing byte may render the entire file unusable. Thus reliable transmission protocols like TCP acknowledge each byte and retransmit any packet not appropriately received. This paradigm is not appropriate for safety messages.

If a safety application is generating updates every 100 msec and a particular message has still not been received 100 msec after it was created, a new message, obsoleting the old one, will already

have been created. Therefore we have focused on the design of a local-area communication service delivering messages within their lifetime with high probability. The lifetime can be thought of as a delay requirement. To capture this QoS notion we define the Probability of Reception Failure (PRF) as follows.

DEFINITION 1. *The probability of failure $PRF(L,\tau)$ of a vehicular network, for a given transmitter-receiver distance L, and message lifetime τ, is the probability that a randomly chosen message transmitted by a randomly chosen vehicle will not be received by a randomly chosen receiver at distance L within time τ.*

In the foreseeable future, the active safety systems on the vehicle will assist the driver rather than substitute for her. Moreover, most safety messages should be consumed by an estimator. For example, the warnings from the slowly moving or stopped vehicle should be consumed by an estimator of the position of the damaged vehicle relative to the receiver. [26] Since an estimator leverages correlations in the time series of messages, it is usually robust to the loss of messages, unless the losses occur in bursts. Therefore PRFs in the range of 1/1000 to 1/100 should be adequate.

In subsection 5.1 we will see the interference experienced by a receiver is larger when it is further from the transmitter. The worst case therefore is when the transmitter-receiver distance is the message range. Therefore all the PRF results we present in this paper are $PRF(Message\_Range, Message\_Life\_Time)$ with the arguments as in table 1.

We assume that the safety messages are to be sent on the control channel. However, the DSRC standards show the control channel also has to communicate other non-safety messages for the remaining channels to be useful. The control channel protocol and the various types of non-safety messages it is to carry are not known at this time. Therefore instead of modelling the non-safety messages explicitly, we evaluate the fraction of the control channel time occupied by safety messages (the channel efficiency). This is measured by channel busy time (CBT). If the CBT of a protocol is low we take it as more accommodative of non-safety messages.

The CBT is defined as follows. We pick a node at random and consider the set of nodes within interference range of the node. For any time period T in the control channel, part of it will be occupied by successful or unsuccessful safety messages transmitted by nodes in this set, and the rest of the time will be idle. Let T_{safety} be the total length of the time periods within T occupied by safety messages. Then we have the following definition:

DEFINITION 2. *The channel busy time of a network is defined by:*

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

In our simulation we take T to be the whole simulation time, and average the CBT at various regions in the network to obtain the measure for the simulation as a whole.

$(1 - PRF)$ is our measure of the service received by safety applications. The CBT is a measure of the cost to non-safety applications. Ideally, both PRF and CBT should be low.

4. PROTOCOL DESIGN

4.1 General Considerations

In a wireless ad-hoc network there are two obstacles to the reliable reception of messages. If two transmitters within interference range of the same receiver transmit concurrently, their transmissions collide at the receiver. The receiver does not receive either message. To combat this problem one designs a Medium Access Control (MAC) protocol, i.e., a set of rules by which a radio decides when to transmit its messages and when to keep silent. Secondly, even if there is no collision, the wireless channel may attenuate the transmitted power so much that it is swamped by thermal noise. This is combated by selecting the transmission energy to be high enough to reach all receivers within the message range with high probability, when there are no collisions.

Transmission energy is determined by transmission power, modulation, and error coding. DSRC radios are to be based on the 802.11a radio. In our evaluation we set the transmission energy control parameters to model the 802.11a radio transmitting over a 20 MHz channel at 5.4 GHz and focus on the MAC design problem, i.e., is there a MAC able to deliver safety messages with sufficiently high reliability within the message lifetimes?

In unicast communication reliability is enhanced by policies based on receiver feedback, e.g. RTS/CTS, TCP, or WTP. [24] These require the sender to learn the identity of its receiver(s). 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.

Our strategies repeat each message without acknowledgement in combination with CSMA and its variants. Our repetition schemes are designed for overlay on CSMA. The following is the specifications of our various designs.

4.2 Protocol Specifications

Figure 1 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 into $n = \lfloor \frac{\tau}{t_{trans}} \rfloor$ slots, where $\lfloor x \rfloor$ is the maximum integer not greater than x, τ is the lifetime, and t_{trans} is

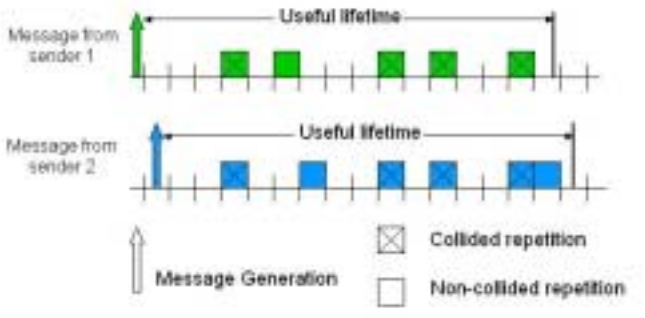

Figure 1: The Concept of Repetitive Transmission

Our protocols use two schemes to reduce PRF, repetition and carrier sensing. Carrier sensing is in the 802.11 MAC. In all the cases but two, our protocol is an overlay on a standard MAC like ALOHA [5] or Carrier Sensing [22]. We call this overlay the MAC extension layer.

Our MAC extension layer would 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 2. Upon receiving a message

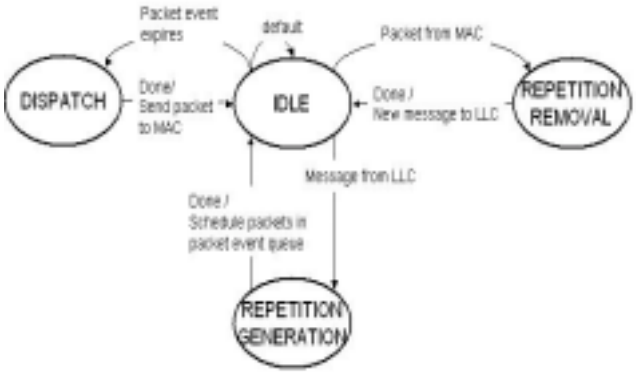

Figure 2: MAC Extension Layer State Machine

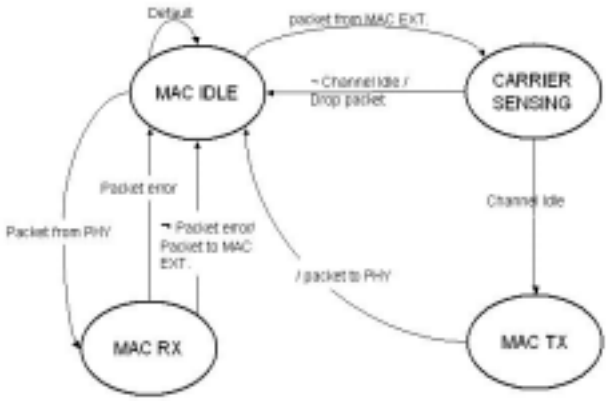

Figure 3: MAC Layer State Machine of the AFR-CS protocol

from the LLC, the MAC Extension transits from IDLE to REPETITION GENERATION state. In this state, the system schedules multiple repetitions of this message in the selected time slots within the message lifetime. Each repetition is an event with a slot number. All these events ordered by slot numbers form a queue called 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 IDLE to 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.

The following are different protocols designed and evaluated by us. They share the same MAC extension layer. as described above, the protocols slot the time locally for each radio. All the protocols we design can be classified into two classes, synchronous and asynchronous. Synchronous protocols slot time to a global clock like in slotted ALOHA [5], i.e. a local slot in each radio starts at the beginning of one global slot of the same size. The 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 protocol is called "fixed" because the packet is always repeated a fixed number of times, i.e., k. The radio does not listen to the channel (i.e. perform carrier sensing) before it sends a packet with AFR.

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 $p = \frac{k}{n}$, where k is again a configuration parameter of the protocol. The average number of transmissions of a message is k. However, for each realization the exact number of repetitions varies. 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 for the synchronization of transmissions by all nodes into common slots.

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

   AFR-CS has its own MAC shown in Figure 3. AFR-CS generates the repetitions in the same way as in the AFR protocol. Whenever a packet is passed down from the MAC Extension, MAC transits from the IDLE to the CARRIER SENSING state. In the CARRIER SENSING state, the system checks the channel status using carrier sensing [22]. 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.

5. EVALUATION METHODS

We have two methods of evaluation: mathematical analysis and simulation. We use mathematical results to get a qualitative understanding of what the simulator might show. The parameter space to be explored is large. The mathematical expressions have also been used to select parts of the parameter space for intensive simulation.

5.1 Mathematical Analysis

For the SPR and APR protocols we have developed mathematical expressions for the probability of reception failure. These expressions can be processed using Matlab.

The details of the mathematical analysis are in [26]. We assume the message generation process is Poisson. Poisson process is an approximation of the superposition of large number of independent periodic processes with various interval and starting time. [11] We further assume the message generation processes of different vehicles are independent. Then the overall message generation process of all vehicles within the interference range of a receiver is also Poisson. [11] However the network traffic is composed of repetitions of the messages. These occur only within the lifetime of the message. Thus the overall packet process on the channel is not Poisson, e.g., in Figure 1, the process of the arrows is Poisson by assumption, but that of the rectangles is not. Hence our analysis is different from those appearing in [8] and [22].

Let n be the total number of slots, i.e. the maximum possible number of repetitions in the message lifetime, k be the number of repetitions for the message (average value for p-persistent protocols and exact value for fixed repetition protocols), S be the event that at least one of the repetitions succeeds, τ be the lifetime of the message, λ be the message generation rate at each individual node, and m be the total number of interferers around a receiver. Then the following inequality gives upper and lower bounds on the PRF of the SPR protocol:

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

For the APR protocol, the PRF at a receiver with m interferers satisfies the following inequality:

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

For both SPR and APR, the bounds are quite tight over the offered traffic range of interest (Table 1). In the rest of the paper we present analytical results with the right hand side of both equation (1) and (2). The corresponding plots for the left hand sides are not distinguishable.

The number of interferers m in equations (1) and (2) is calculated by:

$$\textbf{Interferer Number} = \frac{2\cdot\textbf{Interference Range}}{\textbf{Meters per Vehicle}}\cdot\textbf{Lane number} \quad (3)$$

The procedure to calculate the interference range, given the transmitter-receiver distance, the message range, and the date rate, are given in Appendix A.

5.2 Simulation

We have developed a DSRC simulator. The simulator is based on two others, namely SHIFT [18] and NS-2 [2]. SHIFT is a well established traffic simulator. It gives us the trajectories of vehicles driving according to validated models on realistic road networks [23]. Figure 4 is a screenshot of the vehicle traffic simulated by SHIFT. We use SHIFT to generate the motion of the radios. This motion is input to NS-2. NS-2 is an open source network simulator widely used in academic community. NS-2 generates the offered traffic, simulates transmissions and receptions, and outputs packet reception data. We post-process the data to obtain channel busy time, probability of reception failure, and the probability of long bursts of failures.

Figure 4: A typical traffic screen-shot of SHIFT

Thus the DSRC simulator is the standard NS-2 release plus

- SHIFT
- The radio model for 802.11a at 5.4 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 5 shows the run-time comparisons. This enhancement has enabled us to simulate networks with up to a thousand vehicles.

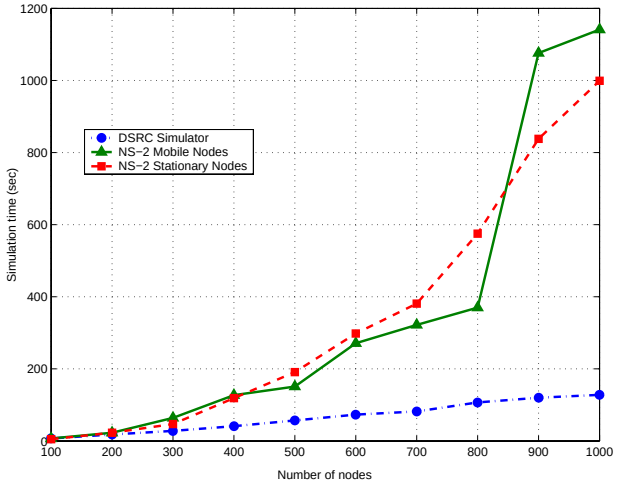

Figure 5: Improvement on the Scalability of PATH DSRC Simulator over NS-2

We use the deterministic Friis Free-space model for short distances and the Two-ray model for longer distances [15] to determine received power, i.e, if the distance between the transmitter and receiver antennas is d, then the power of the signal decreases as d^2 when the distance is short and d^4 when the distance is large.

6. EVALUATION RESULTS

We study homogeneous offered traffic in this paper. The repetition number k, transmission power, data rate, and packet size are the same for all nodes. In the mathematical analysis we assume the inter-vehicle distances are the same as well. In the simulation we specify the average flow of the highway. The inter-vehicle distances vary in space and time.

Figure 6 shows the analytical and simulated PRF of the APR and SPR protocols for the nominal values in Table 2. The analytical plots are from inequalities (1) and (2). The analytical and simulation results match well. Intuition suggests when a message is repeated more than once the chances of it being received may rise. On the other hand repetition increases the aggregate number

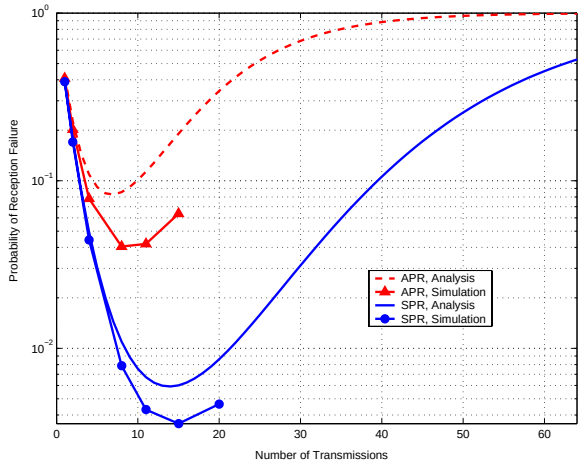

Figure 6: Validation of Simulation Results with Analytical Model

of collisions, implying repetition beyond a certain level should be counter-productive. Figure 8 confirms this. In both analysis and simulation, there is an optimal number of repetitions. This optimal number is different for different message ranges, message generation rates, vehicular traffic densities, message sizes, etc. Figure 7 shows the variation of the optimal repetition number and the minimum PRF with message range. Other parameter values are as in Table 2.

The reason that the simulation results in Figure 6 are consistently better than the analytical ones is the following. Since the message generation process is Poisson rather than periodic, the lifetime of two or more consecutive messages from the same node can overlap. The repeated packets of a prior message can thus select the same time slot to transmit as the packets of a later message. In the mathematical analysis we treat previous messages the same as messages from the other nodes, i.e. the node's packets from a prior message can collide with its packets from a later message. In simulation we let the packets from the latest message overwrite any colliding packets from earlier messages. This is more realistic. Therefore we see an enhanced performance in simulation.

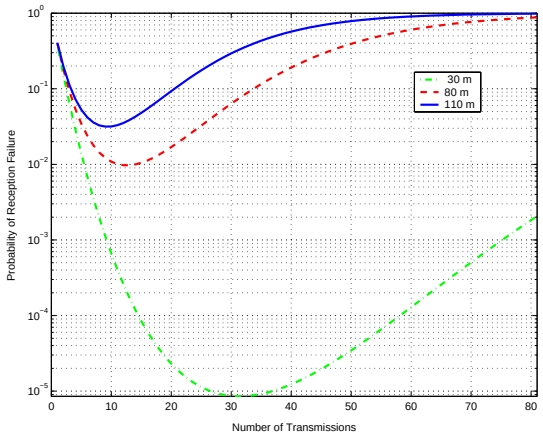

Figure 7: Probability of Reception Failure at different message ranges: SPR in the nominal setting, analytical PRF generated by Matlab

Table 2: Nominal Setting Parameters

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

Figure 8 shows the performance of the protocols as a function of the number of repetitions. Other parameters are as in table 2. The curves are based on output from the DSRC simulator. CSMA parameters (e.g., DIFS) have been kept fixed at their 802.11 values. As will be discussed shortly, there is an optimal data rate for a protocol under a given setting. In this Figure we show the simulation results of all the protocols at their respective optimal rate.

The best protocols are AFR-CS and SFR. SFR would require a clock synchronization infrastructure. Therefore AFR-CS is the better solution. Note also the PRF improvement over 802.11a is one order of magnitude. This shows that repetition helps combat interference by giving a transmitter more chances to transmit, and making interfering nodes transmit at different times. The better performance of the AFR-CS protocol compared to 802.11 indicates that repetition mitigates hidden terminal impact even without using RTS/CTS.

Clearly, for the same repetition methods (i.e. fixed repetition or p-persistent repetition), the synchronous protocols outperform the asynchronous protocols. The synchronous protocols eliminate partial overlaps between packets from different nodes. This observation agrees with previous results on slotted and non-slotted ALOHA [20]. Also for the same repetition method, a CSMA protocol is better than a non-CSMA protocol. CSMA listens before transmission, avoiding many potential collisions. The reception failures for CSMA protocols are mostly due to hidden terminals. The Fixed repetition protocols outperform the corresponding p-persistent protocols. The reason is that the fixed repetition protocols are better at maintaining the number of repetitions for each message, i.e. there is less fluctuation between the actual number of repetition of each message and the expected number of repetitions. The higher variance in the p-persistent case hurts them. We conjecture they gain less by transmitting more frequently than they lose by transmitting less frequently.

Figure 9 is a plot of CBT versus repetition number for the two protocols. It shows that CBT increases with the repetition number. With the same number of repetitions the AFR-CS protocol has smaller CBT than other proposed protocols. Not surprisingly, the 802.11 has small CBT since it does not repeat. These plots are for the nominal parameters in Table 2. Therefore the rest of our evaluation uses AFR-CS. In Figure 8, the PRF of AFR-CS keeps decreasing with number of transmissions. However the PRF shown in the plot already levels off. In another test, we keep increasing the number of repetitions and observe that the probability of reception failure of AFR-CS protocol does increase as observed in other protocols, though at very large repetition numbers. The result is not shown here to save space.

The Channel Busy Time is a measure of the fraction of channel capacity left over for non-safety messages. As the repetition number goes up so should CBT. Thus there is an inverse relationship between PRF and CBT up to the optimal repetition number. Curves in Figure 10 show this tradeoff. As the quality of service

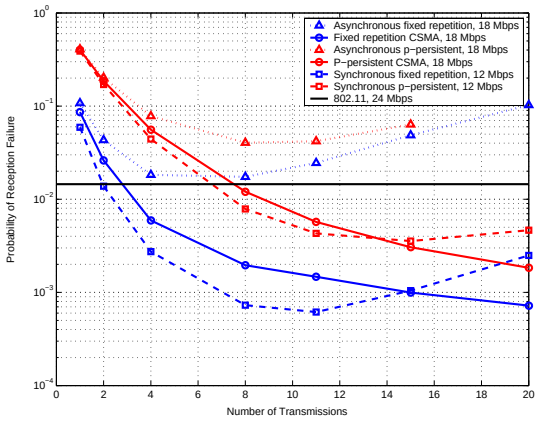

Figure 8: Probability of Reception Failure for Proposed Protocols in the Nominal Setting

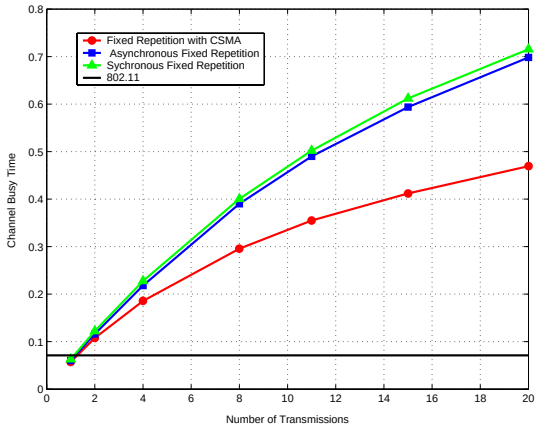

Figure 9: Channel Busy Time in the Nominal Setting

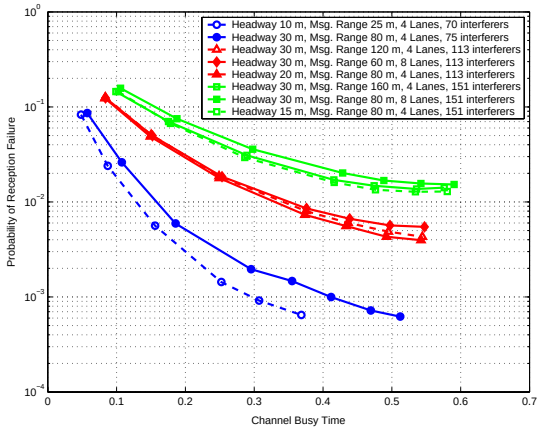

Figure 10: Performance of AFR-CS Protocol as a Function of Interference Indicator

Table 3: Optimal Data Rate for All the Simulated Protocols in the Nominal Setting

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

to the safety applications is raised, that of for other applications in control channel comes down. Therefore these curves are a good way of evaluating the performance of our protocols.

Equations (1) and (2) shows performance depends on the number of interferers. In an actual traffic simulation this number varies in complex patterns. Nevertheless, since the vehicle traffic does not change much within the transmission of one message, we can regard it as a series of snapshots when evaluating the number of interferers. Hence, the single number evaluated by (3) is a good predictor of the performance. Figure 10 shows that for small transmission time the dynamics of the topology makes almost no difference to aggregate network performance. The curve for 30-meter headway, 60-meter message range, 8 lanes and the curve for 20-meter headway, 80-meter message range, and 4 lanes are clustered together because they have the same number of interferers calculated by (3), i.e., 113. The number of interferers for the nominal case is 75.

Intuition suggests that for each number of interferers and repetition number there may be an optimal data rate. If the transmission rate is raised, the transmission time reduces, tending to reduce the probability of collision. On the other hand the power required to cover the message range also rises, thereby raising the number of interferers. Figure 11 shows this for AFR-CS protocol with the nominal parameter combination in Table 2. Table 3 shows the optimal data rates for all the protocols in the nominal parameter setting.

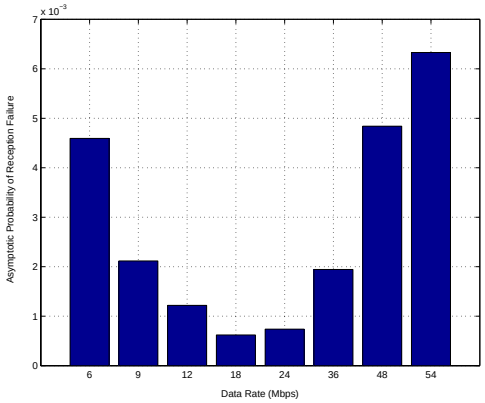

Figure 11: Probability of Reception Failure for Various Data Rate in the Nominal Setting: AFR-CS Protocol

Figure 12 shows the probabilities of bursts of failures of different lengths for the nominal parameters in Table 2. The probabilities

are small. This is due to the memoryless feature of the channel in simulation. The probability a receiver sees two or more consecutive failures is negligible. This is good for estimation.

Figure 13 pulls these various results together to get a sense of the feasibility of supporting safety applications on the control channel. Feasibility depends on a PRF and CBT requirement. Given a PRF and CBT requirement and a combination of parameter values within the ranges in Table 1, our simulation data can show whether it meets the requirements. We do this by assuming the AFR-CS protocol and optimizing the protocol for repetition number, transmission rate, and selecting the modulation and code rate to minimize the power required to cover the message range. Figure 13 shows feasibility for a PRF less than 1/100 and a CBT less than 50%. For example, the 200 msec message rate, 250 byte message at 140 interferers is feasible. This corresponds to a 30 meter, 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. It has the same interferer number.

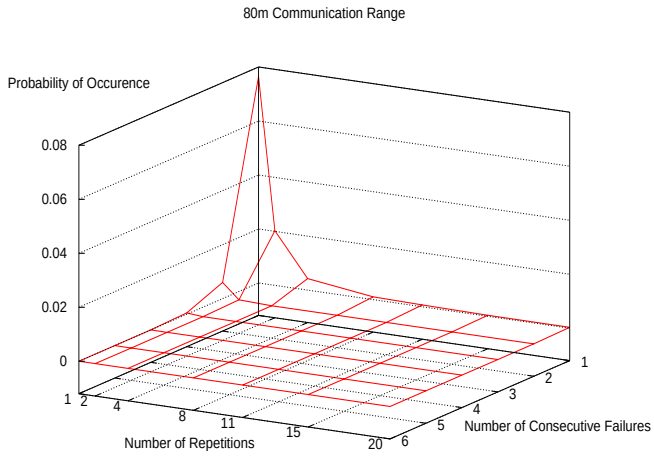

Figure 12: Probability of message failure bursts vs. repetition number: AFR-CS Protocol in the nominal setting

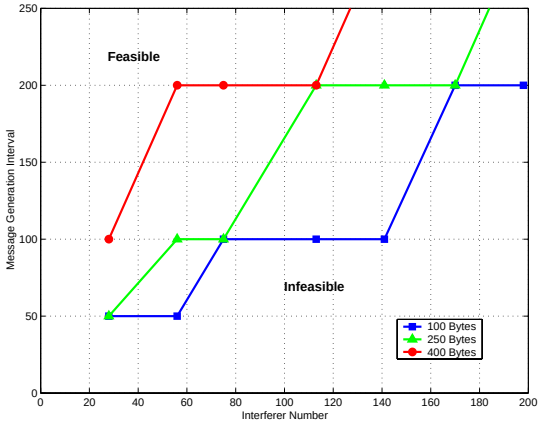

Figure 13: Feasibility Regions for Probability of Reception Failure < 0.01 and CBT $< 50\%$: AFR-CS Protocol

7. CONCLUSION

We have evaluated the feasibility of exchanging safety messages between vehicles based on 802.11a. This is the DSRC technology platform.

We have estimated reasonable ranges for the offered safety traffic and developed two QoS measures, namely PRF and CBT. The PRF is the QoS experienced by safety applications. Lower is better. The CBT is of interest because we expect the channel to be shared with other non-safety messages. The CBT is a measure of the potential to accommodate these other messages. Lower CBT is better as well.

Table 2 represents our estimate of the range of data traffic that might be offered by safety application designers. Our first finding is that the entire range is not feasible. The PRFs become too high (1/10 or higher) at some values.

Our second finding is that some offered traffic levels are feasible if network designers and safety application designers work together. Consider the 200 msec, 140 interferer point on the 250 byte line in figure 13. Driver reaction times in near-miss situations are 0.7 seconds or higher, implying an on-board safety system relying on messages communicated every 200 msec would be able to recognize the situation faster and provide timely assistance to the driver. Furthermore, the vehicle position information included in safety messages will come from GPS. This usually updates no faster than 5 Hz. The 250 byte message size is adequate. The 140 interferer number corresponds to a 4 lane highway at capacity flow, with speed between 50 to 55 mph, and a message range of 150 meters. At these speeds almost all light-duty passenger vehicles are able to stop within 150 meters. Thus this is an adequate value for the message range. Safety system designers have a reasonable chance of designing safety systems within these offered traffic limits. Likewise, when the highway is jammed, e.g. the average density is 15 meters per vehicle, a message range of 80 meters covering 5 cars in either direction, also corresponds to 140 interferers. Thus at these operating points a PRF of 1/100 or lower is feasible.

The probability of consecutive losses is an order of magnitude lower. This strengthens the case for feasibility because safety messages will be consumed by estimators. These will correlate an entire sequence of messages to produce the best possible map of neighboring vehicles. An estimator should be robust to the occasional loss of messages.

This argument about feasibility suggests future design work in the intersection of communications and transportation engineering. If the vehicle is to transmit to a 150 meter range on highways at capacity and 80 meters on jammed highways, it needs to adapt communication and protocol parameters to the flow of vehicular traffic. We require adaptive control at the physical and MAC layers in broadcast communications. Most adaptive control schemes rely on receiver feedback. This is problematic in broadcast communications.

This analysis has some limitations. The channel model is memoryless. If a truck appears between two cars and remains there, disrupting communications, for several seconds, the probabilities of successive failures will be worse than predicted by these analyses. Thus the slow fading characteristics of the vehicle-vehicle channel need to be better understood. Secondly, the CBT is only an indirect means to estimate the accommodation of non-safety traffic. There will be multiple classes of traffic sharing the channel. We have characterized the safety traffic. The DSRC community

needs to characterize other classes of traffic. This will enable a better feasibility study. Furthermore, safety traffic itself is of different classes. We hope to do further analysis that models multiple classes of safety traffic and evaluates the QoS for each class.

Acknowledgment

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

8. REFERENCES

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

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

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

[4] ISP-vehicle location referencing standard. *SAE Standard J1746*, July 2001.

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

[6] 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.

[7] 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.

[8] 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.

[9] Federal Communications Commission. FCC 99-305. FCC Report and Order, October 1999.

[10] Federal Communications Commission. FCC 03-024. FCC Report and Order, Feburary 2004.

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

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

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

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

[15] W. C. Y. Lee. *Mobile Communications Design Fundamentals*. John Wiley & Sons, 2 edition, 1993.

[16] 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.

[17] P. Olson. Perception-response time to unexpected roadway hazards. *Human Factors*, 28(1):91–96, January 1986.

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

[19] W. Pattra-Atikom, P. Krishnamurthy, and S. Banerjee. Distributed mechanisms for quality of serivce in wireless LAN. *IEEE Wireless Communications*, pages 26–34, June 2003.

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

[21] 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.

[22] 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(12):1400–1416, December 1975.

[23] 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.

[24] J. Walrand and P. Varaiya. *High-performance Communications Networks*. Morgan Kaufmann, 2nd edition, 2000.

[25] Y. Xiao. Enhanced DCF of IEEE 802.11e to support Qos. *Proceedings of IEEE WCNC*, pages 1291–1296, 2003.

[26] Q. Xu. *Control, Estimation, and Communication Design Applied to Vehicle Safety Systems*. PhD thesis, University of California at Berkeley, 2004.

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

APPENDIX

A. 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 date 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, $r_i = \sqrt{\frac{AP_t}{P_i}}$. All nodes closer than r_i from the receiver can interfere.

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

$$r_i = 10^{\frac{\beta}{20}} \cdot r \tag{4}$$

Hence, the interference range as well as the number of interferers of a receiver is a linearly increasing function of its distance to the transmitter[2]. All the following results were taken when the distance between the transmitter and receiver is the message range. So all the results are for the worst case.

[2] Although 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