UC Berkeley

Research Reports

Title

Multi-Channel Medium Access Control for Dedicated Short Range Communications

Permalink

https://escholarship.org/uc/item/5ct6m97s

Authors

Mak, Tony K.
Laberteaux, Kenneth P.
Sengupta, Raja
et al.

Publication Date

2006-05-01

eScholarship.org

Powered by the California Digital Library
University of California

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

Multi-Channel Medium Access Control for Dedicated Short Range Communications

**Tony K. Mak, Kenneth P. Laberteaux,
Raja Sengupta, Mustafa Ergen**

California PATH Research Report
UCB-ITS-PRR-2006-5

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

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 15650 & 94138

May 2006

ISSN 1055-1425

Multi-Channel Medium Access Control for Dedicated Short Range Communications

Tony K. Mak*, Kenneth P. Laberteaux‡, Raja Sengupta§, and Mustafa Ergen†
*§Department of Civil and Environmental Engineering
†Department of Electrical Engineering and Computer Science
University of California, Berkeley, CA 94720-1740
‡Toyota Technical Center
Ann Arbor, MI 48105
Email: *tonykm@path.berkeley.edu, ‡klaberte@acm.org, §raja@path.berkeley.edu, †ergen@eecs.berkeley.edu

Abstract

This paper describes a medium access control (MAC) protocol to enable multi-channel operation for dedicated short range communication (DSRC). In particular, we focus on the challenge of supporting potentially high-bandwidth commercial or infotainment communications between vehicle and roadside in hotspots over several service channels, while concurrently enabling time-critical vehicle-vehicle communication for safety in a separate channel. In our architecture, within hotspots, communication is aided by one of the access points in the hotspot. This access point is designated the Coordinating Access Point (CAP). Outside hotspots, communication is for safety and is conducted in an ad-hoc fashion. The CAP protocol design is a variant of IEEE 802.11 PCF, modified for multi-channel operation. The design objective is to maximize utilization of the service channel used for non-safety communication while meeting the Quality of Service (QoS) constraints of the safety communications. The performance of 802.11 DCF, PCF, and the CAP extension is quantified by simulation in NS-2. The mobility model represents a 4-lane freeway at maximum vehicular traffic flow derived from the SHIFT traffic simulator. The CAP design is shown to significantly enhance both safety and non-safety communication relative to DCF and PCF only.

KEYWORDS: Wireless LAN, DSRC, WAVE, Vehicular Communication, IEEE 802.11, PCF, DCF

I. Introduction

THE United States Department of Transportation has declared that the reduction of vehicular fatalities is a top priority [4]. There is serious interest within government and industry in transforming 802.11 into a technology able to make automotive travel safer. This is evidenced by

1) the emergence of an 802.11 based standard, i.e., 802.11p [28], for a spectrum labeled Dedicated Short Range Communications allocated by the Federal Communications Commision (FCC) [3] with priority for safety communications,
2) the release of requirements [5] for vehicle-vehicle communications for safety applications by the Vehicle Safety Communications Consortium (VSCC) comprised of the automotive OEMs in partnership with the National Highway Traffic Safety Administration (NHTSA), and
3) the release of requirements for roadside-vehicle communications for collision avoidance at intersection [6] and the creation of the Cooperative Intersection Collision Avoidance (CICAS) consortium [1] to design and prototype a system.

This paper explores the challenge of using an 802.11-like radio in the vehicle to support both safety and non-safety applications. The connection between 802.11 radios and safety provides a strong case for integrating such radios into cars. The case grows stronger still if these radios could be used concurrently by more conventional applications like congestion advisories, digital map updates, electronic toll collection, mobile infotainment, or multimedia, i.e., *non-safety and commercial applications*. To quote the FCC ([3]):

> *We conclude that it is possible to license both public safety and non-public safety use of the 5.9 GHz band. Accordingly, we adopt open eligibility for licensing and technical rules, most of which are embodied in the ASTM-DSRC standard, aimed at creating a framework that ensures priority for public safety communications.*

The standard referred to by FCC bases DSRC on 802.11a. In the same report and order the FCC divided the spectrum into six 10 MHz service channels and a control channel. Safety messages can be sent on the control channel but non-safety transactions or connections have to be conducted in a service channel. Hereafter we refer to the non-safety transactions or connections as *service communications.* Since 802.11 radios demodulate one channel at a time, the various aspects of the ruling create a challenge. If the 802.11 radio on a vehicle is on a service channel while a safety message is transmitted on the control or safety channel, how can the vehicle receive the message? This is the problem motivating this paper.

The literature has designs, reviewed in section II, for multi-channel networking with single channel radios. When communication is connection-oriented, sender and receiver use some protocol to rendezvous, negotiate a channel, and go there for the duration of the connection. However, we think safety communication will not be connection-oriented. The literature on safety

[1] http://www.its.dot.gov/cicas/index.htm

Application	Packet Size (Bytes)/Bandwidth	Allowable Latency(ms)	Network Traffic	Range (m)	Priority
Intersection Collision Warning/Avoidance	∼100	∼100	Event	50-300	Safety of Life
Cooperative Collision Warning	∼ 100/ ∼ 10Kbps	∼100	Periodic	50-300	Safety of Life
Work Zone Warning	∼ 100 ∼ 1Kbps	∼ 1000	Periodic	50-300	Safety
Transit Vehicle Signal Priority	∼100	∼1000	Event	300-1000	Safety
Toll Collection	∼100	∼50	Event	≤ 15	Non-Safety
Service Announcements	∼100/ ∼2Kbps	∼500	Periodic	0-90	Non-Safety
Movie Download (2 hours of MPEG 1) 10 min. download time	> 20Mbps	N/A	N/A	0-90	Non-Safety

TABLE I
EXAMPLES OF DSRC APPLICATIONS AND REQUIREMENTS.

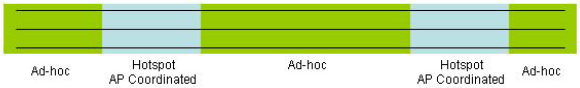


Fig. 1. Protocol Concept

messages ([5]–[7]) suggests they will report information like the position or speed of the sender, motion status like *stopped, braking hard, turning*, or road condition information like *ice, slippery, congestion*. These messages are short (order of 100 to 200 bytes), arise unpredictably from in-vehicle applications reacting to sensor data, and useful to many vehicles. Hence safety messages require protocol design for a lot of broadcast, and connectionless transport without rendezvous. Our design aims to be efficient for broadcast of short, time-critical safety messages by many vehicles. Service communications can be connection or transaction-oriented.

Our design philosophy is to maximize the bandwidth available for service communications, while meeting the Quality of Service (QoS) for safety messages emerging in the literature ([5]–[7]). The literature provides size, latency and range requirements for safety messages. Table I summarizes some typical numbers in these references. Message size is between 100 to 200 bytes. Latency is typically between 100 and 500 msec. Ranges are between 50 and 300 meters. The range signifies the message should be received by all vehicles within that range of the sending vehicle. We denote this range by VSMR (Vehicle Safety Message Range). Since 802.11p radios can communicate up to 300 meters, we assume safety messages are communicated in a single hop. One QoS measure for safety messages is the probability a safety message, once transmitted, is received by a randomly chosen receiver within VSMR of the sender. We also quantify the time between consecutive opportunities given to a vehicle to transmit its safety messages. For example, if safety message latencies can be as small as 100 msec, a vehicle should receive an opportunity to transmit nearly every 100 msec.

Since the various players in the vehicular application space are converging on 802.11a based DSRC, our solutions try to build on 802.11. In particular we evaluate 802.11 DCF as a solution, 802.11 PCF as a solution, and finally a design called the Coordinating Access Point (CAP) configuration proposed here. The CAP configuration extends PCF and combines it with a slightly modified DCF to provide better support for concurrent safety and non-safety communication than either DCF or PCF alone. The contributions of this paper are the CAP configuration design, and the relative performance of DCF, PCF, and CAP. The results show PCF is better than DCF and the CAP configuration is better than both.

We assume all safety messages are sent on a single channel. This could be the DSRC control channel. We assume non-safety communications occur in hotspots on the road as is usual for 802.11 (see figure 1). On the other hand, safety communications are assumed to occur both inside and outside the hotspots. The CAP solution requires the presence of an access point, the CAP, only in hotspots. The CAP has to coordinate channel access by all vehicles in the vicinity of the hotspot. Outside the hotspot, i.e., where there are only safety communications, we require communications to be ad-hoc. Since safety messages can arise anytime and anywhere, all the DSRC players prefer this. After all any infrastructure used for safety message exchange between vehicles would have to be anytime and anywhere. This would hinder DSRC deployment. Figure 1 illustrates a freeway covered by AP Coordinated regions corresponding to hotspots separated by ad-hoc networking regions. The ad-hoc networking regions are for safety communication only.

In the CAP configuration the ad-hoc protocol is a modified DCF. We hope the modifications in section V will be considered minor and practical by the 802.11 industry. By emphasizing DCF as the ad-hoc protocol, we do not wish to suggest it provides acceptable message loss numbers for safety communication. The results in this paper indicate about a 3% loss when all vehicles transmit safety messages. While it is generally recognized in the active safety community that safety applications need to tolerate some rate of message loss, there is no common understanding of the magnitude of loss to be tolerated. Numbers as high as 10% have been suggested because there is potentially a lot of overlapping information in a stream of messages emanating from a vehicle. For example, if the messages report on position, position is highly correlated across the stream. In some sense, the stream communicated is not compressed.

Rather we emphasize DCF because it is deployable, in the DSRC standard, and will deliver acceptable performance when the network is lightly loaded, i.e., at low market penetrations. DCF will probably be the first ad-hoc DSRC protocol deployed. Hence we emphasize it to show how the CAP solution could work with DCF. In our evaluations we use DCF as a baseline and argue the relative rather than absolute performance of the CAP configuration. Getting better performance for concurrent safety and service communication will require better performance for safety communication alone. We have tried to design the CAP configuration to have this property. Given a better ad-hoc protocol it will deliver better performance. The CAP configuration can work with a family of ad-hoc protocols. The restrictions defining the family are in section V.

The structure of the paper is as follows. Section II reviews the literature. Design is described in three sections with progressive levels of detail. Section III describes the design architecture in terms of hardware configurations, the time and spatial division underlying the protocol design. Section IV describes the different kinds of frames and control messages used by the design. Section V specifies the design rigorously using state machines. Section VI presents some logical properties of the design as theorems. The theorems explain why the design is structured the way it is. The proofs appear as an appendix (section XI). Thereafter the design is evaluated by simulation using NS-2. Section VII is a brief description of simulation parameters. Section VIII presents the simulation results. Since the design relies on different power levels for spatial division section IX discusses the selection of power levels. Finally section X concludes the paper.

II. Prior work and Technology

A preliminary version of the design appeared as a conference article [1]. This paper extends the version with protocol designs, power level design, proofs of theorems about the design, and performance evaluations set in the context of 802.11 DCF and PCF. Our prior work on ad-hoc protocols for vehicle-vehicle communication appears in [2], [8].

Xu [8] and Korkmaz [9] present preliminary ad hoc protocol designs to enhance broadcast message reception for safety over a single DSRC channel. These ad-hoc approaches generally obtain reliability by increasing repetitions, handshaking, acknowledgements, i.e. trading reliability with goodput efficiency. Enhanced Distributed Coordination Function (EDCF) [10] of IEEE 802.11e is a single channel protocol that tries to reduce access delay for delay-sensitive messages. However, it does not solve the hidden terminal problem for the broadcast communication. Any of these ad-hoc protocols could potentially be used as the ad-hoc component of the design in this paper.

To adapt any of these ad hoc protocols for the DSRC multi-channel environment, the channel coordination problem must be addressed. Our preliminary simulation shows that if each vehicle is equipped with an 802.11a radio, and the radio is allowed to switch out of the safety channel for non-safety services, the safety performance in the safety channel degrades dramatically as service time increases (see figure 10 in section VIII).

Multi-channel MAC protocols in the literature try to increase the overall throughput of the network by permitting multiple disjoined communications to occur simultaneously over multiple channels. There are two classes of approaches. The first is the multi-radio multi-channel approach (e.g. [12]–[15]) and the second is the single-radio multi-channel approach (e.g. [16]–[18]).

For the multi-radio multi-channel protocols, the general approach is to have one radio, called control radio, dedicated to the control channel used to reserve data channels, and one or more radios, called data radio(s), conduct the actual data communications on any of the remaining channels. The channel reservation process is an extension to the 802.11 RTS-CTS handshake [11], where the sender first transmits a RTS to its receiver containing a list of free channels observed by it. If its receiver agrees with any one of the channels on the list, it replies with a CTS with the chosen channel; and finally before they tune their data radio to the chosen channel, the sender transmits a confirmation so that the potential interferers around the sender will not use the same channel.

Various criteria areused by the sender and its receiver to choose the "best channel" to conduct their data communication. In the DPC [12] and DCA [13] protocols, each node tracks the current usage of each channel, the criteria for "best channel" is one which is not current being used. The criteria in the MMCCS [14] protocol is to choose a channel that maximizes the signal-to-interference-ratio (SINR) at the receiver and minimizes the interference caused to all other active receivers. Similarly, RBCS [15] tries to pick the clearest channel at the receiver (i.e. the channel that has the lowest SINR measured at the receiver). By contrast, we focus on an architecture able to deliver value even to a vehicle with one 802.11 radio.

The single-radio multi-channel protocols are as follows. In CHAT [16], time is slotted, and each node hops from one channel to the other, spending one time slot in each channel, in a known channel hopping pattern. In each time-slot, when a sender has data to transmit to its receiver, it contends for channel access using a protocol like RTS/CTS . After the sender and its receiver gain the right to access the channel, they stay in the current channel to conduct their data communication while others continue the hopping schedule. Once the data communication is finished, the sender and its receiver quickly re-synchronize to the hopping schedule. Since at any given hop, not every node is in the same channel, broadcast communication is difficult. To solve this problem, CHAT requires each node to store a list of receivers within broadcast range. When a node has a message to broadcast, it repeats the same message over different hops until all receivers on its list receive the message.

To increase parallelism, SSCH [17] removes the constraint of having every node use the same channel hopping sequence. Each node in SSCH has its own hopping sequence. To ensure each node can find its receivers, it is required to periodically announce its hopping schedule. When a node has a message to send, it either waits until its receiver eventually meets it on the same channel or the sender partially synchronizes to its receiver's schedule. For broadcast communication, SSCH suffers the same problem as CHAT. Each node in SSCH repeatedly transmits its broadcast message over different hops/channels, and the number of repetitions is a design parameter. Obviously frequent channel switching limits the overall channel utilization for these protocols. Furthermore, safety applications such as Cooperative Collision Avoidance (CCA) require each vehicle to periodically broadcast its position information. Having each safety message be repeated for the benefit of each receiver will deteriorate efficiency.

MMAC [18] tries to reduce the overall channel switching overhead by taking advantage of the IEEE 802.11 Power Saving Mechanism [11], where ATIM windows are modified for channel reservations, and rest of the interval is used for data communication on channels. Each node is required to synchronize to the ATIM window. In each ATIM window, each node is required to return to the default channel for channel reservations. The channel reservation process is based on the RTS/CTS mechanism. At the end of each ATIM interval, a sender begins its data communication with its receiver on their chosen channel. However, the authors did not address the broadcast communication. All these single radio approaches require stringent time synchronization, which remains an open problem for Vehicle Ad-Hoc Networks (VANETs).

In the DSRC service hot-spot, the DCAP protocol configuration contributed by this paper provides broadcast communication with bounded latency. The maximum service channel utilization can be as efficient as the single-radio multi-channel protocols. Since each vehicle requires a single radio, our system would be as economical as the other single-radio multi-channel solutions discussed. The DCAP configuration protocol is feasible for VANET since it does not require every vehicle along the highway to be time synchronized. Finally, the protocol is built on top of the 802.11 DCF and PCF [11], which are widely accepted by the industry, therefore, the development time and cost can be greatly reduced. As the results in section VIII show, the DCAP configuration outperforms DCF or PCF alone. Therefore we believe it constitutes a step in the right direction. However, until vehicle safety applications are better understood it will remain unclear whether even the DCAP performance levels are good enough.

III. Architecture

Our design for concurrent safety and non-safety communications relies on roadside access points. We distinguish between two kinds of access points as follows:

- *Service access point (SAP)* - A roadside unit (RSU) that provides non-safety services, called a *service access point*, should conduct these services within an *access point service region*. Only vehicles located within this region should avail of these services. The SAP will advertise its services in the control channel but conduct the transactions in a service channel. We will use the terms service region and hot-spot interchangeably.
- *Coordinating access point (CAP)* - An RSU that coordinates the safety and service transmissions in its proximity is called a *coordinating access point*.

A single access point could be both SAP and CAP.

A. System Configurations

We propose two configurations based on these two kinds of access points. The configurations differ in their performance and cost. In the first configuration, a *coordinating* AP is co-located with one or more service AP's. Since all coordination functions are executed on the control channel, the coordinating AP dedicates its radio to the control channel. The *service* AP's could dedicate their radios to the service channels. This configuration is called *dedicated coordinating* AP (DCAP).

In the second configuration a single RSU shares the service and coordinating AP responsibilities by cycling between the control and service channels. This configuration reduces cost but, as we shall see, also reduces service channel throughput. This configuration is called the *integrated coordinating* AP (ICAP).

The DCAP configuration is the basic design. Modifications required for the ICAP configuration are pointed out as necessary.

B. Time division of the Control Channel

Figure 2 shows the basic time division in the control channel. Time is partitioned into periodic, regulated intervals, called the *repetition period*. The period should be of length T, where T is determined by the maximum tolerable latency of safety messages[2]

[2] One may object to setting the repetition interval equal to the safety delay requirement. The delay jitter inherent in any protocol implementation would likely cause the violation of a strict T sec. latency guarantee. One may also argue that if the proposed arrangement only ensures that each vehicle have a transmission every repetition period, and if the safety messages are not strictly periodically generated, then achieving a T second delay requirement mandates that the repetition interval be $T/2$.

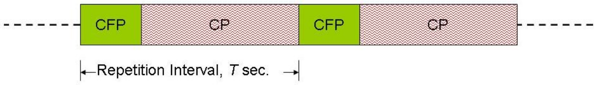


Fig. 2. Basic time division in the control channel

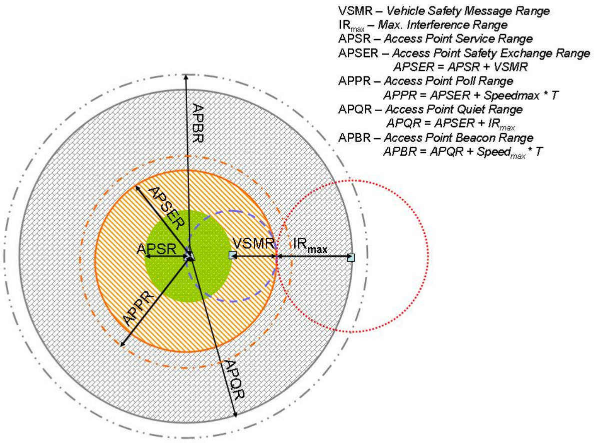

VSMR – Vehicle Safety Message Range
IRmax – Max. Interference Range
APSR – Access Point Service Range
APSER – Access Point Safety Exchange Range
APSER = APSR + VSMR
APPR – Access Point Poll Range
APPR = APSER + Speedmax * T
APQR – Access Point Quiet Range
APQR = APSER + IRmax
APBR – Access Point Beacon Range
APBR = APQR + Speedmax * T
APBR
APSER
APSR
VSMR
IRmax
APPR
APQR

Fig. 3. The spatial division around the AP

We permit vehicles to transmit a safety message once per CFP, i.e., approximately once every T seconds. Each period is divided into two sub-periods: a regulated *contention-free period* (CFP), and unregulated *contention period* (CP). During the CFP, each vehicle in a region, defined later called the *access point safety exchange region*[3], is individually polled. At this point the vehicle can transmit its safety messages while all others must remain silent. This process is similar to the *point coordination function* PCF [11]. The CP follows the completion of the CFP. During the CP,

- vehicles located in the service region can receive services by switching to service channels,
- the remaining vehicles can send safety messages using an ad-hoc protocol,
- the coordinating AP executes control functions in preparation for the next CFP (see section IV-B).

We define the *available service transaction time* (ASTT) as the largest fraction of time a vehicle within the service region is permitted to stay on the service channel. The ASTT for vehicles within the service region is approximately $\frac{T-\|CFP\|}{T}$. This neglects the channel switching time which for 802.11a radios can be made as small as 40-80μs [20]. Non-safety service providers want high ASTT. Our protocol design objective is to maximize ASTT while ensuring safety message communication with acceptable latency and reliability. Latency is determined by the choice of T and reliability has to do with suppressing collisions through the spatial division described in the next subsection.

Our design resides in the CAP and vehicle protocol entities as described in section V. The CAP communications will enable the vehicle to know when to leave the control channel and return again. The SAP and service channel protocols will need to be able to handle a vehicle that departs periodically to the control channel. Other than this no other design modifications are proposed for the SAP or service channel protocols.

C. Spatial division and communication range

We propose the spatial division in figure 3. For the sake of the discussion, all communication ranges in this paper are represented as ideal circles. These are subsequently translated into transmission power levels as described in section IX.

We use the notation $\Re(X, R)$ to denote a circular region centered at radio X with radius of R. Thus, to describe the *access point service region*, we use $\Re(AP, APSR)$, where $APSR$ is the radius of the service region. Vehicles within this region are expected to depart for the service channel during the CP.

The purpose of the spatial division is to ensure all vehicles within $\Re(AP, APSR)$ send and receive all relevant safety messages during the CFP, i.e., before they depart to the service channels in the CP. The protocol logic is set up to provide each vehicle in $\Re(AP, APSR)$ the opportunity to execute a full safety exchange (FSE) in the CFP. A vehicle executes an FSE when all safety messages generated by it within the last T seconds are received by all their intended recipients, and all safety messages intended for the vehicle and generated within the last T seconds are received by the vehicle. In practice, as

[3] The service region is always contained in the access point safety exchange region.

Control Packet Type	Range	Functional Descriptions
Beacon	APBR	used to notify vehicles for the schedule of the contention free period (CFP)
CF$_{Start}$	APBR	used to notify the beginning of the CFP
CF$_{Poll}$	APPR	used to notify a vehicle for the right to transmit
CF$_{End}$	APBR	used to notify the end of the CFP
Service$_{release}$	APSR	used to notify vehicles within the service region for the schedule of next CFP
ServiceAnn	APSR	used by service providers to announce their services on the control channel
Assoc$_{Req}$	APBR	used by vehicles to request to be added to the poll list
Assoc$_{Resp}$	APBR	used by AP to respond to the add request
De-Assoc$_{Req}$	APBR	used by vehicle to request to be removed from the poll list
De-Assoc$_{Resp}$	APBR	used by AP to respond to the remove request

TABLE II
THE LIST OF CONTROL PACKET TYPES

seen from the simulation in section VIII, some fraction of these messages will be lost due to fading or packet collision. It is assumed the intended recipients of a a safety message generated by vehicle v are all within the region $\Re(v, VSMR)$, where VSMR abbreviates Vehicle Safety Message Range. This number is estimated to lie between 50 and 300 meters [5].

Let

$$APSER = APSR + VSMR. \tag{1}$$

$\Re(AP, APSER)$ is called the *access point safety exchange region*. Since the maximum range of a safety message is limited to VSMR, all vehicles within $\Re(AP, APSER)$ must be polled by the AP within the CFP to give each vehicle in $\Re(AP, APSR)$ the opportunity to execute a full safety exchange.

Let

$$APPR = APSER + \Delta \tag{2}$$

where $\Delta = \nu_{max} \times T$ is the maximum possible distance a vehicle can travel in one period T. $\Re(AP, APPR)$ is called the *access point poll region*. We require the poll to be sent with sufficient power to reach all vehicles within $\Re(AP, APPR)$. The extra transmission distance Δ is used by the AP to notify vehicles that they are about to enter $\Re(AP, APSER)$. These vehicles will register with the AP in the CP as described in Section V-A. Thus when they enter the $\Re(AP, APSER)$, the AP will be ready to poll them.

Let IR_{max} denote the maximum possible distance at which a safety message transmission from one vehicle can interfere with reception of a safety message at another. IR_{max} is determined by the transmission power required to cover the VSMR[4]. Let

$$APQR = APSER + IR_{max}. \tag{3}$$

For every vehicle in $\Re(AP, APSER)$ to receive safety messages without collision, vehicles within $\Re(AP, APQR)$ must be silent during the CFP unless polled by the AP.

To ensure silence we require the AP to transmit a beacon with sufficient power to reach all vehicles within $\Re(AP, APBR)$, where

$$APBR = APQR + \Delta. \tag{4}$$

$\Re(AP, APBR)$ is called the *access point beacon region*. We require every vehicle receiving a beacon to keep quiet unless polled by the AP. Once again, the extra distance Δ is used to notify the vehicles about to enter $\Re(AP, APQR)$ to keep quiet until the CFP is over. The beacon frame in this protocol specifies the number of time slots before the next CFP starts. This makes it slightly different to the beacon frame in 802.11.

IV. DCAP DESIGN: DATA MODEL

This section describes the different kinds of control packets and frames in the DCAP design. The various packets are summarized in table II.

[4] In such scenarios, IR_{max} is generally larger than VSMR.

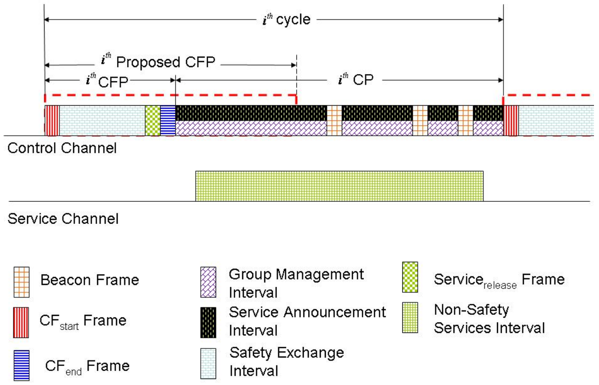


Fig. 4. The timeline of control and service channel (only one service channel shown) during the i^{th} cycle.

A. *Collision Free Period*

As shown in Figure 4, each system cycle starts with a CFP. The CFP begins with a CF$_{start}$ frame, proceeds to a *safety exchange* interval, and typically ends with a Service$_{release}$ frame followed by a CF$_{end}$ Frame. Each CFP has an announced duration. However, the AP may end the CFP before this proposed CFP length after it completes polling all vehicles in its poll region. The difference between CFP duration and Proposed CFP duration in figure 4 illustrates this. To start a new CFP, the AP transmits a CF$_{start}$ frame with enough power to reach every vehicle in the beacon region ($\Re(AP, APBR)$). The *safety exchange* interval is used by vehicles within the $\Re(serviceAP, APSR)$ to conduct their *safety exchange*s. The coordinating AP polls each vehicles on its poll list. To allow sufficient time for each vehicle to reset its hardware from transmit state to receive state and vice-versa, every transmission in the CFP is separated by a *Short Interframe Spacing* (SIFS) [11]. Since vehicles within the service region ($\Re(AP, APSR)$) switch to the service channel during the CP, they miss all the beacons. Instead the Service$_{release}$ frame informs them of the schedule of the next CFP. This frame is transmitted with just enough power to reach vehicles within the service region. The Coordinating AP ends a CFP by transmitting a CF$_{end}$ frame. The CF$_{end}$ is transmitted with the same power as the CF$_{start}$ frame.

B. *Collision Period*

The end of CFP is followed by the collision period (CP). Vehicles in the service channel are free to leave for the service channel during this time. The Coordinating AP performs group management functions, advertises available services, and sends beacons to inform all vehicles (including newly arriving vehicles) of the upcoming CFP schedule.

1) Group management: The *group management interval* is used by vehicles entering or leaving $\Re(AP, APPR)$ to notify the AP of their presence. This enables the AP to ensure its poll schedule will include all vehicles needed to complete the *safety exchange*s required by vehicles in the service region. Upon reception of an association or de-association request from a vehicle, the AP replies with a confirmation (e.g. association response or de-association response) to the vehicle, and adds or removes the vehicle from its poll list. In the ICAP configuration the AP will need to stay on the service channel for part of the CP to execute the group management function. This will reduce ASTT.

2) Service announcements: The service announcement interval is used by the APs to advertise the services offered in the service region on the service channels. The DCAP design is agnostic to the format of these announcements. For example, the standards in [28] are compatible with this design. In the ICAP configuration the AP will have to switch out of the service channel during the CP to make these announcements on the control channel. This will also reduce ASTT.

3) Beaconing: To create a CFP in the i^{th} cycle, the AP has to transmit beacons in the $(i-1)^{th}$ cycle. Every vehicle that receives a beacon will update its network allocation vector (NAV). The vehicle will remain silent for the duration of the CFP (duration of the NAV) unless it is polled. Vehicles that do not receive any of the beacon transmissions during the CP will continue to operate using the *ad-hoc* protocol throughout the next CFP. They can potentially interfere with the reception of polled messages during the CFP. Since the control channel is not centrally scheduled during the CP, the beacons sent by the AP must contend for channel access just like any vehicle message, i.e. their transmission and reception is not guaranteed. They do this using the ad-hoc protocol. Clearly, the probability of beacon reception is critical to the reliability of the safety exchanges during the CFP. To increase the probability of beacon reception the AP may optionally repeat its beacon multiple times, as shown in figure 4. Vehicles that receive at least one beacon in the $(i-1)^{th}$ cycle will set their network allocation vector (NAV) to the end of the i^{th} CFP, i.e. they will not interfere during the i^{th} CFP.

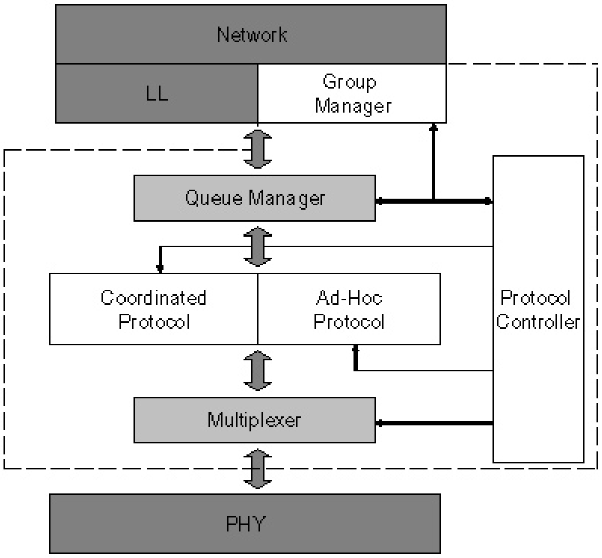
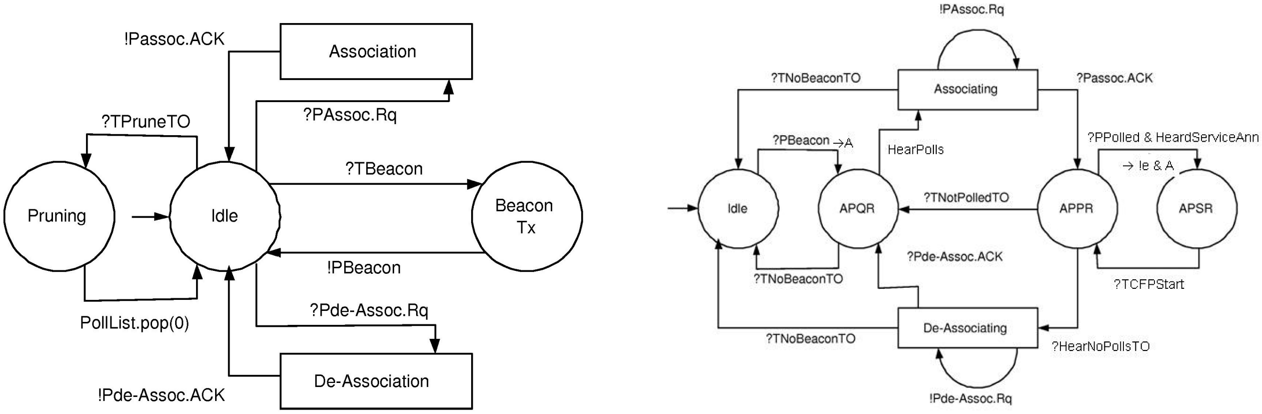


Fig. 5. The Medium Access Control (MAC) Protocol Architecture



(a) AP

(b) Vehicle

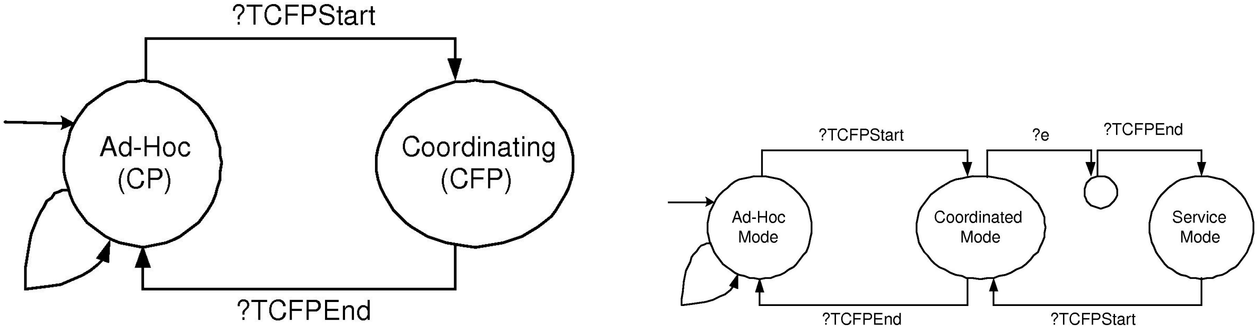
Fig. 6. Group Management Protocol State Machine

V. DCAP Design: Protocol

Figure 5 shows the DCAP protocol architecture. This section describes designs for the components in the dashed box.

Vehicle communication is intended to be under the control of the *Coordinated Protocol Entity* during the CFP and the *Ad-hoc Protocol Entity* during the CP or when out of range of a Coordinating AP. The *Protocol Controller Entity* manages this transition. It does so by controlling the data path in the *Multiplexer Entity*. The *Group Manager* manages the joining and leaving of vehicles from the Coordinating AP poll list. The *Queue Manager* in the figure passes packets on demand to the *Ad-hoc* or *Coordinated* protocol entities. Likewise it accepts packets from the Coordinated Protocol or Ad-hoc Protocol entities on demand, demultiplexes them, and passes them on to the *Group Manager* or *LL*. The Queue Manager in our current simulator implements a FIFO queue. It could be modified to implement a priority queue as suggested in the DSRC standards.

The notation convention for the state machines is as follows. Transitions are labeled with input events (events received by the state machine), output events (events output by the state machine), and predicates or actions on internal variables of the state machine. Input event names are preceded by a *?*, output event names by a *!* and predicates or actions by nothing at all. A label like $?e, P \rightarrow !f, A$ on a transition means the transition is triggered if predicate P on variables read by the machine is true, and event e is received. Completion of the transition will result in output of the event f and action A. A may change values of some variables, start timers, and so on. Events are usually timeouts or packets exchanged with other protocol entities. A packet event name begins with a *P* and a timeout event name with *TO*. The timers are shared variables written by one protocol entity and read by one or more entities.



(a) AP

(b) Vehicle

Fig. 7. Protocol Controller

A. Group Manager

The *Group Manager* state machine for the CAP is in figure 6(a) and that for the vehicle in figure 6(b). The initial state of the vehicle *Group Manager* is Idle. It stays in the Idle state unless it receives control messages from a CAP. When the *Group Manager* receives a beacon message, i.e., it is within $\Re(AP, APBR)$,it switches from state Idle to APQR, and sets a CFPStart and CFP end timer. This is denoted by the transition label $?PBeacon \rightarrow A$. A abbreviates the actions *SetCFPStartTimer, SetCFPEndTimer*. These timers are read by the *Protocol Controller*. While in APQR it executes the same timer set actions every time it receives a beacon, i.e., there is a self loop transition at APQR, not shown in the figure, labeled $?PBeacon \rightarrow SetCFPStartTime, SetCFPEndTimer$. The same self-loop exists at states *Associating, De-Associating* and *APPR*.

The *Protocol Controller* receives the TCFPStart and TCFPEnd inputs when these timers count down to zero. When the *Group Manager* is in the APQR state, it will switch back to Idle if no beacon is received within a timeout period. Alternatively it will switch to Associating when a poll message is received, i.e., it is within $\Re(AP, APPR)$. In the Associating state, the *Group Manager* tries to register with the AP, to ensure it will be polled in the next CFP. The association process is as follows. The *Group Manager* generates an association request, passes the message to the Queue Manager and activates a retry timer with a timeout parameter called *GMRTimeout*. This is not shown in the figure. The *GMRTimeout*is chosen to give acceptable association and de-association performance. Upon the reception of the association response, the *Group Manager* de-activates its retry timer, and advances from its current state to APPR. Otherwise, it keeps retrying whenever the retry timer expires, staying in the Associating state until it is acknowledged. When in the APPR state, if it hears polls, but is not polled for the duration NotPolledTO, it will switch back to Associating. If it is polled and has heard service announcements, signifying it is in $\Re(AP, APSR)$, it sets the CFP start and end timers, outputs an event e and transitions to state APSR. The purpose of e is to permit the protocol controller to transition to *Service Mode* at the appropriate time. On the other hand, if it does not hear polls for a certain duration, signifying it may be outside $Re(AP, APPR)$, it will switch from the APPR state to the De-Associating state. In the De-Associating state, the *Group Manager* tries to de-register from the AP. It uese a re-try behavior like that in the Associating state.

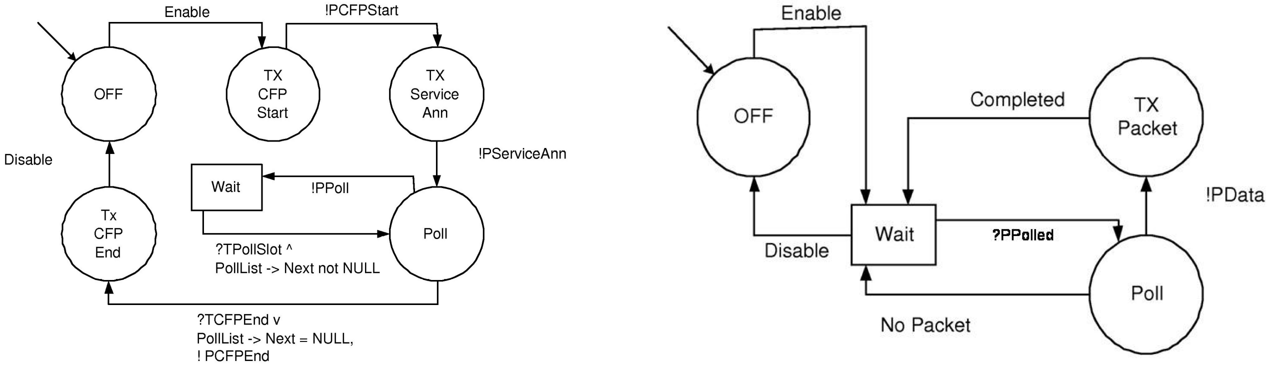
At all states, if the *Group Manager* does not receive any beacon for a timeout period, it automatically switches back to the Idle state. This transition is not shown for all states in the figure. In the system evaluation, all timeouts are equal to the cycle time.

Since the vehicle de-registering is at least distance APPR away from the AP, the request and confirmation messages are transmitted at beacon power level to ensure they will reach the AP. The association and de-association requests do not significantly load the channel. Assuming a maximum flow of 2200 vehicles/hour/lane, and an eight lane highway, there should be an average of one vehicle registering or de-registering per 100 ms.

The peer protocol entity on the CAP is relatively straightforward. It responds to association, de-association requests, and transmits beacons periodically. Every entry on the poll list has a lifetime. The pruning loop in the state machine pops the poll list at the appropriate intervals.

B. Protocol Controller

Figure 7(b) is the state machine specification of the *Protocol Controller* in the vehicle, and figure 7(a) that in the CAP. In the vehicle, the *Ad-Hoc Mode* is the default state. In this state, the *Protocol Controller* enables the MAC to operate in the *Ad-Hoc* protocol by configuring the Multiplexer to route packets between *Ad-Hoc* protocol entity and the *PHY* layer. Likewise in Coordinated Mode, it sets the *Multiplexer* to route packets between the *Coordinated* protocol entity and the *PHY*. The *Protocol Controller* moves from Ad-Hoc Mode to Coordinated Mode and back based on the CFPStart and CFPEnd timers



(a) AP

(b) Vehicle

Fig. 8. Coordinating Mode State Machine

set by the *Group Manager* as described in the *Group Manager* subsection. Likewise when the *Group Manager* moves into its APSR state it emits an event *!e* (see figure 6(b)). This drives the protocol controller into Service Mode when the current CFP ends. It stays there till the start of the next CFP.

When the CFPEnd timer expires the *Protocol Controller* switches from Coordinated Mode back to Ad-Hoc Mode unless the *Group Manager* is in the APSR state and receives the schedule of the next CFP via the Service$_{release}$ frame. In this case, the *Protocol Controller* will change its current state to Service Mode. This co-ordination between *Group Manager* and emphProtocol Controller is not shown in the figures.

We do not specify the state of the Multiplexer when the protocol controller is in the Service Mode. The MAC could operate in the ad-hoc mode or follow a third *service channel* protocol not specified here. When the CFPStart timer expires again the *Protocol Controller* transitions back from Service Mode to Coordinated Mode again.

The peer protocol entity in the CAP is straightforward. It is time driven with its transitions triggered by CFPStart and CFPEnd timers.

C. Coordinated Protocol

The state machine in figure 8(b) specifies the vehicle's *Coordinated* protocol entity. Figure 8(a) specifies that in the CAP. The default state is OFF meaning the protocol does not transmit or receive any messages. The entity is enabled, i.e., transitions into the Wait state, when the *Protocol Controller* transitions into Coordinated Mode. In the wait state the entity can receive messages but is not allowed to transmit unless polled. The reception path is not shown in the figure. It simply passes all received messages up to the queue manager. When it is polled, it switches from the Wait state to Polled, and asks the *Queue Manager* for a safety packet or *Group Manager* packet to transmit. If the *Queue Manager* is currently empty, it immediately switches to Wait. Otherwise, it advances to the TX Packet State, and prepares the packet for transmission. Once transmission is done, it switches back to the Wait state. When the *Protocol Controller* transitions out of Coordinated mode, this entity is disabled, i.e, it transitions back to the OFF state.

The protocol entity in the CAP (figure 8(a)) is also enabled when the *Protocol Controller* is in Coordinating mode and disabled otherwise. When enabled, it transmits a CFPStart frame, service announcements, and polls vehicles on its poll list. Finally when the CFPEnd timer expires or it reaches the end of its poll list, it sends out a CFPEnd frame.

D. Ad Hoc Protocol

Our aim is to be compatible with a variety of ad-hoc protocols. Some examples are the protocols in [8]–[10] or 802.11DCF. The evaluation in this paper is based on 802.11DCF as the ad-hoc protocol.

Since 802.11DCF relies on the virtual carrier sensing through the *network allocation vector* (NAV), the *Protocol Controller* updates the NAV to reflect the start and the end of the CFP. We require some modifications to the standard 802.11DCF. First, we introduce the OFF state, which allows the *Protocol Controller* to switch it on or off. Secondly, whenever the protocol is enabled, it has to randomly back-off first before contending for channel access. Since nodes not polled in the CFP (e.g. nodes in $\overline{\Re(AP,APSR)}\bigcap\Re(AP,APBR)$) may have buffered their safety packets during the last CFP. If they all transmit at the beginning of the CP, their messages will collide with each other. Finally, whenever the protocol successfully gains access to the channel, it has to check whether there is sufficient time to transmit the current packet (i.e. check the packet transmission time against the time before the next CFP) to prevent interference at the beginning of the CFP. If the remaining time is not sufficient, it pushes the packet back to the *Queue Manager* and keeps silent.

VI. DCAP Design:Logical Properties

The design in this paper has been created to have certain logical properties. These are summarized as theorems in this section. The proofs are in section XI.

The logical properties are safety and efficiency properties. For safety, we have sought to enable a *full safety exchange (FSE)* every cycle for every vehicle. A vehicle experiences a Full Safety Exchange in a cycle if all neighboring vehicles within distance VSMR receive a safety message from the vehicle during the cycle and the vehicle receives a safety message from all the same neighbors within the cycle. Needless to say, due to collisions or fading this does not always occur. Nevertheless, the design strives to give each vehicle the opportunity for an FSE. For efficiency, we have sought to maximize the fraction of time spent on the service channel per cycle by each vehicle in the service region, subject to the constraint that each vehicle receive the opportunity for an FSE. The fraction is quantified by the ASTT (Available Service Transaction Time) as defined in section III-B.

The quantities APBR, APSR, APSER in this section are as defined by equations 1, 2, 3, and 4 in section III,. Likewise the CP and CFP are also as defined in the same section. $\overline{S}$ denotes the complement of the set S. The following notation is also used in this section.

- t_i: Starting time of the $i-$th cycle.
- T: Duration of each cycle.
- δ_{max}: Maximum duration for each CFP.
- $D_i(n, r)$: The set of nodes within a circle centered at node n, with radius r, during the time interval $[t_i, t_{i+1})$.
- δ_i: Duration of the CFP in the i^{th} cycle. Note $\delta_i < \delta_{max}$.
- $FSE_i(n, r)$: Full safety exchange indicator function for a node n and range r in CFP_i. It is 1 if node n experiences an FSE with all vehicles in $D_i(n, r)$ in the period CFP_i, and is 0 otherwise.

We assume $\delta_{max} < T$. To a first order δ_{max} is

$$\delta_{max} = APPR * vehicleDensity * numberOfLanes * 2 * transmissionTime \tag{5}$$

$$transmissionTime = \frac{safetyMessageSizeInBits}{transmissionRate} \tag{6}$$

The idealizations made to establish the theorems are as follows.

Assumptions::

1) The proof uses a collision model. Each transmission has a specified range and each node has a location. A transmission is received if the distance between transmitter and receiver is less than the specified range and there is no collision. A collision occurs if one or more nodes within interference range (IR_{max}) of the receiver transmit concurrently.
2) Maximum interference range for nodes other than the AP is IR_{max}.
3) Each node other than the AP has only one radio, and the radio can only receive data on one channel at a time.
4) If x is a poll range, then a node n is polled in CFP_i iff node n is in $D_i(AP, x)$.
5) Each node executes the state machines in section V.
6) Nodes move in discrete steps, and they change position at the t_i's. The maximum distance a node can move in a time step is $\nu_{max} \times T$.
7) The number of vehicles in a given area is proportional to the size of the area.
8) The AP transmits beacons periodically in $[t_i, t_{i+1})$. There is at least one beacon transmitted in $[t_i, t_i + \delta_i)$.

The first theorem asserts the FSE safety property targeted by the DCAP design. It is achieved under the assumptions above and by hypothesizing that every vehicle in the beacon region receives a beacon in every cycle. Thus in practice, the design must be configured to ensure high beacon reception probability (see figure 15 in section VIII).

Theorem 1: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then every node in $D_i(AP, APSR)$ will complete its full safety exchange (FSE) in CFP_i.

The next theorem asserts our poll range is minimal assuming the FSE requirement has to hold. The minimality of the poll range is required to argue the minimality of the CFP and the maximality of the ASTT.

Theorem 2: Let *poll_range* be a poll range other than $APSER$. If poll range has the property that for any i and node $n \in D_i(AP, APSR), FSE_i(n, VSMR) = 1$, under the assumption of Theorem 1, then $poll\_range \geq APSER$. If $\delta_i \propto |D_i(AP, poll\_range)|$, then when $poll\_range = APSER$, δ_i is minimized.

The next theorem asserts the minimality of the beacon range assuming the FSE property has to hold. This is important because the beacon interferes with the safety messages of vehicles that are not interested in using the service channel (see figure 12 of section VIII), i.e., it deteriorates safety message reception for vehicles in the outer part of the APQR and beyond the APQR. Thus it is important it be minimized.

Theorem 3: Let *beacon_range* be a beacon range other than $APBR$. If beacon range has the property that for any $n \in D_i(AP, APSR)$, $FSE_i(n, VSMR) = 1$ under the assumption of Theorem 1, then $beacon\_range \geq APBR$. When $beacon\_range = APBR$, number of silent nodes, i.e. $\overline{D_i(AP, APSER)} \cap D_i(AP, APBR)$, in CFP_i is minimized.

The following theorem establishes the latency bound on safety messages in terms of the parameters of the DCAP design.

Data Rate	6Mbps
Message Rate	1 message per 100ms
Safety Message + Header	150 bytes
AP System Cycle	100ms
Transmission Opportunity per Polled Vehicle	1
GMRTimeout	10ms

TABLE III
SIMULATION PARAMETERS

Theorem 4: If every node in $D(AP, APBR)$ receives a beacon in both $(i-1)^{th}$ and i^{th} cycles, then for every node l in $D(AP, APSER)$, the time between consecutive polls is bounded by $T \pm \delta_{max}$.

The last theorem summarizes the safety and efficiency properties. It relies on theorems 1 and 2.

Theorem 5: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then the protocol is safe and efficient for all nodes n in $D_i(AP, APSR)$ in the following sense

1) $FSE_i(n, VSMR) = 1$
2) The service time, $T - \delta_i$, is maximized.

VII. SIMULATOR

We evaluate the protocol configurations of interest by simulating a 4-lane highway at capacity, i.e., with a flow of about 2200 vehicle/hour/lane at an average speed of 55 mph. The average spacing between vehicles at this flow and speed is approximately 30 meters. This is the typical maximum flow condition for U.S. freeways and therefore creates the largest number of vehicles registering and de-registering with the CAP.

The CAP is installed at the midpoint of the simulated highway, with APSR = 80 meters (see figure 9). At about 80 meters the RSSI of the DSRC radio transmitting at the 27 Mbps setting moves into the -80 dBm to -70 dBm range (see figure 110, Appendix G in [5]). Thus we choose the nominal APSR to enable reliable communication at the 27 Mbps data rate[5]. The highest supported DSRC data rate for non-safety services is 27 Mbps, since DSRC prefers non-safety service channels be 10 MHz wide, and it is based on 802.11a chipsets offering a maximum of 54 Mbps over 20 MHz channels [28]. Larger APSR values are also evaluated to provide insight into the behavior of the design.

All safety messages are exchanged in a 20 MHz channel at 6 Mbps. Though DSRC channels are usually 10 MHz, the FCC ruling permits two 10 MHz channels to be combined to form a 20 MHz channel if necessary. In our opinion, the performance results in section VIII show the necessity. Field work shows 6 Mbps over a 20 MHz channel is the recommended data rate for safety message exchange (see page 107, Appendix G, in [5]).

We use vehicle trajectories generated by the SHIFT traffic simulator [29]. This has been validated with actual data from Interstate I-880 [30].

We have implemented the DCAP protocol design in *NS*-2 [24]. The trajectories output by SHIFT are input to NS-2 which in turn outputs the communication network performance data. The DCF and PCF implementations already exist, though DCAP requires some modification to the DCF CSMA implementation. We build on the DCF and PCF [25].

We use a collision model to capture multiple access interference. Every message has a transmission range and interference range. If a receiver node is within transmission range of the sender and no other node within interference range of the receiver transmits concurrently, the receiver node receives the transmission. We need a power attenuation model to determine the interference range corresponding to a transmission range. This is the content of sub-section VII-A. Since all message losses in our simulations occur due to collision, in reality there will be additional message losses due to shadowing and small-scale fading. These will degrade the performance of all the evaluated protocol configurations. The magnitude of these additional losses will depend on the shadow or fade margins incorporated when determining the transmit power of a message.

We use a collision model in our simulations. This is because no consensus exists on fading and shadowing models for vehicle-vehicle communication. Amongst other things, these would depend on the type and mounting of antennas on vehicles and these are still being debated. Thus our performance results can only be interpreted relative to the DCF and PCF baselines derived and included in this paper. In practice, performance of both design and baselines will be worse due to additional losses caused by fading.

The basic simulation parameters are listed in Table III. All messages are transmitted at 6Mbps as stated above. The CAP system cycle is 100 ms, so that vehicles within $\Re(AP, APSER)$ are given an opportunity to transmit a safety message once every 100 ms. GMRTimeout is chosen to be 10ms. If a vehicle does not receive an association or de-association response from the AP, it will try again 10ms later. The 150 byte packet size permits inclusion of vehicle speed, GPS position, heading, and about 80 bytes of protocol header [27].

[5] At an 80 meter APSR a vehicle traveling 55 mph is in range of the APSR for over 6 seconds. If ASTT is 80%, as happens in our nominal case, a vehicle could download as much as 16 MB at 27 Mbps.

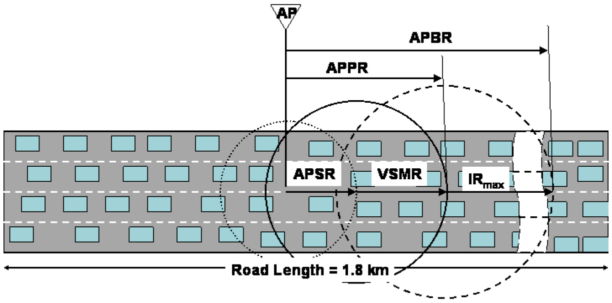


Fig. 9. Network Topology and Communication Ranges. Access Point Service Range = 80 meters, Vehicle Safety Message Range = 150 meters, Access Point Poll Range = 236 meters, and Access Point Beacon Range = 536 meters. Average headway between vehicles is 30 meters

The 100 ms system cycle time means a vehicle gets to transmit a safety message roughly every 100 ms. This is the fastest communication rate envisaged by the Vehicle Safety Communication Consortium (VSCC) for all but one very short range application (page 16 of [5]).

The VSMR is chosen to be 150 meters. This range is chosen to enable a vehicle stopped on the freeway to warn an oncoming vehicle. An oncoming vehicle traveling at 55 mph and decelerating at 2 m/s/s will stop in 150 meters. The stopping distance at a speed determines the largest desired message range [27]. A vehicle approaching at 65 mph will have to decelerate at 3 m/s/s. These are reasonable decelerations, observed during driving, and are well within the capability of almost all drivers and cars.

The 150 meter VSMR range and the 6 Mbps data rate imply IR_{max} is 300 m. This is based on the method in section VII-B. The maximum possible vehicle speed chosen for protocol design is 120 mph, i.e., ν_{max} = 120 mph or 53.64 meters/sec. From these numbers and the equations in section III, APSER = 230 meters, APPR = 236 meters, APQR = 530 meters and APBR = 536 meters. For simplicity, communication range for association and de-association messages are chosen to have the same range as the beacons.

A. Relating Message Range to Interference Range

Message ranges are VSMR for safety messages, APSR for service announcements, and determined by equations (2) and (4) for polls and beacons respectively. All these definitions appear in section III.

The power required to cover a range depends on the data rate. We use the deterministic Friis Free-space model for short distances and the Two-ray model for longer distance [26] to determine the received power. Data rate is determined by modulation and coding. The higher data rates, i.e., larger modulation constellations and smaller code rates, require higher transmission power to cover a given range. We use a data rate of 6 Mbps. We have obtained the Signal to Noise+Interference ratio required at the receiver to receive at this data rate from an 802.11a chipset manufacturer and used it in the calculations below.

Let range be denoted by R, the SINR threshold at the chosen data rate be denoted by β and transmission power by P_t. The procedure is:

1) Calculate the desired received power by $P_r = N \cdot 10^{\frac{\beta}{10}}$ where N is the thermal noise power.
2) Calculate the desired transmission power using the following equation:

$$P_r = P_t K \left[\frac{d_o}{R}\right]^{\gamma}. \tag{7}$$

Here P_t is the transmit power, P_r the received power computed in the previous step, K is a dimensionless constant which depends on the antenna characteristics and average channel attenuation, d_o is a reference distance for the antenna far-field, and γ is the path loss exponent [21]. This is supported by empirical data for free-space path loss at a transmission distance of 100m [23]. The value of γ on the other hand depends on the propagation environment.

B. Calculating IR_{max}

Beacon range depends on the maximum interference range of a safety message transmission IR_{max}. This section describes how to determine IR_{max}. Once IR_{max} is known the beacon transmission power is calculated as in section VII-A. The IR_{max} calculation method is:

1) Calculate P_r and P_t as above for $R = VSMR$.
2) Calculate the minimum power required to interfere (P_i) by $P_i = 10^{\frac{\beta}{10}} P_r$, since if interference prevents reception of the message the of received power to interference power will be less than β in dB.
3) Calculate IR_{max} from

$$P_i = P_t K \left[\frac{d_o}{IR_{max}}\right]^{\gamma}. \tag{8}$$

Note

$$10^{\frac{-\beta}{10}} P_r = P_t K \left[\frac{d_0}{IR_{max}} \right]^{\gamma} \Rightarrow 10^{\frac{-\beta}{10}} \frac{1}{R^{\gamma}} = \frac{1}{IR_{max}^{\gamma}},$$

by substituting equation (7). Thus the relationship is independent of P_t, K, d_0 when γ is the same for R and IR_{max}. We use a 2-ray model with $\gamma = 2$ before the cross-over point and $\gamma = 4$ after. The crossover is at about 240 meters.

VIII. Simulation Results

We evaluate the communication of safety and non-safety messages in a multi-channel environment in three protocol configurations. These are DCF only, PCF in the service hotspot only, and the DCAP configuration which is DCF combined with PCF enhanced with the spatial division in section III.

For the parameter values in section VII the CFP duration is about 21ms. This implies ASTT for vehicles within the service region $\Re(AP, APSR)$ is about 79%. At the maximum flow condition on a four lane highway, this is maximum service channel utilization reached by the DCAP design. On an 8-lane highway the CFP would double and the ASTT would be about 58 %. The channel access delay experienced by a vehicle is 100 msec. The jitter in this delay can be 21 ms, i.e., a vehicle may wait 121 msec between transmissions. Jitter can be substantially less if new vehicles joining the poll list are added to its end. Our implementation does this. Thus we observe a delay that is almost 100 msec with very little jitter. Results in this section show that protocol message loss probabilities are small. The expected values of delay is almost 100 msec.

In addition to these QoS parameters, performance is quantified by the Sender Based Probability of Message Reception (SBPMR) and Receiver Based Probability of Message Reception (RBPMR) defined as follows.

The SBPMR of node x in the i^{th} cycle, $SBPMR_i(x)$, is defined as,

$$\frac{1}{K(i)} \sum_{k=1}^{K(i)} \frac{num\_receiver\_recvd(x,k)}{|D_i(x, VSMR)|}, \tag{9}$$

where $K(i)$ is the number of messages transmitted by node x in the i^{th} cycle, $num\_receiver\_recvd(x,k)$ is the number of receivers in $D_i(x, VSMR)$ that received the k_{th} message. Similarly, the RBPMR of node x in the i^{th} cycle, $RBPMR_i(x)$, is defined as,

$$\frac{num\_message\_recvd_i(x)}{num\_intent\_message_i(x)}, \tag{10}$$

where $num\_message\_recvd_i(x)$ is the number of messages received by x in the i^{th} cycle and $num\_intent\_message_i(x)$ is the number of messages generated by $D_i(x, VSMR)$. The sender based probability of message reception in a region R, $SBPMR(R)$, is defined as,

$$\frac{1}{N} \sum_{i=1}^{N} \frac{1}{|D_i(R)|} \sum_{\forall x \in D_i(R)} SBPMR_i(x), \tag{11}$$

where $D_i(R)$ is the set of nodes in region R in the i^{th} cycle and N is total number of simulation cycles. Under suitable ergodic assumptions, it can be interpreted as the probability that a randomly chosen receiver within range VSMR of a randomly chosen sender will receive a randomly chosen message sent by it. Likewise the RBPMR defined next, can be interpreted as the probability that a randomly chosen message sent by a randomly chosen sender will be received by a randomly chosen receiver within range VSMR. The receiver based probability of message reception in a region R, $RBPMR(R)$, is defined as,

$$\frac{1}{N} \sum_{i=1}^{N} \frac{1}{|D_i(R)|} \sum_{\forall x \in D_i(R)} RBPMR_i(x). \tag{12}$$

Most results are presented in terms of RBPMR since in all but one case the two are equal. In all these cases the plots are marked with the abbreviation PMR. Where the two are distinct we use the abbreviations RBPMR and SBPMR.

We compute the probability of beacon reception to give insight into the performance of the DCAP design. This is calculated over the set of vehicles outside $\Re(AP, APSR)$ and within the $\Re(AP, APBR)$. It is defined as,

$$\frac{1}{N} \sum_{k=1}^{N} \frac{num\_recvd(k)}{num\_intent(k)}, \tag{13}$$

where N is the total number of simulated system cycles, $num\_recvd(k)$ is the number of vehicles in the set that received a beacon in the k^{th} cycle, and $num\_intent(k)$ is the total number of vehicles in the set in the k^{th} cycle.

Figure 10 shows the performance if 802.11 DCF is used without modification. The best PMR with 802.11 DCF is 0.97. This is the baseline we seek to maintain, i.e., the PMR delivered by the DCAP design should be no worse than that delivered by 802.11 DCF. We use 802.11 DCF as our baseline because it is a widely deployed protocol available for the exchange of

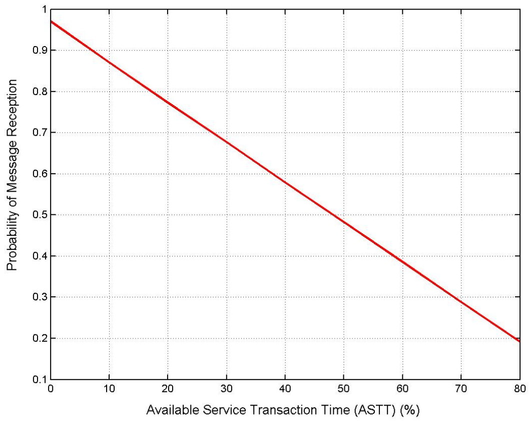


Fig. 10. Adhoc with service

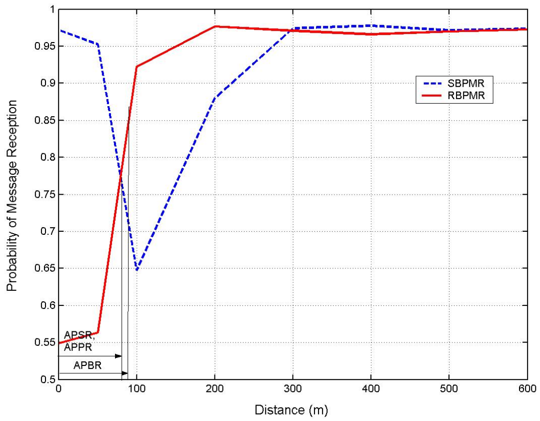


Fig. 11. 80211PCF with channel switching

messages in a vehicular ad-hoc network. As expected, the PMR drops linearly with the time vehicles spend on the service channel. When the service channel time is 80% of 100 msec, the PMR is as low as 0.2. The vehicles leave for the service channel randomly, independently, and asynchronously. Clearly if service channels are to be utilized efficiently better design is required.

Figure 11 shows the performance using PCF in the service hotspot only. Since the DCAP design is an extension of PCF, PCF in the service hotspot only can be viewed as a special case of the DCAP design. It corresponds to $APPR = APSR = APBR$. The AP polls the vehicles in the service region only. Vehicles outside the service region use 802.11DCF. Just as in normal PCF, there is a CFP and CP. During the CFP the service region vehicles are polled to send their safety messages. They depart after the CFP to the service channel. The vehicles outside the service region stay on the service channel the entire time and use 802.11 DCF to send their messages during the CP and CFP.

In figure 11, we plot performance in terms of the sender based probability of message reception (SBPMR) and receiver based probability of message reception (RBPMR) to illustrate the problems of this design. Vehicles within the service region have an SBPMR performance similar to 802.11DCF without service. Vehicles right outside the service region have the worst SBPMR performance because as much as half of their receivers are within the service region, and these receivers are not on the control channel when they transmit in the CP. On the other hand, we see the opposite trend for the RBPMR measure. The receivers inside the service region have poor performance since they are not on the control channel 100% of the time. When their senders transmit, they miss the messages. The opposite is true for receivers outside the service region. They potentially receive each message. Performance is never better than the ad-hoc case by either measure. In a significant region it is worse. Thus PCF needs to be enhanced in some way. Our response is the spatial division added to produce DCAP.

Figure 12 shows the DCAP configuration does not suffer the problem experienced PCF in the service hotspot only. For nodes within the service region, SBPMR and RBPMR are very close to each other. This is the reason for the spatial division added to PCF.

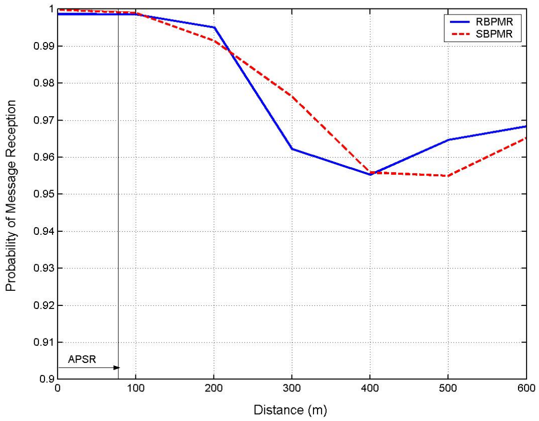


Fig. 12. Coordinated AP Performance

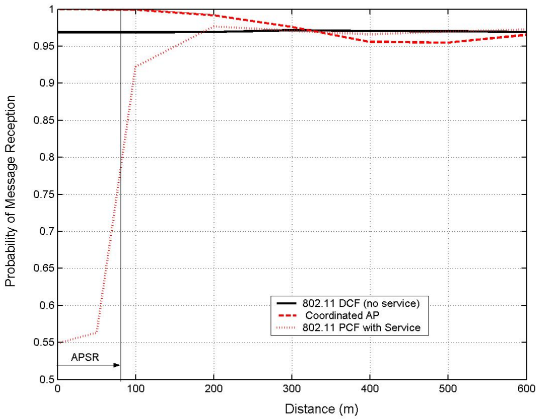


Fig. 13. 802.11 DCF and PCF versus coordinated AP

Figures 12 and 13 show the performance of the DCAP design. Figure 13 combines figures 10, 11, and 12 in the RBPMR measure. Performance upto about 300 meters from the AP is superior to the ad-hoc case. One can see this more clearly in figure 12. The dashed line representing DCAP merges with 1 near the vertical axis. This is so even though the service region vehicles are now spending 80 out of 100 msec on the service channel. Between 300 and 600 meters the performance is poorer than the ad-hoc case. One can see this more clearly in figure 14. The reception probabilities drop down to between 0.95 and 0.96 in comparison to 0.97 in the ad-hoc case. The degradation is less than 2%. The degradation is a function of beacon power, poll power, and beacon rate. These are set by equations 1 through 4. These figures are based on a beacon rate of 3 beacons per cycle. We do not know how to remove this slight degradation to vehicles outside 300 meters. The high power beacon and poll messages cause additional interference reducing performance relative to the ad-hoc case.

Figure 14 shows the sensitivity of the DCAP design performance to the number of beacons per cycle. The DCF line is slightly wavy because of the variations in inter-vehicle spacing along the highway. As the number of beacons is increased performance inside the service region goes up while that in the 300 to 600 meter zone goes down. Thus the number of beacons should not be any larger than necessary. The performance difference inside the service region for 3 and 6 beacons is not significant. While the difference between the 1 and 3 beacon plots is more noticeable. Figure 15 shows the reason for the smaller difference between the 3 and 6 beacon lines. The performance improvement arising from additional beacons is related to the probability the beacons are received. This probability is almost level after 3 beacons. Thus the performance of the DCAP design, in particular the performance balance inside and outside the service region, can be adjusted by varying the number of beacons between 1 and 3.

We choose the beacon power so that the beacon range will be $APBR = APQR + \Delta$ (equation 4), where $APQR = APSER + IR$ (equation 3). Figure 16 shows the impact of choosing $APQR = APSER + \alpha IR$ where α varies between 0.1 and 1. The dashed line represents the worst case performance outside the service region, e.g., the lowest value on the Coordinated AP line in figure 13. As beacon power rises the performance inside the service region improves (solid line) and

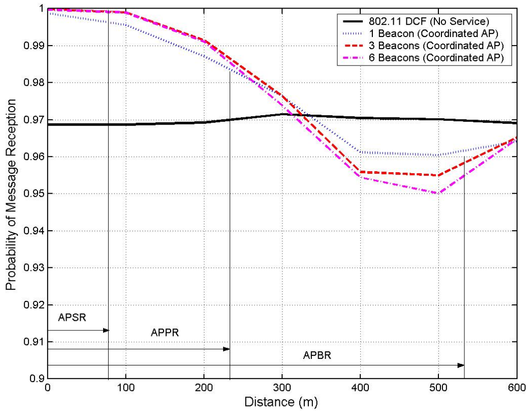


Fig. 14. Coordinated AP Overhead

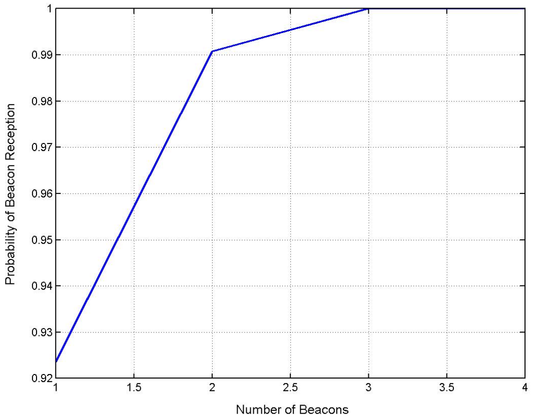


Fig. 15. Beacon reception

that outside the service region drops (dashed line). Thus the performance of the DCAP design, in particular the performance balance inside and outside the service region, can be adjusted by varying the beacon power.

Figure 17 evaluates the ability of the DCAP design to scale to larger service regions. Here as the service region size is being raised, beacon and poll powers are being raised in accordance with equations 1,2, 3, and 4. As the service region size is increased performance outside the hotspot deteriorates. This is because there are more vehicles to be polled in the service region, increasing the length of the CFP. This reduces the CP and thereby also reduces the time available for other vehicles to send their safety messages. We envisage the design supporting hotspots with range 50 to 150 meter. The DCAP configuration will not scale to larger service regions.

If adjacent hotspots overlap to create larger contiguous service regions, coordination by a single CAP is not efficient. To a rough approximation, if VSMR is 150 meters, interference range is about 300 meters. This means vehicles at opposite ends of a hotspot with radius 150 meter could transmit concurrently without interfering with each other. This suggests the path to efficient design lies in controlling service regions that are several hundred meters or more in dimension with multiple CAPs with synchronized polling schedules. Figure 18 illustrates this. These schedules should allow non-interfering vehicles to be polled concurrently to keep ASTT at a reasonable value. The poll and beacon ranges could still be derived using the equations in this paper with a small APSR value as in this paper. Then beacon and poll power would then have the order of magnitude in this paper. We think the protocol to be followed by the vehicle could also be as described in this paper.

If the CAP polling schedules are to be synchronized, CAP clocks would have to be synchronized. Given the magnitudes of 802.11 intervals like PIFS, DIFS, etc., the clocks would need to be synchronized to microsecond precision. This is difficult without using sophisticated technology that would raise cost. For example, synchronization together with centralized computation of all polling schedules for optimal operation could be realized if the CAPs were all put on an optical network like FDDI. Distributed synchronization and polling coordination using the wireless channel itself for such synchronization at vehicular traffic volumes is an unsolved problem to the best of our knowledge.

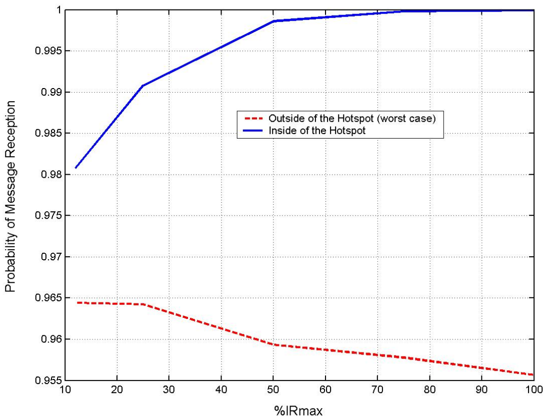


Fig. 16. Different beacon ranges

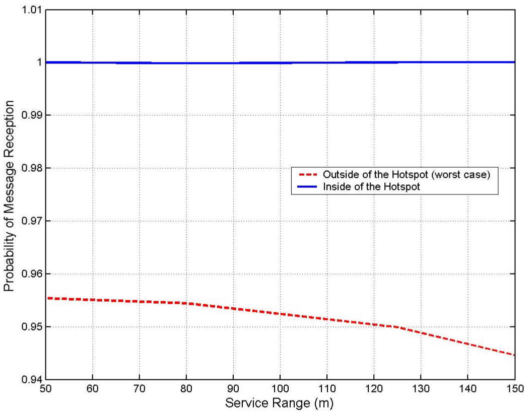


Fig. 17. Different service ranges

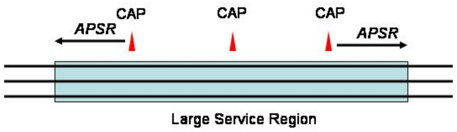


Fig. 18. Controlling a Large Service Region

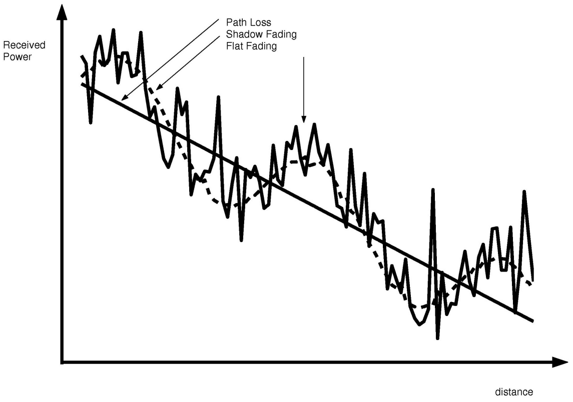


Fig. 19. Received signal versus distance [21]

Environment	γ range
Urban macrocells	3.7-6.5
Urban microcells	2.7-3.5
Office Building (same floor)	1.6-3.5
Office Building (multiple floors)	2-6
Store	1.8-2.2
Factory	1.6-3.3
Home	3

TABLE IV
TYPICAL PATH LOSS EXPONENTS

IX. POWER DETERMINATION

This section presents a method to choose transmission power levels assuming a shadowing model is known. We assume the model is lognormal.

We think of received signal power at different distances from the transmitter as illustrated in figure 19. There is a path loss component determining the drop in average power with distance. The total received power is determined by the path loss component superimposed with a slowly varying shadowing component caused by the environment, e.g., buildings or highway structures, and a much faster small-scale fading component. We model the shadowing component by a lognormal random process and show how to use the model to pick transmission power. We do not do the same for flat or small-scale fading because it fluctuates much more rapidly in space, i.e., on the order of half a wavelength, thereby averaging out to zero for our purposes [19].

The CAP needs to divide its surrounding region into service, poll, and beacon reception regions by transmitting its service, poll, and beacon messages with different levels of power. These are AP to vehicle communications where the AP antenna is assumed to be placed higher than the vehicles. We show how to choose the power of these messages assuming a lognormal shadowing model. We do not address vehicle to vehicle communication since we are not sure of the right form of the shadowing model. Antenna designs remain unsettled for vehicle-vehicle communication.

Our path loss model is

$$P_r(d) = P_t K \left[\frac{d_o}{d}\right]^\gamma \tag{14}$$

implying that transmit and receive power in dBm are related by

$$P_t = P_r(d) - 10\log_{10} K + 10\gamma \log_{10}\left[\frac{d_o}{R}\right] \tag{15}$$

Here P_t is the transmit power, $P_r(d)$ the received power at distance d from the transmitter, K is the dimensionless constant used in equation 7 determined by antenna characteristics and average channel attenuation, d_o is a reference distance for the antenna far-field, and γ is the path loss exponent [21]. The value of γ depends on the propagation environment. Table IV summarizes typical path loss exponents [22], [23].

We model shadowing by a Gaussian random variable ψ with 0 dB mean and variance σ_ψ^2. Typically $\sigma_\psi^2 = 3.65dB$ for a lognormal shadowing model. Hence our ratio of received to transmitted power in dB is given by:

$$\frac{P_r(d)}{P_t}(dB) = 10\log_{10} K - 10\gamma \log_{10}\frac{d_o}{d} - \psi. \tag{16}$$

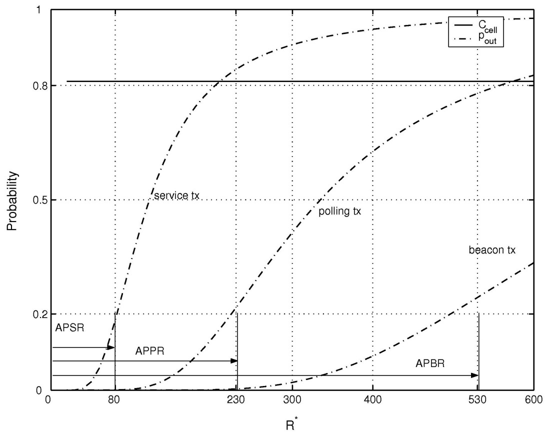


Fig. 20. Cell coverage and outage probability with shadowing, $P_{min} = -120dBm$, $\gamma = mR + n$

We define the outage probability at a given distance d as

$$\begin{aligned} p_{out}(d) &= Prob(P_r(d) < P_{min}) \\ &= 1 - Q\left(\tfrac{P_{min} - (P_t + 10\log_{10} K - 10\gamma \log_{10}(d/d_o))}{\sigma_\psi}\right) \end{aligned} \tag{17}$$

where P_{min} is the minimum received power required for message reception. The Q function is the complementary error function below:

$$Q(z) = \frac{1}{2} erfc\left(\frac{z}{\sqrt{2}}\right). \tag{18}$$

Based on $p_{out}(d)$ we define a cell outage probability $P_{out}(R)$ for a cell of radius R around the transmitter as

$$P_{out}(R) = \frac{2}{R^2} \int_0^R p_{out}(r) r dr. \tag{19}$$

When the aim is to reach all vehicles within some distance R^* around the Coordinating AP, the transmit power is chosen so that $P_{out}(R)$ will be small when $R < R^*$ and rise rapidly when $R > R^*$.

Within the cell of radius R^* the received power should be above the message reception threshold throughout the area. This is captured by defining a cell coverage measure $C(R^*)$ defined as

$$C(R^*) = E\left[\frac{1}{\pi R^{*2}} \int_{cell\_area} 1[P_r(r,\theta) > P_{min}] r dr d\theta\right]. \tag{20}$$

Combining these equations yields the following closed-form solution for C;

$$C = Q(a) + \exp\left(\frac{2 - 2ab}{b^2}\right) Q\left(\frac{2 - ab}{b}\right) \tag{21}$$

where

$$\begin{aligned} a &= \tfrac{P_{min} - P_t - 10\log_{10} K + 10\gamma \log_{10}(R/d_o))}{\sigma_\psi} \\ b &= \tfrac{10\gamma \log_{10} e}{\sigma_\psi} \end{aligned} \tag{22}$$

The aim is to choose the transmit power so that cell coverage will be sufficiently high. γ is assumed to be between 2 and 6 and incremented linearly with the distance.

The DCAP design has three regions, i.e., beacon region, polling region, and service region. We choose the transmit power for each message using equation 21 so that C is almost the same in all the regions. The figures are computed for $C = 0.8$. Thus the method is to target an outage probability and then derive the corresponding power levels. One can see that a service packet has high outage probability in the polling and beacon regions. It has low outage probability in the service region. This is desirable. Likewise the polling packet has a high outage probability in the beacon region.

X. Conclusion

We have explored the problem of creating a wireless protocol and architecture for a vehicle-to-vehicle and vehicle-to-infrastructure communication system. The goal is ensuring that low-latency safety messages are delivered with high probability and low latency (e.g. 100 msec.). At the same time, the system should maximize the fraction of time available for vehicles to perform transactions with roadside access points on a separate service channel. Challenges imposed by DSRC include operating within a multi-channel environment with an 802.11 radio (vehicles tuned to commercial service channels cannot simultaneously receive safety messages in the control channel) and the highly dynamic network topology characterized by communication nodes moving with vehicular properties.

The solution proposed here extends the 802.11 base protocol currently specified for DSRC. It assumes that DSRC non-safety services will involve APs and requires at least one in each hotspot to regulate the timing of channel transitions for vehicles entering the service area. We refer to this AP as a coordinating access point (CAP). In areas without services we enable the exchange safety messages amongst vehicles with an ad-hoc protocol such as 802.11 DCF or any other able to obey the CAP in the vicinity of a hotspot.

Service-seeking vehicles and those proximate to them conduct a full safety exchange during a collision free period, where all safety message broadcasts are scheduled by the access point. At the completion of the collision free period, vehicles within the service area may switch to service channels to perform desired transactions. Vehicles outside of the service area will complete their safety exchange and are otherwise free to transmit non-scheduled data. Vehicles out of range of a CAP, i.e., outside its beacon range operate in ad-hoc mode, as do vehicles within beacon range during contention periods. Thus the solution builds on 802.11 PCF within range of a CAP and combines it with 802.11 DCF out of CAP range to comprehensively support safety message exchange throughout a highway.

Evaluations are conducted using NS-2. Trajectories of moving vehicles are produced by SHIFT and represent a four lane highway at maximum flow. We evaluate supporting safety and non-safety communication using DCF, PCF in the service hotspot only, i.e., without our spatial division, and the DCAP configuration. In the DCF evaluation the vehicles leave the safety message channel randomly and asynchronously since there is no signal available to synchronize their departure. Since the targeted recipients of a message are often away when the message is transmitted, safety message reception is poor. PCF restricted to the service hotspot also does poorly within about 300 meters of the AP for the same reasons. Many of the intended recipients of safety messages are away on the service channel when the message is sent.

The DCAP design delivers more consistent performance as a function of distance from the CAP. We view the performance of the ad-hoc protocol where there are no service hotspots as a desirable performance requirement. DCAP performance is significantly better within the hotspot but about 2% worse between 300 and 600 meters away from the CAP. We know how to reduce the 2% tax by making safety message reception inside the hotspot a bit worse but cannot eliminate it.

Evaluations are conducted using a collision model. Thus all power considerations are transformed into transmission ranges and corresponding interference ranges. This transformation can provide for shadow and small-scale fade margins. We use a collision model because most of the communication in the simulator is vehicle-vehicle and we do not know of established fading or shadowing values for such communication. All message losses occur due to collisions. In practice there will be some additional loss due to shadowing and small-scale fading. The amount of additional loss will depend on the margins assumed when determining the transmission power of different messages. If the shadow or fade margins have to be larger than assumed in this paper, the transmission power corresponding to VSMR will have to rise, but IR_{max} will rise still more deteriorating the performance of the DCAP, PCF in hotspot, and DCF only configurations, i.e., the new design and the baselines used for comparison will all deteriorate.

Thus the principal finding of this paper is the relative performance of the DCAP, PCF in hotspot, and DCF only configurations. Relative to the other two, the DCAP design is able to offer consistent QoS to safety messages as vehicles travel into the hotspot, use the service channels, and travel out. QoS refers to the probability a safety message transmitted by a randomly chosen vehicle within distance VSMR, and the delay between consecutive opportunities given to a vehicle to transmit its safety messages.

XI. Acknowledgments

This research was supported in part by Toyota Technical Center, USA, Inc., fund No. 94138 and Caltrans RTA65A0177-15650.

References

[1] T. K. Mak, K. P. Laberteaux and R. Sengupta., A Multi-Channel VANET Providing Concurrent Safety and Commercial Services, In Proceedings of the 2nd ACM Workshop on Vehicular Ad-hoc Networks, Koln, Germany, September 2005.

[2] M. Ergen, D. Lee, R. Sengupta, and P. Varaiya, Wireless Token Ring Protocol, IEEE transactions on Vehicular Technology, vol.53, no.6, Nov. 2004, pp.1863-81.

[3] USFCC, Report and Order, FCC 03-324, Dec. 2003.

[4] J. Paniati (Dir., ITS, U.S Dept. of Transp.), Intelligent Safety Efforts in America, 10th ITS World Conf. http://www.its.dot.gov/speeches/madridvii2003.ppt, Nov. 17, 2003.

[5] Vehicle safety communications project: Final report. submitted to NHTSA and FHWA in response to cooperative agreement number DTFH61-01-X-001. January 2005.

[6] S. E. Shladover, Effects of Traffic Density on Communication Requirements for Cooperative Intersection Collision Avoidance Systems (CICAS), PATH Working paper PWP-2205-1, California PATH, University of California, Berkeley.

[7] R. Sengupta, S. Rezaei, S. E. Shladover, D. Cody, S. Dickey and H. Krishnan, Cooperative collision warning systems: Concept definition and experimental implementation, In review Journal of Intelligent Transportation Systems.

[8] Q. Xu, J. Ko, T.K. Mak, and R. Sengupta, Vehicle-to-Vehicle Messaging in DSRC, First ACM Workshop on Vehicular Ad Hoc Networks(VANET), 2004.

[9] G. Korkmaz, E. Ekici, F. Ozguner, U. Ozguner, Urban Multi-hop Broadcast Protocol for Inter-vehicle Communication System. Proceedings of the 1st ACM Workshop on Vehicular Ad Hoc Network (VANET), pages 76–85, 2004

[10] S. Mangold, S. Choi, G. Hiertz, O. Klein, B. Walke, Analysis of IEEE 802.11e for QoS Support in wireless LANs, IEEE Wireless Communications, pages 40–50, 2003

[11] IEEE 802.11 Working Group, Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications, August 1999.

[12] W.C. Hung, K.L. Law and A. Leon-Garcia, A Dynamic Multi-Channel MAC for Ad Hoc LAN, In Proc. 21stt Biennial Symposium on Communications, pages 31-35, Canada, June 2002

[13] S.L. Wu, C.Y. Lin, Y.C. Tseng, and J.P.Sheu, A New Multi-Channel MAC Protocol with On-Demand Channel Assignment for Multi-Hop Mobile Ad Hoc Network, Int'l Symposium on Parallel Architectures Algorithms and Networks (I-SPAN) , 2000, pp. 232-237.

[14] A. Nasipuri, J. Mondehe, Multi-channel MAC with Dynamic Channel Selection for Ad Hoc Networks, Technical Report, January, 2004.

[15] N. Jain, S. Das, A. Nasipuri, A Multichannel MAC Protocol with Receiver-Based Channel Selection for Multihop Wireless Networks, In Proceedings of the IEEE International Conference on Computer Communication and Networks (ICCCN2001), Phoenix, AZ, October 2001

[16] A. Tzamaloukas and J.J. Garcia-Luna-Aceves, Channel Hopping Multiple Access with Packet Trains for Ad-Hoc Networks, In Proc. of the IEEE IC3N'98, Seventh International Conference on Computer Communications and Networks, 1998

[17] P. Bahl, R. Chandra, J. Dunagan, SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks, Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, September 2004

[18] J. So, N. Vaidya, Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using A Single Transceiver, Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, May 2004

[19] G. S. Prabhu, P. M. Shankar, *Simulation of Flat Fading Using MATLAB For Classroom Instruction.* IEEE Trans. on Education, Vol. 45, No. 2, February 2002, pp. 19-25.

[20] F. Herzel, G. Fischer, H. Gustat, An Integrated CMOS RF Synthesizer for 802.11a Wireless LAN, IEEE Journal of Solid-state Circuits, 18(10), October 2003

[21] A. Goldsmith, *Wireless Communications.* Campridge University Press, October, 2005.

[22] A. Bahai, B. Saltzberg, M. Ergen, *Multi Carrier Digital Communications: Theory and Applications of OFDM.* Springer, Inc, October, 2004.

[23] V. Erceg, L. J. Greenstein, S. Y. Tjandra, S. R. Parkoff, A. Gupta, B. Kulic, A. A. Julius, and R. Bianchi, *An empirically based path loss model for wireless channels in suburban environments. IEEE Journal on Selected Areas in Communications,* pp. 1205-1211, July 1999.

[24] Network Simulator (ns-2), http://www.isi.edu/nsnam/ns/.

[25] A. Lindgren and A. Almquist. IEEE 802.11 PCF Mode. http://www.sm.luth.se/ dugdale/index/software.shtml

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

[27] Q. Xu, T. Mak, J. Ko , R. Sengupta, Vehicle-Vehicle Safety Messaging in DSRC, In Proc. of the 1st ACM Workshop on Vehicular Ad-hoc Networks, October 2004, Philadelphia, USA.

[28] Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle System - 5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ASTM E2213-03, Sep. 2003

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

[30] Q. Xu, Control, Estimation, and Communication Design Applied to Active Vehicle Safety Systems, PhD. Thesis, Fall 2005, University of California, Berkeley.

APPENDIX I: PROOFS OF THEOREMS

This appendix states the proofs of the theorems in section VI. The following notation is used in this section.

Definitions::

1) S: The set of all vehicles in the system
2) $\bar{A}$: is the complement of the set A.
3) t_i: Starting time of the $i-$th cycle.
4) T: Duration of each cycle.
5) ν_{max}: Maximum speed in meter/sec. that a vehicle can move
6) *Contention-Free Period* (CFP): interval where nodes uniquely transmit according to a schedule.
7) CFP_i: The CFP interval $[t_i, t_i + \delta_i)$ in i^{th} the cycle.
8) δ_{max}: Maximum duration for each CFP. Note $\delta_{max} < T$.
9) δ_i: Duration of the CFP in the i^{th} cycle. Note $\delta_i < \delta_{max}$.
10) τ: The duration of each time slot in $[t_i, t_i + \delta_i)$.
11) *Contention Period* (CP): Interval during which nodes transmit using a contention based MAC protocol.
12) CP_i: Duration of the contention period $[t_i + \delta_i, t_{i+1})$ in the cycle.
13) *Vehicle Safety Message Range* (VSMR): Maximum range at which a safety message should be received without multiple access interference
14) IR_{max}: The maximum distance between a receiver and an interferer. Transmitters at distance greater than from a receiver cannot interfere with its receptions.
15) *Access Point Service Range*(APSR): The maximum range at which the Access Point (AP) offers services.
16) *Access Point Safety Exchange Range* (APSER): The range within which the AP polls each vehicle for safety transmission. $APSER = APSR + VSMR$
17) *Access Point Poll Range* (APPR): The range within which the AP polls each vehicle for safety transmission. $APPR = APSER + \nu_{max} \times T$.

18) *Access Point Quiet Range* (APQR): The range at which the AP requires vehicles to be silent unless polled during the CFP. $APQR = APSER + IR_{max}$.
19) *Access Point Beacon Range* (APBR): The maximum range to which the AP transmits beacons. $\{APBR = APQR + \nu_{max} \times T\}$.
20) $B_i(n)$: Number of beacons received by node n in $[t_i, t_{i+1})$.
21) $B_{CFP_i}(n)$: Number of beacons received by node n in CFP_i.
22) $D(n, r)$: The set of nodes within a circle centered at node n and with radius of r.
23) $D_i(n, r)$: The set of nodes within a circle centered at node n, with radius r during the time interval $[t_i, t_{i+1})$.
24) $\Re(n, r)$: A circular region centered at node n and with radius of r.
25) $Msg_i(n)$: Message indicator function of node n in CFP_i, if node n transmits its data, $Msg_i(n)$ = 1, if node n does not transmit its data, $Msg_i(n) = 0$.
26) $R_i(n, m)$: Reception indicator function for a message from node n to node m in $[t_i, t_i + \delta_i)$, 0 if node m did not receive the message from node n, 1 if node m received the message from node n.
27) SA_i: Allocator function (one to one) that maps node n to a non-overlapping time slot in $[t_i, t_i + \delta_i)$. $SA_i : n \in A_i \mapsto k \in \{t_i, t_i + 1 \times \tau, ..., t_i + (|A_i| - 1) \times \tau\}$ where A_i = $D_i(AP, APPR)$. $|A_i|$ is the cardinality of set A_i.
28) $STATE(n, [t_1, t_2))$: The system state of node n in $[t_1, t_2) \in$ {Ad-Hoc, AP Coordinated, Service}
29) $FSE_i(n, r)$: Full safety exchange indicator function for a node n and range r in CFP_i. It is 1 if node n experiences an FSE with all vehicles in $D_i(n, r)$ in the period CFP_i, and is 0 otherwise. For all the receivers within range r of node n, interferers of node n and its receivers should be in the AP Coordinated state while they are exchanging their safety messages. Moreover, if node n has data to send, all its receivers should receive, and if its receivers have data to send, node n should receive. If the above conditions are not met, FSE will be zero. More precisely,

$$\begin{array}{l} FSE_i(n,r) = 1 \Leftrightarrow \\ \forall m \in D_i(n,r).\forall_j \in D_i(n, IR_{max}) \cup D_i(m, IR_{max}). \\ STATE(j, [t_i, t_i + \delta_i)) = APCoordinated \wedge Msg_i(n) \neq 0 \Rightarrow R_i(n,m) = 1 \\ \wedge Msg_i(m) \neq 0 \Rightarrow R_i(m,n) = 1. \\ FSE_i(n,r) = 0, otherwise. \end{array} \tag{23}$$

30) *Node*: A vehicle with one radio, which can operate across multiple channels, traveling up to ν_{max}. It transmits its safety messages on the control channel with enough power to cover the VSMR, and interferes receptions at ranges no greater than IR_{max}. Node is also referred as vehicle in this proof.
31) *AP*: An access point coordinating medium access by all nodes within the $\Re(AP, APQR)$ during the CFP or providing service to vehicles within the $\Re(AP, APSR)$ during the CP.

Assumptions: The idealizations made to establish the theorems are as stated in section VI. We re-state them for convenience.

1) The proof uses a collision model. Each transmission has a specified range and each node has a location. A transmission is received if the distance between transmitter and receiver is less than the specified range and there is no collision. A collision occurs if one or more nodes within interference range (IR_{max}) of the receiver transmit concurrently.
2) Maximum interference range for nodes other than the AP is IR_{max}.
3) Each node other than the AP has only one radio, and the radio can only receive data on one channel at a time.
4) If x is a poll range, then a node n is polled in CFP_i iff node n is in $D_i(AP, x)$.
5) Each node executes the state machines in section V. In particular, the proofs focus on the one state machine in figure 21. This is figure 7(b) of section V stated differently to make the proofs more accessible. The vehicle protocol controller in figure 7(b) transitions between the same modes as in figure 21 but is driven by timers in practice.
6) Nodes move in discrete steps, and they change position at the t_i's. The maximum distance a node can move in a time step is $\nu_{max} \times T$.
7) The number of vehicles in a given area is proportional to the size of the area.
8) The AP transmits beacons periodically in $[t_i, t_{i+1})$. There is at least one beacon transmitted in $[t_i, t_i + \delta_i)$.

Proofs: We first prove three lemmas and then use them to prove the five theorems stated in section VI.

Lemma 1: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then all nodes in $D_i(AP, APQR)$ will be in AP Coordinated state in CFP_i. More precisely,

$$\begin{array}{l} (\forall j \in D_{i-1}(AP, APBR), B_{i-1}(j) \geq 1) \Rightarrow \\ (\forall k \in D_i(AP, APQR), \\ STATE(k, [t_i, t_i + \delta_i)) = AP\ Coordinated) \end{array} \tag{24}$$

Proof: By Assumption 6 and Definition 19, $D_i(AP, APQR) \subseteq D_{i-1}(AP, APBR)$. Thus, by hypothesis, $B_{i-1}(j) \geq 1$ for all node j in $D_{i-1}(AP, APBR)$. The result follows from Assumption 5.

The different nodes referred to in the statement and proof of the following lemma are illustrated in figure 22.

Lemma 2: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then for all nodes l in $D_i(AP, APSER)$, any safety messages transmitted by node l will be received by all vehicles located in $D_i(l, VSMR) \cap D_i(AP, APSER)$. More

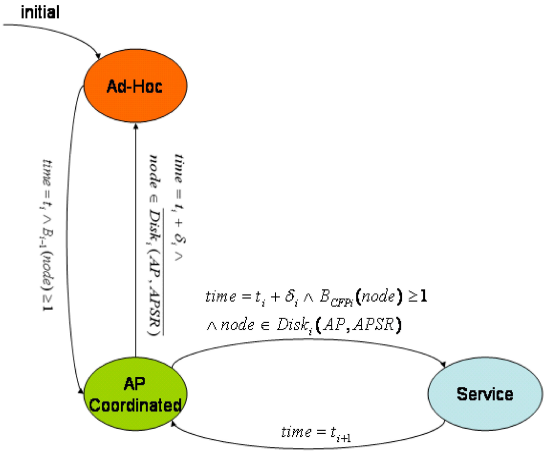

initial
Ad-Hoc
AP Coordinated
Service
$time = t_i \wedge B_{i-1}(node) \geq 1$
$time = t_i + \delta_i \wedge$
$node \in \overline{Disk_i(AP, APSR)}$
$time = t_i + \delta_i \wedge B_{CFPi}(node) \geq 1$
$\wedge\, node \in Disk_i(AP, APSR)$
$time = t_{i+1}$

Fig. 21. Vehicle Protocol Controller as assumed in the proofs

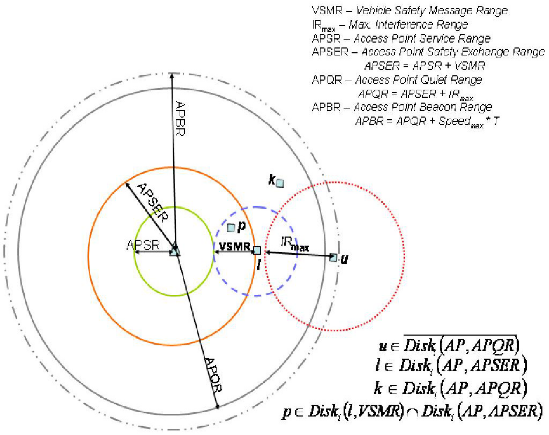

VSMR – Vehicle Safety Message Range
IR_{max} – Max. Interference Range
APSR – Access Point Service Range
APSER – Access Point Safety Exchange Range
APSER = APSR + VSMR
APQR – Access Point Quiet Range
APQR = APSER + IR_{max}
APBR – Access Point Beacon Range
APBR = APQR + $Speed_{max}$ * T
APBR
APSER
APSR
VSMR
IR_{max}
APQR
k
p
l
u
$u \in \overline{Disk_i(AP, APQR)}$
$l \in Disk_i(AP, APSER)$
$k \in Disk_i(AP, APQR)$
$p \in Disk_i(l, VSMR) \cap Disk_i(AP, APSER)$

Fig. 22. Illustration for Lemma 2

precisely,

$$\begin{aligned} &\forall i, (\forall j \in D_{i-1}(AP, APBR), B_{i-1}(j) \geq 1) \\ &\Rightarrow (\forall l \in D_i(AP, APSER), \\ &\forall p \in D_i(l, VSMR) \cap D_i(AP, APSER), \\ &Msg_i(l) \neq 0 \Leftrightarrow R_i(l, p) = 1) \end{aligned} \tag{25}$$

Proof: Pick any CFP i. By Assumption 2, any node v only interferes with receptions in $D_i(v, IR_{max})$. Thus, a node $u \in \overline{D(AP, APQR)}$ cannot interfere with any receptions at any node $l \in D(AP, APSER)$, since $APQR = APSER + IR_{max}$. In addition, from Lemma 1, any node $k \in D_i(AP, APQR)$ is in AP Coordinated state during CFP_i, so it will be silent unless polled. Thus, a node k creates no interference to any node l in CFP_i. Since $\overline{D_i(AP, APQR)} \cap D_i(AP, APQR) = S$, receptions at node l are free of interference from any nodes in CFP_i. By Assumption 1, receivers receive only if they are within communication range of the sender. Let l, p be as in the hypothesis. Node l is within the $\Re(AP, APSER)$, node p is within the $\Re(l, VSMR)$, and there are no interferers. Thus,$Msg_i(l) \neq 0 \Leftrightarrow R_i(l, p) = 1$.

Lemma 3: $D_i(AP, APSER)$ contains every node in $D_i(AP, APSR)$ and all its receivers. More precisely, $(D_i(AP, APSR) \subset D_i(AP, APSER)) \wedge \forall n \in D_i(AP, APSR)$, $D_i(n, VSMR) \subset D_i(AP, APSER)$.

Proof: By definition 16, $APSER = APSR + VSMR$. Thus, the result follows.

Theorem 1: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then every node in $D_i(AP, APSR)$ will complete its full safety exchange (FSE) in CFP_i. More precisely,

$\forall j \in D_{i-1}(AP, APBR), B_{i-1}(j) \geq 1) \Rightarrow (\forall n \in D_i(AP, APSR), FSE_i(n, VSMR) = 1)$

Proof: By Lemma 3, for all $n \in D_i(AP, APSR)$, node n and all its receivers are contained in $D_i(AP, APSER)$. By Lemma 2, if $Msg_i(n) \neq 0$ for node n in CFP_i, then for any $m \in D_i(n, VSMR)$, $R_i(n, m) = 1$. Similarly, if $Msg_i(m) \neq 0$ for node m in CFP_i, then $R_i(m, n) = 1$. By Definition 18 and 16, for all interferers $k \in D_i(n, IR_{max}) \cup D_i(, IR_{max})$, k are contained in $D_i(AP, APQR)$ since $APQR = APSER + IRmax$ and $APSER = APSR + VSMR$. By Lemma 1, every node in $D_i(AP, APQR)$ is in AP Coordinated state in CFP_i. Thus, node n and m will be able to receive each other's message and messages from the AP free of interference. By assumption 4, n and m will be polled once in CFP_i. The theorem follows from the definition of $FSE_i(*, *)$.

Theorem 2: Let *poll_range* be a poll range other than $APSER$. If poll range has the property that for any i and node $n \in D_i(AP, APSR), FSE_i(n, VSMR) = 1$, under the assumption of Theorem 1, then *poll_range* $\geq APSER$. If $\delta_i \propto |D_i(AP, poll\_range)|$, then when *poll_range* $= APSER$, δ_i is minimized.

Proof: Suppose *poll_range* $< APSER$. By Assumption 4, and since $APSER = APSR + VSMR$, there exists a node $n \in D_i(AP, APSR)$ and $m \in D_i(n, VSMR)$ such that node m is not polled in CFP_i. Thus $FSE_i(n, VSMR) \neq 1$, proving the first part. By Assumption 7, $|D_i(AP, poll\_range)| \geq |D_i(AP, APSER)|$. Thus if $\delta_i \propto |D_i(AP, poll\_range|$, when *poll_range* $= APSER$, δ_i is minimized.

Theorem 3: Let *beacon_range* be a beacon range other than $APBR$. If beacon range has the property that for any $n \in D_i(AP, APSR)$, $FSE_i(n, VSMR) = 1$ under the assumption of Theorem 1, then *beacon_range* $\geq APBR$. When *beacon_range* $= APBR$, number of silent nodes, i.e. $\overline{D_i(AP, APSER)} \cap D_i(AP, APBR)$, in CFP_i is minimized.

Note: $\overline{D_i(AP, APSER)} \cap D_i(AP, APBR)$ is defined to be the silent nodes in CFP_i because they are the set of nodes which will not be polled by the AP in CFP_i. They are required to be silent for the benefit of all nodes in $D_i(AP, APSR)$ to complete their *full safety exchange* (FSE). Minimizing the set of silent nodes maximizes the control channel reusability outside of the AP's coordinating area.

Proof: Suppose *beacon_range* $< APBR$. Since $APBR = APSR + VSMR + IR_{max} + \nu_{max} \times T$, there exists a node $n \in D_i(AP, APSR)$, $m \in D_i(n, VSMR)$, and $k \in D_i(m, IR_{max})$ such that $B_{i-1}(k) = 0$, so the state of node k in is not in AP Coordinated state. Thus $FSE_i(n, VSMR) \neq 1$, which contradict the hypothesis. Note that a *beacon_range* $= APSR + VSMR + IR_{max}$ is not enough since even if all vehicles in this distance receive a beacon in $(i-1)^{th}$ cycle, there could be new vehicles who haven't received a beacon entering the $\Re(AP, APQR)$ in CFP_i. Since $APBR$ is the minimum beacon range, by Assumption 7, $|\overline{D_i(AP, APSER)} \cup D_i(AP, APBR)|$ is minimized.

Theorem 4: If every node in $D(AP, APBR)$ receives a beacon in both $(i-1)^{th}$ and i^{th} cycles, then for every node l in $D(AP, APSER)$, the time between consecutive polls is bounded by $T \pm \delta_{max}$. More precisely,

$$\begin{aligned}
&(\forall j \in D_{i-2}(AP, APBR), \forall k \in D_{i-1}(AP, APBR),\\
&B_{i-2}(j) \geq 1 \wedge B_{i-1}(k) \geq 1)\\
&\Rightarrow (\forall l \in \{D_{i-1}(AP, APSER) \cap D_i(AP, APSER)\},\\
&T - \delta_{max} \leq SA_i(l) - SA_{i-1}(l) \leq T + \delta_{max})
\end{aligned} \tag{26}$$

Proof: By Assumption 4, AP will individually poll every node in $\Re(AP.APSER)$. Considering any schedule used by the nodes in CFP_i. For a node $l \in D_{i-1}(AP, APSER) \cap D_i(AP, APSER)$, the longest and the shortest wait time between two consecutive polled are the followings: If $SA_{i-1}(l) = t_{i-1}$ and $SA_i(l) = t_i + (|D_i(AP, APSER)| - 1) \times \tau$, then $SA_i(l) - SA_{i-1}(l) = T + \delta_i - \tau \leq T + \delta_{max}$ (e.g. longest wait time). If $SA_{i-1}(l) = t_{i-1} + (|D_{i-1}(AP, APSER)| - 1) \times \tau$ and $SA_i(l) = t_i$, $SA_i(l) - SA_{i-1}(l) = T - \delta_{i-1} + \tau \geq T - \delta_{max}$ (e.g. shortest wait time). Therefore, $T - \delta_{max} \leq SA_i(l) - SA_{i-1}(l) \leq T + \delta_{max}$, for all $l \in D_{i-1}(AP, APSER) \cap D_i(AP, APSER)$.

Theorem 5: If all nodes in $D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then the protocol is safe and efficient for all node n in $D_i(AP, APSR)$ in the following sense:

1) $STATE(n, [t_i + \delta_i, t_{i+1})) = SERVICE$
2) $FSE_i(n, VSMR) = 1$
3) The service time, e.g. $T - \delta_i$, is maximized.

Proof: To show a node $n \in D_i(AP, APSR)$ will change to the Service state in CP_i, we need to satisfy the guard conditions in figure 21. By Lemma 1, if all node $j \in D_{i-1}(AP, APBR)$ receive a beacon in period $[t_{i-1}, t_i)$, then all interferers of any node n in $D(AP, APSR)$ are in the AP Coordinated state in CFP_i. By Assumption 8, the AP will transmit a beacon in CFP_i and node n will receive it. This proves node n will transition to the Service state in CP_i. By Theorem 1, $FSE_i(n, VSMR) = 1$. By Theorem 2, δ_i is minimized. Thus, service time, $T - \delta_i$, is maximized.