Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Performance of beacon safety message dissemination in Vehicular Ad hoc NETworks (VANETs)[*]

YOUSEFI Saleh[‡1], FATHY Mahmood[1], BENSLIMANE Abderrahim[2]
(*[1]Computer Engineering Faculty, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Tehran, Iran*)
(*[2]Laboratoire d'Informatique d'Avignon LIA, 339 chemin des Meinajaries, BP 1228-84911, Avignon cedex 9, France*)
E-mail: syousefi@iust.ac.ir; mahfathy@iust.ac.ir; abderrahim.benslimane@univ-avignon.fr

Received July 5, 2007; revision accepted Oct. 1, 2007

Abstract: Currently, there is a growing belief that putting an IEEE 802.11-like radio into road vehicles can help the drivers to travel more safely. Message dissemination protocols are primordial for safety vehicular applications. There are two types of safety messages which may be exchanged between vehicles: alarm and beacon. In this paper we investigate the feasibility of deploying safety applications based on beacon message dissemination through extensive simulation study and pay special attention to the safety requirements. Vehicles are supposed to issue these messages periodically to announce to other vehicles their current situation and use received messages for preventing possible unsafe situations. We evaluate the performance of a single-hop dissemination protocol while taking into account the quality of service (QoS) metrics like delivery rate and delay. We realize that reliability is the main concern in beacon message dissemination. Thus, a new metric named effective range is defined which gives us more accurate facility for evaluating QoS in safety applications specifically. Then, in order to improve the performance, the effects of three parameters including vehicle's transmission range, message transmission's interval time and message payload size are studied. Due to special characteristics of the safety applications, we model the relationship between communication-level QoS and application-level QoS and evaluate them for different classes of safety applications. As a conclusion, the current technology of IEEE 802.11 MAC layer has still some challenges for automatic safety applications but it can provide acceptable QoS to driver assistance safety applications.

Key words: Safety applications, Inter-vehicle communications, Vehicular Ad hoc NETworks (VANETs), Application level QoS, Effective range
doi:10.1631/jzus.2007.A1990 **Document code:** A **CLC number:** TN92

INTRODUCTION

Intelligent transportation systems (ITSs) have been investigated for many years in Europe, Japan and North America, with the aim of providing new technologies able to improve safety and efficiency of road transport. Most of the previous systems are centralized and include either cellular or infrastructure-based roadside/vehicle communications (Morimoto *et al*., 1999; Andrisano *et al*., 2000). Recently, there is public interest to invoke Vehicular Ad hoc NETwork (VANET) as a complementary or/and independent possibility for future ITS. Major research programs have been involved to connect vehicles with each other and with the Internet, for example, PReVENT project (http://www.prevent-ip.org) in Europe, InternetITS (http://www.internetits.org) in Japan, and Network on Wheels (http://www.network-on-wheels.de) in Germany. VANET does not need any infrastructure and connection links between nodes are established when their distance is less than a vehicle's transmission range. VANETs are based on short-range wireless transmission (e.g., IEEE 802.11). The Federal Communications Commission (FCC) has allocated 75 MHz of spectrum in the 5.9 GHz band for Dedicated Short Range Communication (DSRC) to enhance the safety and pro-

---

[‡] Corresponding author

[*] Project partially supported by the Iran Telecommunication Research Center (ITRC)

ductivity of the nation's transportation system (Federal Communications Commission, 2004). DSRC ruling has permitted both safety and non-safety (commercial) applications, provided safety messages are accorded priority. As a part of DSRC standard, IEEE 802.11p (IEEE, 2004) improves IEEE 802.11 to deal with vehicular environment which includes data exchange between high-speed vehicles and between vehicles and the roadside infrastructure.

VANETs tend to be very challenging and a comprehensive survey about communication challenges is provided in (Yousefi *et al*., 2006). Although many decisions in this field have not been taken yet, according to FCC frequency allocation we can categorize two main classes of applications for vehicular ad hoc networks: comfort and safety.

In comfort applications, the goal is to improve passenger comfort and traffic efficiency. Examples for this category are: traffic-information system, route optimization, electronic toll collection, map download, video download, and Internet transactions. These applications are predicted to grow very fast in the near future.

In safety applications, the goal is to improve the safety level of passengers by exchanging safety relevant information between vehicles. The information is either presented to the driver or used by automatic active safety system. Some examples are: cooperative forward collision warning, left/right turn assistant, lane changing warning, stop sign movement assistant and road-condition warning. Due to the stringent delay requirements, applications of this class may demand direct vehicle-to-vehicle communication.

Each safety application demands some message exchanging between vehicles. These massages can be classified in two categories: alarm and beacon, which have different dissemination policies and roles in safety improvement. Alarm messages are issued by vehicles to announce others about the already happened events in a specific point of a road, like car crash, icy surface, etc., whereas, beacon messages are issued periodically. Using the received beacons vehicles try to inhibit possible events (not already occurred) like erroneous lane changing, forward collisions, wrong left/right turning, etc. Furthermore, beacon messages might be used by other applications (e.g. routing protocols). Note that messages mentioned above are complementary to each other. While alarm messages may be able to inform the driver in time about already happened events in order to prevent more incidents, beacon messages can prevent many incidents before they take place. Moreover, since alarm messages announce events, they are more critical and should be disseminated with higher priority.

The dissemination of alarm safety messages as well as comfort messages has been widely investigated in recent literature (Benslimane, 2004; Wischhof *et al*., 2005; Adler *et al*., 2006). However, to the best of our knowledge, there are quite few studies about beacon safety message dissemination and previous works are mostly discussing simplified cases which will be reviewed in the next section.

In this paper, we intend to fill this gap by conducting extensive simulation study to evaluate the performance of disseminating beacon safety messages in a typical crowded traffic situation while using IEEE 802.11 (the base for DSRC standard) as the MAC layer. For this purpose, some metrics determining QoS, like delivery rate and delay have been evaluated. Furthermore, realizing the importance of reliability requirement in safety applications specifically, a new metric named effective range is defined, which gives us more accurate capability to investigate quality of service. In order to improve the performance, we study the effects of three parameters on the mentioned metrics including (1) transmission range (transmitter power level), (2) message transmission interval and (3) packet payload size. We show that there are some optimum (or sub-optimum) set of values which lead to higher performance.

Afterwards we have modeled the relationship between communication-level QoS and the application-level QoS. Communication-level QoS is considered mostly by protocol designers, while application-level QoS is considered directly by users (drivers). We believe that due to special characteristic of safety applications these two types of qualities are not necessarily the same. Understanding this issue certainly influences the feasibility study which we peruse through this paper. Our findings show the possibility for near-term deploying of some safety applications which demand weaker QoS satisfaction, i.e., driver-assistance applications. Nevertheless, for fully automatic applications we should wait for more advances in communication field in the farther future.

The rest of the paper is structured as follows.

Section 2 reviews the relevant literature. Section 3 defines the traffic model and introduces the simulation setup. Section 4 investigates the communication challenges. Section 5 proposes some methods to address those challenges. In Section 6 the relationship between application- and communication-level QoS is modeled and the performance of different classes of safety applications is studied. Finally, Section 7 concludes the paper.

RELATED WORK

According to (Crash Avoidance Metrics Partnership, 2004), many safety applications require beacon messages be sent with transmission ranges from 50 to 300 m. On the other hand, DSRC is based on IEEE 802.11a which currently supports about 300 m range for messages exchange and it is expected that the communication range reaches 1000 m when commercial products are available (IEEE, 2004). Therefore, it could be quite reasonable to consider single-hop dissemination as an important type of future inter-vehicle communications. It should be stressed that when we talk about one-hop communication, we will get involved in the MAC layer broadcasting which is quite different from the network layer forwarding (Beacon messages will need single-hop broadcasting at MAC layer, while alarm safety messages and comfort messages usually demand multi-hop broadcasting/unicasting in network layer).

Broadcasting techniques are broadly investigated in the literature, but most of the works concern multi-hop broadcasting (i.e., flooding) (Williams and Camp, 2002; Lipman *et al*., 2004; Lou and Wu, 2004; Alshaer and Horlait, 2005). To the best of our knowledge, one-hop broadcasting has not been considered so widely.

It is to be noted that there is no RTS/CTS signaling in standard IEEE 802.11-like MAC layer for broadcast mode and so it is more similar to pure CSMA layer channel. However, achieving high reliability for all neighbor nodes (not only one specific destination) in a likely very dense network environment, as we encounter in beacon message dissemination for VANET, are issues which should be treated differently from classical CSMA literature (Wu and Varshney, 1999).

Some researchers tried to investigate the ways to improve reliability when a source broadcasts data for all nodes in its neighborhood. Li *et al*.(2004a; 2004b) proposed first an analytical model able to find a transmission power that maximizes one-hop broadcast coverage in CSMA environment and then an adaptive algorithm that converges to the beforehand fixed transmission power. Their method considers static scenarios (i.e., sensor networks) and all nodes use the same transmission power. However, their adaptive algorithm is not suitable for VANET because of slow convergence. Torrent-Moreno *et al*. (2005) proposed a centralized power control methodology called FPAV to find the optimum transmission range for each node in a dense VANET environment. The final goal is to keep traffic load lower than a predefined threshold, i.e., about half of the nominal channel capacity. They consider static situation but their algorithm is able to set transmission power for each node individually. These works study just the effect of power control on the performance of the one-hop broadcasting and the effects of other factors like transmission interval and packet payload size have not been studied.

Another category of research tackled the problem of reliable broadcasting by considering more deterministic MAC layers, instead of CSMA, in order to avoid collisions. Kabarowski and Zagorski (2005) proposed an algorithm for safety message dissemination in VANETs; the mentioned approach needs the road to be conceptually divided into geographical sectors of relatively small length. This implies that cars must be able to determine the sector they are currently in (e.g. by utilizing GPS). Thus each sector is allowed to transmit only in specific time slots and these time slots are allocated in a way that only sectors in a sufficient distance transmit in parallel. Borgonovo *et al*.(2004) and Mohsin *et al*. (2006) also proposed dynamic TDMA approach (but for general MANETs), which have different slot allocation methodologies. Although these algorithms present good results in simulation study, their capability for real-life implementation is in doubt, mostly because of their need to centralize knowledge of all nodes in the network to allocate slot times properly. That is the main reason that industrial community has based their preferred standard for VANETs on IEEE 802.11-like protocol called DSRC.

Furthermore, some researchers tried to improve the reliability by adopting ACK mechanisms. They argue that since there is no RTS/CTS handshake protocol in the broadcast mode, hidden terminal problem affects delivery rate severely (as it will be shown in this paper too). So, it is needed to adopt another mechanism for increasing reliability of message dissemination. Park and Palasdeokar (2005) proposed issuing negative acknowledge (NAK), whenever a node detects a collision. The sender then reacts to the NAKs by re-broadcasting the message. Moreover, Korkmaz *et al.*(2004) tried to imitate RTS/CTS signaling for broadcast scenarios as they forced some selective receivers to answer to the sender. This signaling has been named RTB/CTB (i.e., Request To Broadcast and Clear To Broadcast) in their work. However, these algorithms are effective just for low-density ad hoc networks with low mobility. In particular, in scenarios like the beacon message dissemination in VANETs, when there are many senders simultaneously, it is likely that the NAKs and CTB themselves become an overhead for the network and make the channel more saturated.

Torrent-Moreno *et al.*(2004) and Xu *et al.* (2004) set up some simulation studies for investigating the characteristics of IEEE 802.11 MAC layer for safety message dissemination in VANETs. The effects of priority on broadcast delivery rate for one-hop broadcast under ideal and probabilistic radio propagation models have been investigated in (Torrent-Moreno *et al.*, 2004). However, in beacon message dissemination it may not be possible to define priority because these messages are not indicating any events and all have similar criticality. However, their approach might be used to give higher priority to alarm messages when they are disseminated. Furthermore, Xu *et al.*(2004) considered a medium density scenario and extends the MAC layer to improve the reliability by re-broadcasting each message several times. Since the predicted transmission range for DSRC is 1000 m, for many traffic situations, it sounds reasonable to expect high densities in the node's transmission range. So this kind of algorithms in IEEE 802.11 MAC layers is not practical in real-life situations. However, similar to (Torrent-Moreno *et al.*, 2004), they studied just MAC layer effects and did not study the effects of power level, transmission range and packet size on the performance of their protocols.

Our work is different two-fold from the above-mentioned studies. Firstly, in order to improve the reliability of message dissemination, we investigate the effects of three parameters including: (1) transmission range, (2) message transmission interval, and (3) message payload size. Secondly, due to special characteristics of safety applications, we have isolated communication-level reliability from application-level reliability and modeled the relationship between them. Then we have deduced the near-term feasibility for deploying of some classes of safety applications (i.e., driver-assistance applications).

TRAFFIC MODEL AND SIMULATION SETUP

In this paper, we address the challenges in dissemination of beacon safety messages between vehicles in IEEE 802.11 MAC layer, which is the base for upcoming DSRC standard. So, moving vehicles in a highway exchange some information about themselves periodically. This information is used by the drivers and/or active safety systems of the cars for preventing unsafe situations. In order to clarify our simulation scenario, we invoke some vehicle's traffic theory. From (Roess *et al.*, 2004) we know that there are three macroscopic parameters: speed (km/h), density (vehicle/km/lane) and flow (vehicle/h/lane) of which their average values are related as follows:

$$V = S \cdot D, \tag{1}$$

where V is traffic flow, S is mean speed and D is density.

During the time, the vehicle's traffic in a highway can be seen in three different phases, as shown in Fig.1. First when the density is low, vehicles drive as fast as they want. This status holds until the density reaches to a value called critical density. This phase is called free-flow traffic and is shown by solid line. Afterwards, some vehicles have to control their speeds in order to keep safe distances from others. This phase is called forced-flow and is shown with dashed line. If the density increases more, the traffic would arrive in jam state and in the worst case vehicles have to stop completely. Clearly, there is a coexistent phase in which both beforehand mentioned effects can be seen. In traffic theory each phase is dealt with in a different manner.

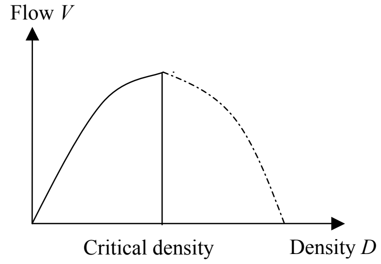


Fig.1 Relationship between flow and density in vehicle's traffic theory

In communication point of view, the free-flow phase is more challenging in the case of connectivity and multi-hop path establishment (Artimy *et al.*, 2004), while due to high vehicle density forced flow phase is of more interest for shared medium access methods and collision avoidance techniques. In the latter case the dense network of vehicles is the main cause of performance impairment. Our considered scenario (Fig.2) is a typical forced-flow traffic situation where vehicles have low relative speed. Because of the large transmission range of vehicles and also the short transmission time of safety messages, the low relative velocity does not change the density of vehicles noticeably. Therefore, we assume constant velocity for vehicles during our simulation. It is to be stressed that this constant velocity assumption does not imply that the vehicles do not have safety problems. On the contrary, they are moving and as a result they need information from neighbor vehicles when they want to use lane changing assistant, cooperative forward collision warning, etc.

As shown in Fig.2, we simulate a platoon of vehicles consisting of 600 vehicles moving in a highway with 8 parallel lanes each lane 5 m wide. Vehicles in each lane are moving with constant speed (100, 120 km/h) separated by an average distance of 20 m which is equivalent to density 50 (vehicle/km/lane). Hence, there are 75 cars in each lane numbered from left to right (e.g., cars from number 1 to 75 in the first lane, 76 to 150 in the second lane, and so on). Such a high level of density in a vehicle's transmission range may take place even with less crowded highway, but with higher transmission ranges (e.g., 1000 m in DSRC). Note that our simulation scenario is static in microscopic point of view as we do not consider the interactions between individual vehicles.

We conduct extensive simulations using GloMoSim library-2.03 (GloMoSim Network Simulator, http://pcl.cs.ucla.edu/projects/glomosim/) while we make use of a deterministic radio propagation model, the two-ray-ground. A typical one-hop broadcast algorithm was implemented and the functionality of the algorithm was examined. Each node sends UDP packets of size 100 or 200 bytes every 100 or 200 ms with a time jitter of 10%. Vehicles use transmission ranges of 50 to 300 m for message exchange. Table 1 shows the simulation setup parameters.

Table 1 Simulation setting parameters

Parameter	Value
Propagation model	Two-ray-ground
Transmission range (m)	50, 100, 150, 200, 250, 300
Carrier sense range	About twice the transmission range
MAC type	IEEE 802.11 (the base for DSRC standard)
Channel bandwidth (Mbps)	6
Traffic type	CBR (UDP)
Period of message dissemination (ms)	100, 200
Message payload size (byte)	100, 200
Number of vehicles	600
Speed (km/h)	100, 120
Traffic density (vehicle/km/lane)	50
Number of lanes	8
Simulation time (s)	60

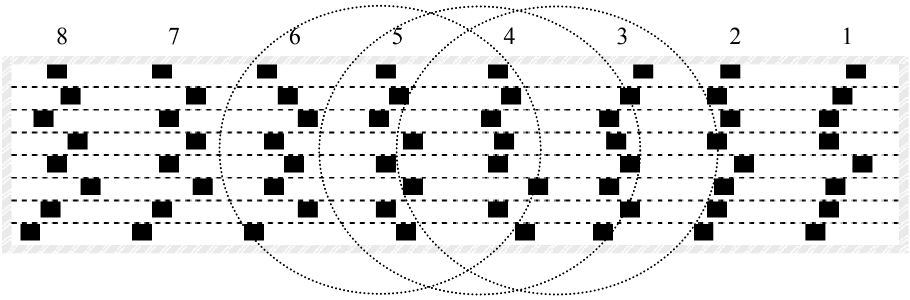


Fig.2 Traffic model of vehicles issuing beacon safety messages and their collisions

We investigate three different scenarios as follows:

(1) Scenario 10P200B: All vehicles send 200 bytes packets every 100 ms. In other words, each vehicle sends 10 packets of 200 bytes data every second.

(2) Scenario 5P200B: All vehicles send 200 bytes packets every 200 ms. In other words, each vehicle sends 5 packets of 200 bytes data every second.

(3) Scenario 10P100B: All vehicles send 100 bytes packets every 100 ms. In other words, each vehicle sends 10 packets of 100 bytes data.

In a typical forced-flow traffic phase, vehicles could be positioned relatively close to each other. Therefore when they want to send their information to neighbors, simultaneous messages collide with each other and the performance of the channel (in terms of delivery rate, delay, etc.) degrades severely. For example, in Fig.2 cars positioned in column 4, depending on their transmission range could interfere with each other and also near side columns (i.e. 5, 6, 3, 2). Each vehicle imposes some load on the shared medium which might result in saturated channel. The behavior of each communication protocol depends highly on the channel load. A saturated environment provides QoS challenges for any protocols. In the following sections we will discuss challenges which are mostly originated from this issue. Various factors affect channel load. For a given scenario, the channel load is obtained as follows:

$$channel\_load \text{ (bit/s)} = \frac{2LR}{d} \cdot \frac{1}{T_{\mathrm{I}}} \cdot P, \qquad (2)$$

where, L represents number of lanes, R (m) represents transmission range, d (m) represents average inter-vehicle distance, T_{I} (s) represents message dissemination interval time, and P (bits/packet) stands for message payload in bits. Table 2 shows the channel loads for the above-mentioned scenarios at different transmission ranges.

Table 2 Channel load in our three scenarios for different transmission ranges

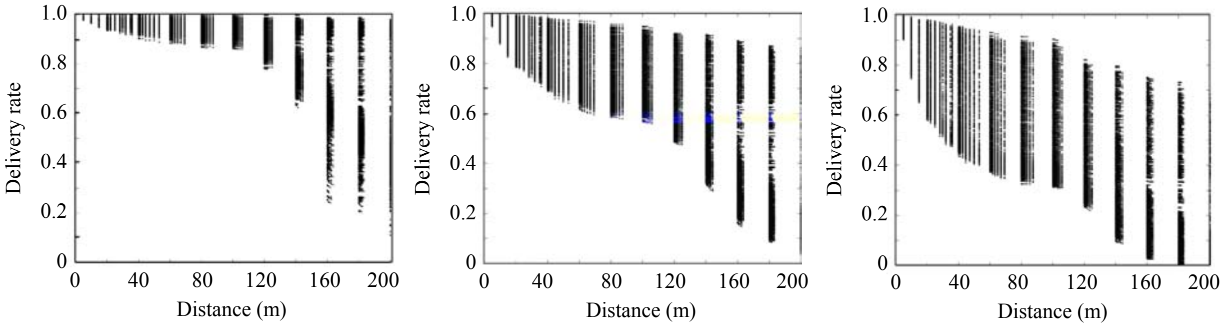
Scenario	Channel load (%)					
	50 m	100 m	150 m	200 m	250 m	300 m
10P200B	14	27	40	54	67	80
5P200B	7	14	20	27	34	40
10P100B	8	16	24	32	40	48

COMMUNICATION CHALLENGES

In this section we will show the most important communication challenges in beacon safety message dissemination protocols by using the above typical scenarios. These results help us to understand the performance of beacon message dissemination. Then in the next section we evaluate some methods to amend these problems through simulation study.

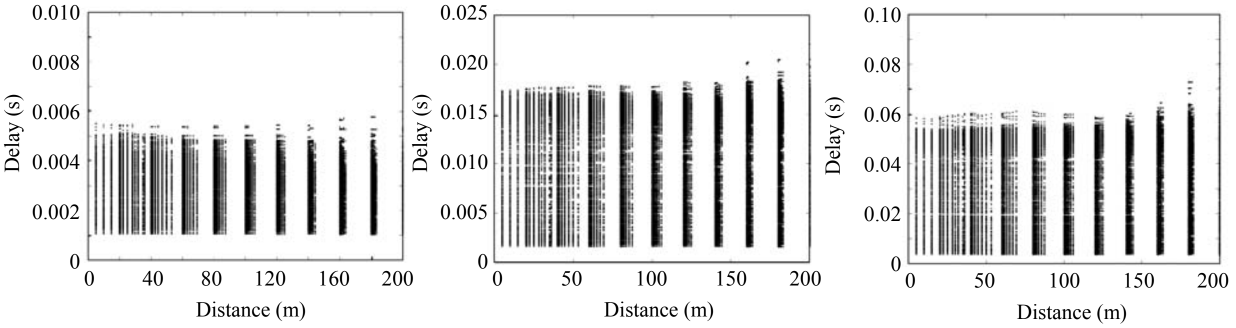
Poor reliability

In our first step, we investigate the influence of distance on delivery rate, which we define as the number of received packets by each vehicle divided by the number of sent packets by other vehicles. Since each message is broadcasted only once, this value is always smaller than one. This is important because of special characteristics of MAC layer which is based on CSMA/CA. On the other hand, safety level of any message dissemination algorithm is affected by the distance covered by the messages successfully. Figs.3a~3c show results for a typical transmission range, i.e. 200 m, in different scenarios. Since we intend to emphasize on strict QoS requirements of safety applications, we bring delivery rates for all available connections, not only average values. Therefore, each dot in Fig.3 (and also Fig.4) represents the delivery rate of a vehicle. As can be seen, the lower load scenarios lead to higher delivery rates. Besides, the delivery rates are decreasing dramatically by increasing the distance and especially this phenomenon is the worst in the border of transmission range (farther than 66% of transmission range, e.g. in the case shown in Fig.3, 130 m). We can describe this border effect, mainly by the well-known hidden terminal problem. A hidden terminal is one that is within the range of the intended destination but out of range of the sender (Tobagi and Kleinrock, 1975). This phenomenon is more troublesome in broadcast mode of IEEE 802.11 MAC layer than the unicast mode. In the unicast communications the partial solution to this problem is the use of RTS (Ready-To-Send)/CTS (Clear-To-Send) packets. However, RTS/CTS signaling should not be used in broadcast mode of IEEE 802.11 because (1) neighbor nodes' information is not available due to node mobility and thus they cannot be included efficiently in the RTS message, and (2) CTS messages sent by multiple receivers will result in collisions.



(a) (b) (c)

Fig.3 Broadcast delivery rate vs. distance from the sender, for transmission range=200 m, in different scenarios
(a) 5P200B; (b) 10P100B; (c) 10P200B



(a) (b) (c)

Fig.4 Delay for all nodes vs. distance from the sender, for transmission range=200 m, in different scenarios
(a) 5P200B; (b) 10P100B; (c) 10P200B

Acceptable delay

Although multi-hop message dissemination could be used for alarm safety messages, we argue that single-hop dissemination protocols would be much suitable in case of beacon messages. Since these messages are supposed to be exchanged between vehicles when they are close to each other, a single-hop transmission (which could be up to 500 m with current technology) is enough for a proper coverage. On the other side, multi-hop transmission for periodic messages causes the medium to be saturated very soon. There are three types of queuing delays which could be considered for each message as follows: (1) The delay incurred in the intermediate nodes: in single-hop dissemination, there are no intermediate nodes and thus we do not have the delay of the network layer. (2) The delay in the application layer queues: in the beacon message dissemination scenarios, if a packet was not sent while the new one is generated, simply it is overwritten by the new one and thus there is no such delay in our case. (3) The delay of channel acquisition because of the characteristicsof the MAC layer, it is the main cause of delay in case of beacon messages.

It should be stressed that there might be delays because of background traffic in the network. In general, the following decreasing priority order between different types of traffic is assumed: alarm safety messages, beacon safety messages and comfort messages (ordinary data messages). Therefore, the beacon messages are not delayed because of comfort messages. Furthermore, in the normal situations the number of alarm messages is quite limited and is ignored here, as we did not take alarm messages into account in the simulation. As a result, the message transmission delays are very low and for most cases below the acceptable value (i.e., 150 ms). This fact is shown in Figs.4a~4c, for three mentioned scenarios. Moreover, lower load scenarios present lower delays. However, there are some exceptions in very saturated medium situations, which will be addressed in the next section. As a result, we focus on reliability as a main concern and metric of QoS through this paper. Moreover, we will define in Section 5 another new metric to study the reliability more accurately for safety applications.

IMPROVING COMMUNICATION PERFORMANCE

Observing such a low delivery rate, the important question would be how to amend the adversity in order to get acceptable QoS for the safety applications. Although there are different ways to control the channel load, we investigate the effects of three parameters: transmission range, transmission interval, and packet payload size.

Transmission range

The transmission range is the average maximum distance in usual operating conditions between two nodes. Since radio transmissions are affected by the environment, it is quite difficult to predict the comportment of a system and to define a radio transmission range of a node in real life. These are some measurable characteristics which indicate the hardware performance in that respect. The transmitted power is the strength of the emissions measured in Watts (or mW). Government regulations limit this power, but also having a high transmit power will be likely to drain the batteries faster. Nevertheless, having a high transmit power will help to emit signals stronger than the interferers in the band. The sensitivity is the measure of the weakest signal that may be reliably heard on the channel by the receiver (it is able to read the bits from the antenna with a low error probability). This indicates the performance of the receiver, and the lower the value the better the hardware. Since sensitivity is hardware's characteristic, we change the power level to achieve different transmission ranges assuming two-ray-ground propagation model.

Whilst higher transmission range results in longer awareness distance and is better in safety point of view, it leads to larger interference domain. As a result packets are more likely to collide with each other and throughput degrades more severely. Finding the optimum power level to get higher capacity is a broadly studied topic in wireless literature, but most of the studies are addressing unicast situation in medium-density and low load scenarios (Kawadia and Kumar, 2005; Behzad and Rubin, 2005; Santi, 2005). There are quite limited studies for broadcasting environment. In this paper we examine transmission range from 50 to 300 m, assuming fixed and similar transmission range for all vehicles.

Transmission interval

This parameter is directly related to the requirements of the safety applications and should be determined based on vehicle speed, driver's reaction time, traffic density, etc. While smaller transmission interval can prevent unsafe situation in higher speeds and more unsafe conditions, it results in more saturated channel and so it is more likely to cause collision between simultaneous transmissions. To the best of our knowledge, finding the best value for this parameter has not been investigated analytically and even through simulation in the literature. We argue that the transmission interval, denoted by T_{I}, should be set in a way that all vehicles have enough fresh information about their neighbors. A vehicle can be supposed to have enough fresh information if the safety system has more up-to-date information about neighbors than the driver and so it warns the driver if he/she makes mistake. For example in Fig.5, a given vehicle B has fresh information about its neighbor A if it receives new information from A before B enters the awareness range of A. In other words, the following equation should hold:

$$T_{\mathrm{I}} \le (d - A_d)/V, \tag{3}$$

where T_{I} (s) stands for transmission interval time, d (m) stands for inter-vehicle distance; A_d (m) stands for awareness radius and V is relative speed. The awareness radius shown in Fig.5 should be relatively large to give the system in $\boldsymbol{B}$ sufficient time to be informed about any significant status (e.g. speed, position, etc.) changes of $\boldsymbol{A}$. Therefore, if we refer to the driver's reaction time by T_{stimuli}, then

$$A_d \ge V \cdot T_{\mathrm{stimuli}}. \tag{4}$$

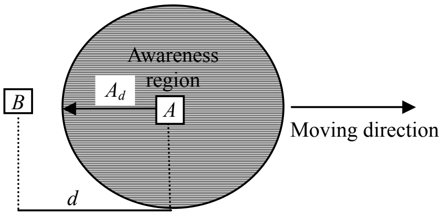


Fig.5 Beacon message dissemination interval computation

The value of message transmission interval (see Table 1) has been computed, giving two different levels of speed V=100 km/h and 120 km/h and

$T_{\text{stimuli}}=0.5$ s (Roess *et al.*, 2004), assuming the worst case when the vehicle in front has to stop completely.

Message payload size

To estimate the packet size value, we consider that every packet will contain several parameters composing the state of the sender, especially location, speed, road hazards, etc., according to some standards like SAE J1746 and MS/ETMCC (Xu *et al.*, 2004). In addition, by including security fields (optionally) which are very important in inter-vehicle communications we can reach message payload sizes ranging from 100 bytes to 500 bytes depending on the specific application requirements. Also, PHY and MAC layers add about 50 bytes to each packet.

Although more accurate information could provide safer situation, similar to what we argued for transmission interval, adding packet size may lead to more saturated channel and as a result more collisions. Nevertheless, due to the nature of CSMA/CA it could be intuitively understood that the effect of increasing packet size on the performance is not so adverse as that of increasing transmission frequency. This is because of the bottleneck of MAC layer, i.e., channel acquisition. In our simulations, we use two typical packet size values: 100 bytes and 200 bytes.

Simulation results

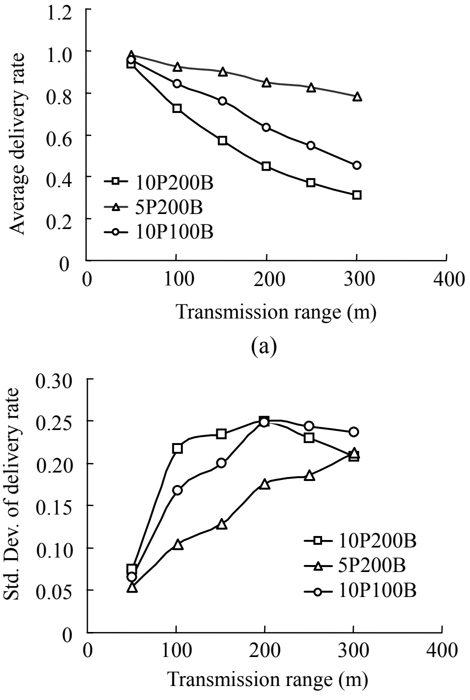
In order to evaluate the performance of our single-hop protocol and observe the effects of the above parameters on QoS, we measured the following three QoS metrics. The first two metrics are popular in networking performance evaluation while the third one, which is newly defined in this paper, is specifically used for evaluating QoS in safety scenarios.

(1) Single-hop broadcast delivery rate: This metric is a criterion for evaluating the reliability and is obtained by measuring the percentage of vehicles which successfully receive a packet amongst all vehicles positioned at a distance less than transmission range of the sender, at the moment that the packet is sent to the channel. This metric is one of the most important QoS requirements for any networking protocols and also for safety applications. Low delivery rates cause some vehicles to be unaware of the unsafe situations and results in accidental events. Since we aim to concentrate on the criticality of safety scenarios, we will present simulation results for both average delivery rate and standard deviation of delivery rates.

(2) End-to-end delay: we obtain this metric by measuring the time duration between issuing a safety message from a sender until it is received by vehicles in its one-hop neighborhood. Clearly, this parameter is also very critical for safety applications to be monitored. Messages delivered lately could be useless, as the driver would not have enough time to react. Therefore, low delay is necessary for a safety message. Since in single-hop message dissemination, delay values are generally acceptable (i.e., below 150 ms), here, we just bring average values for delay.

(3) Effective range: In a typical safety scenario, the range covered successfully by a safety application or the related message dissemination protocol is the most important QoS metric. This range can be defined as a distance at which for some intended metrics, acceptable level of quality is achievable. Here, the term ‘acceptable’ implies the satisfaction of pre-defined QoS confidence level. In this work, we define the effective range as the distance from the sender within which minimum delivery rate is higher and maximum delay is lower than pre-defined QoS confidence levels. Due to the criticality of safety scenarios, we will consider extreme values, not average values. Since the above simulation results showed acceptable delays in the case of single-hop, we just measure delivery rate for obtaining effective range. For situations where delays are higher than 150 ms, we shall consider effective range as zero. Since delivery rate metric stands for reliability, this new metric presents the reliability of the safety message dissemination protocol or application.

In what follows, some simulation results are given. Firstly the results for delivery rates of our single-hop algorithm are presented. Fig.6a shows average delivery rates versus transmission ranges for different scenarios mentioned in Section 3. As can be seen, by increasing the load of the scenario, the delivery rates are decreasing. In other words, increasing transmission range results in more crowded channel and therefore lower delivery rate is observed. Comparison between 10P100B and 5P200B scenarios could be interesting. According to Table 2, the imposed loads in both scenarios are close to each other but from Fig.6a we can see that the scenario with higher transmission interval and larger data packets behaves much better than the other, which sends smaller packets but more frequently. This phenomenon can be described by the nature of CSMA/CA MAC protocols, where nodes have to compete to acquire the channel. When the number of nodes grows, acquiring the channel becomes a bottleneck. Since sending more packets implies more frequent channel acquisition, our simulation results show lower delivery rates for the 10P100B scenario.



(a)

(b)

Fig.6 Delivery rate versus transmission range. (a) Average delivery rate; (b) Standard deviation of delivery rate

Moreover, Fig.6b shows standard deviation of delivery rates in terms of transmission range. Since safety applications are life-preserving applications, only average value of delivery rates does not say everything about the QoS level. Actually it could be misunderstanding as some vehicles may have very low delivery rates. This is the main reason that we presented the delivery rates of all vehicles in Fig.3. Having standard deviation of delivery rates in addition to average delivery rate give us more comprehensive insight about QoS level. Obviously lower standard deviation is more trusting from safety point of view. As can be concluded, standard deviation of delivery rates increases as the transmission range increases and more crowded channel usually leads to higher standard deviation of delivery rates. However, for distances greater than 200 m where the collisions are more than a threshold, almost all sent packets encounter saturated channel and the standard deviations start to decrease slightly.

Furthermore, we evaluate our protocol in terms of end-to-end delay. Results are shown in Fig.7 for average delays. As shown, although they follow a rising trend with increasing transmission range, delays are generally below our acceptable threshold 150 ms. The only exception is in scenario 10P200B where in the transmission range equal to 300 m, the channel gets highly saturated and average delay goes up to 550 ms. This is because in a busy medium each vehicle has to wait for a long time in order to acquire the channel.

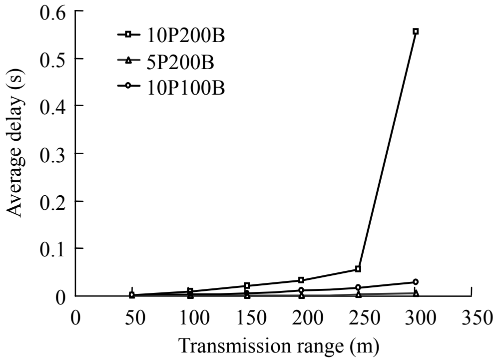


Fig.7 Average delay versus transmission range

The ultimate goal of any message dissemination protocol is to transfer messages to the intended receivers. Therefore, as a last analysis, we measure the range feasibility of the message dissemination protocol for safety applications by measuring effective range metric defined above. We consider a threshold equal to 90%. So, we measure the distances at which the minimum delivery rates are above 90% in each of the three mentioned scenarios. For scenario 10P200B, when the transmission range is 300 m, the effective range is considered zero because the delay is higher than the intended level. Fig.8 shows that 10P200B is the worse scenario because of saturated channel load. However, 5P200B presents a good effective range and can be a candidate as a sub-optimum design option. Note that although the imposed load in 5P200B and 10P100B are rather close to each other, the effective range of 5P200B is much larger in most of the cases. This fact can be described in that in 10P200B nodes have to compete for the channel acquisition more frequently than 5P200B.

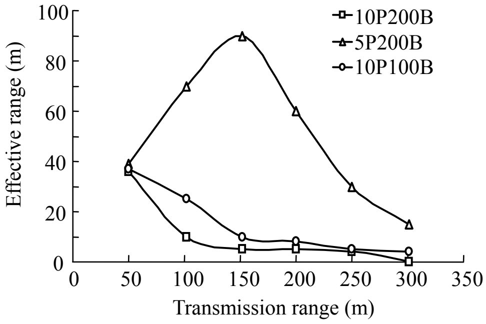


Fig.8 Message dissemination (communication level) effective range (for threshold of 90%)

While selected QoS confidence level (i.e., 90%) might not be suitable enough for many safety applications, we mention these results to show the effects of transmission range message transmission interval and message size on the effective range of the protocol. However, the QoS confidence level for message dissemination protocol is the function of the QoS confidence level of the safety application which is going to be deployed in the highest layer of the protocol stack. This issue needs a model which relates them. In the next section we will propose a framework for such a relationship.

Discussion

Our results show that safety applications in VANETs which need hard QoS satisfaction, despite of their criticality and public concern, have many severe communication challenges. The main cause of these challenges is MAC layer and its special characteristics of shared medium. Current trend toward using IEEE 802.11 MAC layer in VANETs is mostly because of implementation concerns. Nevertheless, intuitively, using more deterministic MAC layers (i.e., TDMA) could be quite better in terms of performance.

It can be understood from our work that accepting the challenges of MAC layer, we still have some design parameters, i.e., transmission range, transmission interval, packet payload size in order to improve the performance of the protocol. We showed the existence of an optimum set of values for these parameters which leads to higher delivery rate (i.e., more reliability) and lower delay. We also showed that decreasing the transmission frequency is more beneficial than decreasing packet size. This issue suggests that one promising method for alleviating saturated medium and at the same time taking care of requirements of safety applications could be sending more information but at lower frequency.

However, the difficulty becomes more apparent when we consider the fact that the above-mentioned design parameters should be chosen by taking into account both communication and safety points of view. For example, although in safety point of view, the longer transmission range is better (due to larger announcement area), it results in saturated medium for communication protocol. Therefore there should be some trade-off values for determining transmission range. Besides, similar considerations exist for transmission interval and packet payload size. However, finding the general optimum set of values for all three parameters is a kind of multi-constraint optimization problem which is difficult to solve. In our simulation study we found that the scenario 5P200B with transmission range 150 m shows the best performance in communication-level point of view but as we will explain in the next section we can achieve higher performance if application-level QoS is taken into account. It seems that ultimate answer for the beforehand mentioned problems, would be an adaptive algorithm which controls the load of the channel by setting design parameters dynamically, getting feedbacks from the vehicle's traffic situation.

APPLICATION-LEVEL QUALITY OF SERVICE

The communication QoS is of most interest to protocol designers, but application-level QoS is more important since it is related to user's satisfaction level. Relationship between these two types of QoS can be made based on the following considerations:

(1) In reliable data transfer protocols, communication- and application-level QoS are usually considered to be the same. This is partly due to the correlation between packets in data transfer applications. The compression techniques intensify this correlation.

(2) In real-time applications, application-level QoS could be different from communication-level QoS. For example the user may be satisfied by receiving the voice with some small interruptions; even some packets are lost in communication layer (e.g., network layer).

We believe that due to emergency aspects of alarm messages, these messages should be categorized in the first group while beacon message dissemination can be put into the second group. This is because loosing an alarm message might lead to incident, but in case of beacon messages each packet with fresh information overwrites the previous packet with stale information. So as long as a fresher packet can be received, safety applications (bases on beacon messages) may not be affected even though several stale packets are lost. Furthermore, the receiver can run a model to compensate for the lost messages by extrapolating from motion values received in the past. In the following we study the safety applications based on beacon messages and call it ‘safety application’ briefly.

Since in single-hop message dissemination, the delay values are mostly acceptable, we intend to model the relationship between communication reliability and application reliability. We assume that a safety application is reliable as long as at least one packet is received by the receiver during N transmissions of the sender. Let P_{com} be the reception probability of the communication protocol (i.e. the delivery rate for each vehicle in the related message dissemination protocol). P_{com} is generally defined as the QoS at the MAC layer level. After N transmission, the probability of receiving at least one of the messages would be:

$$P_{\text{app}}(N)=P(\text{at least 1 successful transmission in } N \text{ tries}) =1-P(\text{all fail in } N \text{ tries})=1-(1-P_{\text{com}})^N, \quad (5)$$

where, P_{app} is the reception probability at the safety application level. It should be emphasized that the above equation is valid only when the packet drops are independent and thus we can say $P(\text{all fail in } N \text{ tries})=(1-P_{\text{com}})^N$. Let T represent the time window duration for a safety application to work properly by receiving at least one message and assume t to be transmission interval of issuing each beacon message. Therefore, Eq.(5) can be rewritten as

$$P_{\text{app}}(T,t)=1-(1-P_{\text{com}})^{T/t}. \quad (6)$$

Eq.(6) presents the relationship between reliability of a typical safety application with attributes T, t (which should be given by safety experts) and the reliability of related communication protocol. Fig.9 shows this relationship for different values of T assuming $t=100$ ms. It shows that the application-level reliability could be higher than the reliability of related communication protocol.

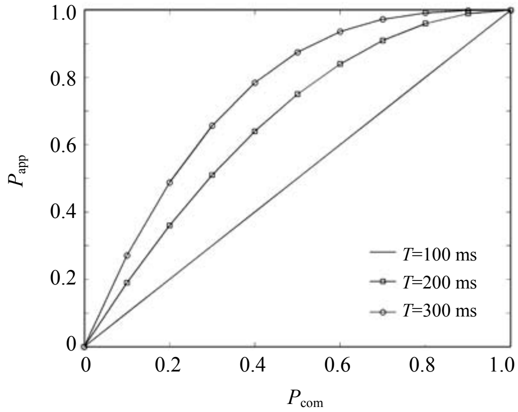


Fig.9 Relationship between application- and communication-level reliabilities for t=100 ms and different T’s

So far, Eq.(6) needs two attributes (T and t) for a given safety application. Moreover, in order to have a clear definition of the required level of QoS, there should be another attribute called QoS confidence level α, which is $P_{\text{app}}(T,t)\geq\alpha$ for all vehicles. As a result, these three parameters together define a safety application for our model. The values of these parameters should be extracted by safety experts and then used by network protocol and application designer. Based on these attributes, we classify safety applications as follows:

(1) Driver assistance safety applications, which are expected to assist the driver for different maneuvers like lane changing, turning left/right, etc. This class of applications can prevent many avoidable incidents caused by the driver’s error. From experiments and based on specific application, $95\% \leq \alpha \leq 99\%$ and $N \leq 3$ are reasonable values for this class.

(2) Automatic safety applications, which are expected to control the vehicle as stand alone systems. Undoubtedly this class of applications demand very high QoS confidence level above 99% and N=1.

In order to have some understanding about nominal applications, we consider two hypothetical safety applications with a QoS confidence level α of 95% and 99%. Then, we assume a time window T equal to 200 ms, 400 ms and 600 ms and a message dissemination interval t=200 ms.

We intend to find the application-level effective ranges. Using the given QoS confidence levels, we find the required threshold for P_{com} from Eq.(6) and then measure the effective range in our simulation using delivery rate for 5P200B. Fig.10 draws application-level effective range as function of the transmission range for different values of the time window T and the QoS confidence level α. As can be seen, despite very poor communication-level effective range, we can expect acceptable communication-level effective range for higher time windows. It suggests that driver assistance safety applications can be deployed with satisfactory effective range. However, when $T = t = 200$ ms the effective range is very low and hardly becomes above the average inter-vehicle distance, hence automatic safety applications cannot be deployed, at least with PHY and MAC layers which we used for our simulation. Fig.10 shows that by increasing the vehicle's transmission range, for each value of T there is a rising trend in application-level effective range until the delivery rates of the message dissemination protocol fall below the required P_{com}, computed from Eq.(6). As this required threshold is higher, the decreasing trend starts in lower transmission ranges as expected.

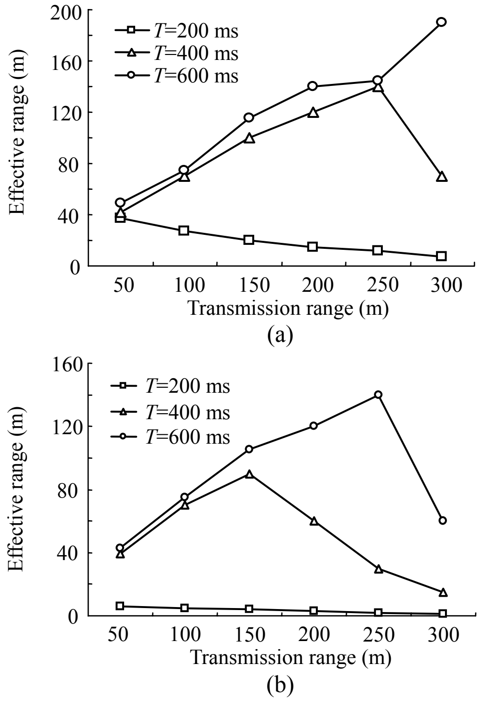


Fig.10 Application-level effective range versus vehicle's transmission range for different QoS confidence levels α in 5P200B scenario. (a) α=95%; (b) α=99%

We conduct our simulation assuming two-ray-ground propagation model which might not be necessarily a good modeling of real-life propagation model especially in VANETs, where there would be many obstacles and also the speed of cars affects signal propagation. Although worse results are expected in real implementations, the values of effective range in Fig.10 are promising for practical deploying.

CONCLUSION AND FUTURE WORK

In this paper we conducted extensive simulation study in order to evaluate the performance of beacon safety message dissemination in Vehicular Ad hoc NETworks. We pay special attention to safety requirements while studying networking performance issues. We realized that the reliability is the main challenge in beacon message dissemination. So, a new metric named effective range was defined which gives us more accurate facility for evaluating QoS in safety applications specifically. Then, in order to improve the performance, the effects of three parameters including vehicle's transmission range, message transmission's interval time and message payload size were studied.

In order to address the driver's satisfaction, we differentiated between communication- and application-level QoS and modeled the relationship between them. Then we evaluated application-level QoS for different classes of safety applications. Especially, we showed that even with current IEEE 802.11 and physical technology, driver-assistance safety applications can be deployed in near term. However, automatic safety applications which control the vehicle independent of the driver might need more mature communication technology in a rather long term period.

We strongly believe that experts in traffic safety should perform full investigation on QoS requirements of different safety applications in order to determine their related attributes (e.g., α, T, t to be imported in our model). This debate does not disallow technical effort for improving communication reliability, but it suggests simultaneous efforts to speed up the realization of safety applications by VANETs.

In our future work, we intend to: (1) investigate theoretical analysis for finding the best values of our design parameters, (2) develop methods for setting optimum or sub-optimum values of the design parameters in an adaptive approach depending on road traffic situation, e.g., speed, density, level of danger, etc., and (3) apply real-life vehicle mobility patterns and scenarios for investigation of coexistent phase in which both force- and free-flow traffic phases appear for a vehicle during its travel.

References

Adler, C., Eigner, R., Schroth, C., Strassberger, M., 2006. Context-adaptive Information Dissemination in VANETs—Maximizing the Global Benefit. Proc. 5th IASTED Int. Conf. on Communication Systems and Networks, p.7-12.

Alshaer, H., Horlait, E., 2005. An Optimized Adaptive Broadcast Scheme for Inter-vehicle Communication. Proc. 61st IEEE Vehicular Technology Conf., p.2840-2844. [doi:10.1109/VETECS.2005.1543865]

Andrisano, O., Nakagawa, M., Verdone, R., 2000. Intelligent transportation systems: the role of third generation mobile radio networks. *IEEE Commun. Mag.*, **38**(9):144-151. [doi:10.1109/35.868154]

Artimy, M.M., Robertson, W., Phillips, W., 2004. Connectivity in Inter-vehicle Ad Hoc Networks. Proc. Canadian Conf. on Electrical and Computer Engineering, p.293-298.

Behzad, A., Rubin, I., 2005. Impact of Power Control on the Performance of Ad Hoc Wireless Networks. Proc. 24th Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM), p.102-113. [doi:10.1109/INFCOM.2005.1497883]

Benslimane, A., 2004. Optimized dissemination of alarm messages in Vehicular Ad-hoc NETworks (VANET). *LNCS*, **3079**:655-666.

Borgonovo, F., Capone, A., Cesana, M., Fratta, L., 2004. ADHOC MAC: new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. *Wireless Networks*, **10**:359-366. [doi:10.1023/B:WINE.0000028540.96160.8a]

Crash Avoidance Metrics Partnership (CAMP), 2004. Identify Intelligent Vehicle Safety Applications Enabled by DSRC. Vehicle Safety Communications Project, Task 3 Report, Public Document.

Federal Communications Commission, 2004. FCC 03-324. FCC Report and Order, February.

IEEE, 2004. IEEE Standard 802.11p. Draft Amendment: Wireless Access in Vehicular Environments (WAVE). Draft 1.0.

Kabarowski, J., Zagorski, F., 2005. Reliable Broadcasting without Collision Detection. Technical Report, DELIS: Dynamically Evolving, Large-scale Information Systems. Germany.

Kawadia, V., Kumar, P.R., 2005. Principles and protocols for power control in wireless ad hoc networks. *IEEE J. Selected Areas Commun.*, **23**(1):76-88. [doi:10.1109/JSAC.2004.837354]

Korkmaz, G., Ekici, E., Özgüner, F., Özgüner, Ü., 2004. Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems. Proc. 1st ACM Int. Workshop on Vehicular Ad hoc NETworks, p.76-85. [doi:10.1145/1023875.1023887]

Li, X., Nguyen, T., Martin, R., 2004a. Analytic Model Predicting the Optimal Range for Maximizing 1-Hop Broadcast Coverage in Dense Wireless Networks. Proc. Int. Conf. of Ad-hoc, Mobile, and Wireless Networks, p.172-182.

Li, X., Nguyen, T., Martin, R., 2004b. Using Adaptive Range Control to Maximize 1-Hop Broadcast Coverage in Dense Wireless Networks. Proc. 1st IEEE Int. Conf. on Sensor and Ad Hoc Communications and Networks, p.397-405. [doi:10.1109/SAHCN.2004.1381941]

Lipman, J., Boustead, P., Chicharo, J., 2004. Reliable Optimized Flooding in Ad Hoc Networks. Proc. IEEE 6th CAS Symp. on Emerging Technologies: Frontiers of Mobile and Wireless Communication, p.521-524. [doi:10.1109/CASSET.2004.1321940]

Lou, W., Wu, J., 2004. Double-Covered Broadcast (DCB): A Simple Reliable Broadcast Algorithm in MANETs. Proc. 23rd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM), p.2084-2095.

Mohsin, M., Cavin, D., Sasson, Y., Prakash, R., Schiper, A., 2006. Reliable Broadcast in Wireless Mobile Ad Hoc Networks. Proc. 39th Hawaii Int. Conf. on System Sciences, p.1-10.

Morimoto, H., Koizumi, M., Inoue, H., Nitadori, K., 1999. AHS Road-to-Vehicle Communication System. Proc. IEEE Int. Conf. on Intelligent Transportation Systems, p.327-334.

Park, S., Palasdeokar, R.R., 2005. Reliable One-Hop Broadcasting (ROB) in Mobile Ad Hoc Networks. Proc. 2nd ACM Int. Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, p.234-237. [doi:10.1145/1089803.1089992]

Roess, R.P., Prassas, E.S., McShane, W.R., 2004. Traffic Engineering (3rd Ed.). Prentice Hall, Upper Saddle River, New Jersey.

Santi, P., 2005. Topology control in wireless ad hoc and sensor networks. *ACM Computing Surveys*, **37**(2):164-194. [doi:10.1145/1089733.1089736]

Tobagi, F., Kleinrock, L., 1975. Packet switching in radio channels. Part II: The hidden terminal problem in carrier sense multiple-access modes and the busy-tone solution. *IEEE Trans. on Commun.*, **23**(12):1417-1433. [doi:10.1109/TCOM.1975.1092767]

Torrent-Moreno, M., Jiang, D., Hartenstein, H., 2004. Broadcast Reception Rates and Effects of Priority Access in 802.11-based Vehicular Ad-hoc Networks. Proc. 1st ACM Int. Workshop on Vehicular Ad hoc NETworks, p.10-18.

Torrent-Moreno, M., Santi, P., Hartenstein, H., 2005. Fair Sharing of Bandwidth in VANETs. Proc. 2nd ACM Int. Workshop on Vehicular Ad hoc NETworks, p.49-58. [doi:10.1145/1080754.1080762]

Williams, B., Camp, T., 2002. Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks. Proc. 3rd ACM Int. Symp. on Mobile Ad Hoc Networking & Computing, p.194-205. [doi:10.1145/513800.513825]

Wischhof, L., Ebner, A., Rohling, H., 2005. Information dissemination in self-organizing intervehicle networks. *IEEE Trans. on Intell. Transp. Syst.*, **6**(1):90-101. [doi:10.1109/TITS.2004.842407]

Wu, L., Varshney, P., 1999. Performance analysis of CSMA and BTMA protocols in multihop networks. Part 1: Single channel case. *Inf. Sci.*, **120**(1-4):159-177. [doi:10.1016/S0020-0255(99)00047-X]

Xu, Q., Mak, T., Ko, J., Sengupta, R., 2004. Vehicle-to-Vehicle Safety Messaging in DSRC. Proc. 1st ACM Int. Workshop on Vehicular Ad Hoc Networks, p.19-28. [doi:10.1145/1023875.1023879]

Yousefi, S., Mahmoud, S.M., Fathy, M., 2006. Vehicular Ad hoc NETworks (VANETs): Challenges and Perspectives. Proc. 6th Int. Conf. on ITS Telecommunications, p.761-766. [doi:10.1109/ITST.2006.289012]