ilmedia

TECHNISCHE UNIVERSITÄT
ILMENAU

Schmidt, Robert Karl; Köllmer, Thomas; Leinmüller, Tim;
Böddeker, Bert; Schäfer, Günter:

Degradation of transmission range in VANETs caused by interference

R.K. Schmidt, T. Köllmer, T. Leinmüller, B. Böddeker, and G. Schäfer

Degradation of Transmission Range in VANETs caused by Interference

Robert Karl Schmidt received his Diploma degree in Computer Science in 2008 from the Technical University Ilmenau, Germany. Afterwards, he joined DENSO AUTOMOTIVE Deutschland GmbH where he focuses his research activities on efficient communication and security in vehicular ad hoc networks.

Thomas Köllmer studies Computer Science at the Technical University of Ilmenau. At DENSO Automotive Deutschland he was researching communication protocols for vehicular ad hoc networks. His further research interests lie in the fields of network security and cryptography.

Tim Leinmüller received his joint-degree in Electrical Engineering from ENST-Paris and University of Stuttgart in 2003. Afterwards, he worked for DaimlerChrysler AG Group Research and Advanced Engineering. In 2007 he joined DENSO AUTOMOTIVE Deutschland GmbH, where his activities focus on research and standardization in the area of Car2Car Communication.

Bert Böddeker graduated with a PhD in computational physics on 'simulation of surfaces of metallic glasses' (has to do with wireless communication between cooperative systems of atoms). Until 2004, he worked as a pioneer on automotive wireless communications for connecting nomadic devices using Bluetooth technology at Berner & Mattner GmbH. Since 2004, he is a Research Engineer Business Planning at DENSO AUTOMOTIVE Deutschland GmbH. His responsibility includes the European part of DENSO's strategy for cooperative systems for vehicle safety.

Günter Schäfer is a full professor of telecommunications/computer networking at the University of Ilmenau, Germany. His main subject areas are network security, protection of communication infrastructures, as well as communication protocols

and architectures. He is a member of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE) and the German Gesellschaft für Informatik (Computer Science Society).

ABSTRACT

Reliability is one of the key requirements for inter-vehicle communication in order to improve safety in road traffic. This paper describes the difficulties of inter-vehicle communication. We focus on an analysis of the state-of-the art MAC protocol draft IEEE P802.11p and its limitations in high load situations. For our analysis we consider a particular safety scenario: An emergency vehicle is approaching a traffic jam. In a simulation experiment, we highlight that severe packet loss can occur. The reliable transmission range can be reduced by up to 90 %. The main reason for this degradation is interference caused by transmissions of other vehicles within the traffic jam. In the study, we focus on the vehicle at the very end of the traffic jam. There, we measure the number of packets per second that are successfully received from the emergency vehicle. The key observation is that only a small fraction of the warning lead time remains which will also reduce the time for the driver to react on this information on an approaching emergency vehicle.

1 INTRODUCTION

Vehicular communication enables the direct exchange of information among vehicles. Such Vehicular Ad-Hoc Networks (VANETs) can support infotainment, traffic efficiency and, most important, safety-related applications. For example, vehicles can warn each other of dangerous locations like an icy road or the end of a traffic jam. Hence, saving life and preventing injury in road traffic is the driving force behind the development of inter-vehicle communication. For these applications it is essential that the inter-vehicle communication is reliable and robust.

Regarding the communication aspects, VANETs are confronted with diverse situations, ranging from very low vehicle densities up to very high vehicle densities. A lonely rural road, high speed autobahn as well as a congested metropolitan area are typical examples. In all of these situations, VANETs have to operate reliably.

Since inter-vehicle communication in VANETs is similar to communication in mobile ad-hoc networks (MANETs) the protocols are also similar. It is envisioned [1] to basically apply ad-hoc communication according to IEEE 802.11 but without the need to form a basic service set in order to improve the ad-hoc capabilities. The respective amendment, IEEE P802.11p [13] is currently under development.

In this kind of communication, i.e. wireless ad-hoc broadcast, the commonly known mechanisms of IEEE 802.11 aiming at reliability of communication do not apply. Acknowledgments or even multi-stage handshakes like RTS/CTS are not realistic for VANETs to support successful message distribution. On the one hand, RTS/CTS are designed for unicast communication. On the other hand, such a handshake is only appropriate if the amount of data to be transfered is much higher than the overhead from RTS/CTS handshake. In VANETs, only few data is sent but periodically, comprising the current position and movement, and maybe additional location information, like a low friction information. The transmitting vehicle can not assure proper reception at the surrounding vehicles. This is because the receivers may be unknown to the sender and no feedback mechanisms are applied, i.e. acknowledgments and retransmissions are not performed.

The basic medium access in ad-hoc mode may provide good performance with low network load. However, in high-load scenarios, an increased loss of messages may occur.

In this paper, we study such extreme situations and analyze the behavior of the current state-of-the-art MAC protocol draft IEEE P802.11p. We define the metric *Reliable Transmission Range*, by which we evaluate different message load scenarios and their influences. Further, we provide insights into the significance of packet loss and derive reasons for packet loss in inter-vehicle safety communication. As we will show, the interference caused by other vehicles' transmissions is the dominating reason. In a simulation study we show the degradation of the reliable transmission range, its origins in the MAC protocol and its mechanism of assessing the occupancy of the communication medium.

The likeliness of interference is significant in high density scenarios. Therefore, we choose a simulation scenario where a vehicle sending important messages, e.g. an emergency vehicle is approaching a very high traffic density. In order to benefit from such an application, which means a reduction of time for the emergency vehicle to arrive at its destination, all vehicles within the traffic jam must be able to receive messages from that particular vehicle. Especially, vehicles at the upstream (the tail-end) of the traffic jam need this information as soon as possible. A loss of information would cause a reduction of time for the driver to steer his car out of the way. In such a scenario, the VANET specific characteristics are obvious. A single node rapidly entering an area of very high node density is regarded as one of the big issues in VANET communication. With this scenario, we are able to evaluate such a situation with a concrete application background. We evaluate the packet loss occurring in different distances to the traffic jam. We also show that the severity of packet loss suddenly increases in high message/node density situations. At some point, a slight increase of the offered load can cause even a message loss of almost 100 % at low distances to the traffic jam.

The remainder of this paper is structured as follows. Section 2 explains the background on signal propagation with focus on VANETs. In Section 3 we take a detailed look at IEEE P802.11p and its consequences on communication. Then, Section 4 summarizes the reasons for packet loss resulting from signal propagation and medium access. The simulation study and its observations are discussed in Section 5. In Section 6, we compare our observations with related studies. We finally draw conclusions in Section 7.

2 RADIO SIGNAL PROPAGATION – ASSUMPTIONS AND MODELS

This section summarizes basics of signal propagation. From a single transmitter's point of view, signal attenuation is the limiting factor for the transmission range. It can be divided into a small and large scale part, i.e. fading and path loss. Small-scale fading, e.g. Doppler spread will be neglected here as we focus mainly on the total signal power which results in interference in far distances. The impact of Doppler spread on communication is discussed for example in [20].

Large-scale path loss in turn, will be described in the first part of this section. The second part covers with external influences that reduce the transmission range: Interference and Noise. Following, we use the Signal-to-Noise Ratio (SNR) to express the strength of a focused signal compared to the noise, whereas the Signal-to-Noise-Interference Ratio (SINR) accumulates the noise and the sum all interfering signals in relation to the focused signal.

The development of models for radio signal propagation is typically done using statistical values from particular regions or even cities. Practical measurements made for a particular communication system in the respective environment are taken to build up such a statistical model [17]. Path loss models compute the signal attenuation or received signal strength for a given distance between transmitter and receiver. Besides signal attenuation due to air propagation there are other important attenuation influences:

— *Reflection:* The electromagnetic is reflected a large surface with a comparably higher dimension than the wavelength.
— *Shadowing:* Particular objects reflect the wave into the opposite direction or strongly attenuate the signal so that behind these object only a weak signal remains.
— *Diffraction:* The wave is bent behind a sharp edge of an object. Thus the wave is able to propagate beyond shadowing objects.
— *Scattering:* In contrast to reflection where the surface must be relatively large, scattering occurs at small dimension surfaces compared to the wavelength. Rough surfaces like plants or trees scatter the wave to multiple directions.

In VANETs we assume that reflection and shadowing are more important than diffraction or scattering as they occur in all environments. A commonly huge surface for reflection effects is the surface of Earth. Regarding shadowing, large vehicles like trucks will strongly contribute to signal attenuation. So, we will also explain the common models for these effects which estimate the average received signal strength. Note that more sophisticated models like ray tracing which accurately track each beam's path are out of scope for this paper. This includes modeling of diffraction effects which depend on the presence of sharp edged installations like buildings. An interesting discussion on ray tracing in outdoor urban wireless networks can be found in [16].

2.1 Large-scale Signal Attenuation: Path loss

A common (non-statistical) model that allows to compute the received signal strength in line-of-sight (LOS) areas is given by the simple transmission formula established by H.T. Friis [8] in 1946. It only considers the signal attenuation over the air and neglects non-line-of-sight (NLOS) components. Assuming an isotropic antenna, the signal power is projected to an area (the surface of a sphere). Hence, it attenuates quadratically with the distance.

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

with P_t the output power of the transmitter, the antenna gains at transmitter and receiver, i.e. G_t and G_r, the wavelength λ and the system loss L which is not related to propagation As seen in above equation, the received power P_r depends mainly on the distance d between transmitter and receiver. This model has been formerly used for satellite communication and microwave radio links [17].

Effects like reflection from the surface of Earth are considered in the Two-Ray Ground model. Strong signal attenuation is commonly modeled using Log-Normal Shadowing. Both models will not be discussed here for the sake of space. The reader is kindly referred to [17].

2.2 Signal to Interference and Noise Ratio

The signal quality and hence the ability to decode information from radio waves depends on the ratio between the focused signal and the sum of all present non-focused (and weaker) signals including the noise floor. This is called the Signal-to-Interference-Noise Ratio (SINR). The ratio expresses that the stronger the signal, the better the signal quality and hence the lower the packet loss probability. The same consideration is valid for the interference, i.e. the weaker the interference, the better the signal quality.

In 5.9 GHz, atmospheric, cosmic or man-made sources do not significantly contribute to the noise level [10]. Only the noise in the receiver antenna has a noteworthy impact on the signal-to-noise ratio. It is often called Thermal Noise. Using the respective equation [17], one can easily determine the noise floor in VANETs being —104 dBm.

Interference has been known to be the key issue for the system performance in cellular networks for years [17]. It can be caused by stations transmitting in the same cell, in a neighboring cell or base stations in the same frequency band. In cellular networks, the problem is coped by a central entity, the base station which organizes the transmissions of its connected mobile phones. Similar problems of interference arise in inter-vehicle communication. However, in VANETs there will be no channel access coordination by a central instance. Analyzing the inter-vehicle interference is part of the simulation study in this paper. In the following, we discuss potential interference due to the OFDM modulation schemes as well as in multi-channel operations.

For inter-vehicle communication, OFDM schemes for signal modulation will be used (see Section 3). Thus, it is clear that a multi-carrier approach is chosen. In such a setting, a high peak-to-average power ratio arises. Each sub-carrier may have a very high peak power. Simply speaking, the result of such high power variations may lead to an out-of-band radiation.

Power leakage and hence interference from neighboring bands into the currently used band is called *Adjacent Channel Interference*. For example, if there are two communication channels directly next to each other, the communication on each channel causes interference to the other channel due out-of-band radiation of the transmitter [17]. Another cause is due to imperfect receiver filters where the receiver is not accurately tuned to the focused channel.

As long as the interferer is spatially separated sufficiently from the receiver, this interference may not lead to information loss. However, if the transmitter is far away from the receiver and hence has a high path loss, the receiver is more sensitive to a near interferer. This situation is commonly referred to as the Near-Far Effect. In other words, the interferer causes sufficient interference to the focused channel so that the SINR ratio becomes too low. Hence, the receiver is not able to decode information.

3 VANET COMMUNICATION BACKGROUND

Vehicular Ad-Hoc Networks comprise unique characteristics compared to Mobile Ad-Hoc Networks. High node mobility and the large spectrum of node densities are known issues for inter-vehicle communication. More specifically, when it comes to applications for road safety the number of constraints is increased. This section explains these specialties by a discussion of the relevant aspects of the IEEE 802.11 protocol family. In this discussion, we are already able to identify issues that may reduce the reliable transmission range.

Table 1 Data rates, modulations, receiver sensitivities as specified by IEEE 802.11 for 10 MHz channel bandwidth.

Data rate	Modulation	Coding rate	Sensitivity (dBm)
3	BPSK	1/2	-85
4.5	BPSK	3/4	-84
6	QPSK	1/2	-82
9	QPSK	3/4	-80
12	16-QAM	1/2	-77
18	16-QAM	3/4	-73
24	64-QAM	2/3	-69
27	64-QAM	3/4	-68

The currently discussed MAC layer standard for VANETs is IEEE P802.11p [13] which is an amendment to IEEE 802.11-2007 [12]. Hence, the following describes the relevant concepts of IEEE 802.11(p) for medium sharing and derives issues for further investigation.

3.1 Data modulation

The Physical Layer Convergence Procedure (PLCP), a sub-layer of IEEE 802.11 defines how data is modulated into signals which are transmitted over the air. Table 1 lists the specified OFDM modulation techniques. The available data rates range

from 3 to 27 MBit/sec according to a channel width 10 MHz. The lowest data rate with the most robust modulation scheme BPSK and lowest coding rate must be feasible with at least —85 dBm received signal strength, i.e. low packet error rates. With increasing data rate, the demand for signal strength increases. For 27 MBit/sec, —68dBm receive power are required.

The respective data rate is applied mainly to the payload. The preamble as well as PLCP which comprises the frame length are coded with most robust data rate, i.e. 3 MBit/sec. Note that at the very beginning of packet, a training sequence is sent which allows receivers to synchronize the following transmission and to equalize the sub-carriers. This is also done to compensate the different velocities of transmitter and receiver. Summarizing, a frame consists of three parts: *1)* Training sequence and *2)* preamble which will be used to trigger and set up the receiver to the respective data rate of the *3)* payload. *1)* and *2)* are needed to detect a packet transmission and *2)*. The preamble includes information how to decode the payload.

Considering the different demands of signal strength, the transmission range of a vehicle can be divided into three ranges, depending on the distance to the transmitting vehicle. Fig. 1 displays them: The communication range is the area where both receiver sensitivity threshold and SINR are met for the payload. Vehicles within this range of the transmitting vehicle are able to decode packets. The detection range, also called carrier-sensing-range, describes the area where other vehicles can detect an ongoing transmission. The detection range is typically larger than the communication range as the SINR for preamble decoding is commonly lower due to a more robust modulation.

Finally, the interference range starts from the point where either the absolute signal power or the SINR is too low to decode information. The transmission of other vehicles in this range are interfered and their local SINR is degraded by this transmission. Theoretically, this area is unlimited but at some point the power of the vehicle's transmission is lower than the thermal noise and hence can be neglected.

3.2 Medium access

In contrast to wired networks like Ethernet where collision detection (Carrier Sense Multiple Access/Collision Detection, CSMA/CD) is applied, stations in wireless networks access the medium by avoiding simultaneous access and thus resulting packet collisions (Collision Avoidance, CSMA/CA). Avoiding packet collisions is the task of appropriate Phy/MAC layer mechanisms, which is basically achieved by listen-beforetalk. Before sending, the medium is locally evaluated whether it is clear or not. If clear, a random backoff timer is applied before starting the transmission to further avoid medium access collisions.
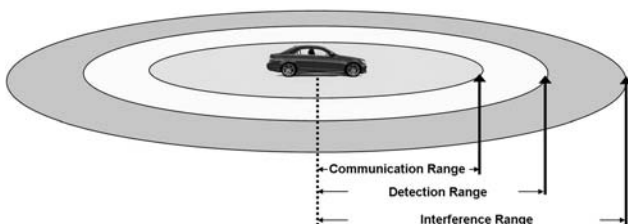
In the IEEE 802.11 protocol family there are two different mechanisms which can be applied for wireless medium access: Point Coordination Function (PCF) and Distributed Coordination Function (DCF). The former needs a central node that provides medium access opportunities to each associated station. DCF operates in a fully distributed manner. All stations access the medium more or less randomly. For that mechanism, it is also noted in IEEE 802.11 [12] that the "DCF is designed to reduce the collision probability between multiple STAs [Stations] accessing a medium, at the point where collisions would most likely occur". That point is the end of a transmission where stations start to contend for the shared medium.

The DCF basically randomizes this waiting time. Two kinds of waiting times are specified: Interframe Spaces (IFS) and the Contention Window (CW) which is divided into equidistant Backoff Slots[1]. So, once the medium is found clear after an ongoing transmission, the station waits for a time given by the Distributed IFS (DIFS) plus the random number of backoff slots. During the whole waiting time, the medium occupancy is assessed. If the medium has become busy before the local backoff has expired, the current value of the backoff is frozen and resumed after the currently ongoing transmission by another station (which has won the contention for the medium). The current draft version of IEEE P802.11p plans to use the DCF for medium contention. It will be enhanced by prioritization techniques according to IEEE 802.11e [11], namely the Hybrid Coordination Function (HCF). As shown in Fig. 2 the HCF allows to make the DIFS variable depending on the priority of the packet. The resulting Arbitration Interframe Space AIFS[*i*] where i is the access category (priority) can be extended for lower priority packets. Also, the length of the contention window varies among different priorities. Highest priority packets have thus the shortest AIFS and the shortest contention window to ensure high likeliness of medium access. The initial contention window size is limited by the CW_{min} parameter. In case of a collision in medium access, this value is doubled. If there are further access collisions it is doubled up to CW_{max} at each stage. This quickly relaxes the problem of medium access collisions. For details on this mechanism, the reader is referred to the study of Banchs and Vollero in [2].
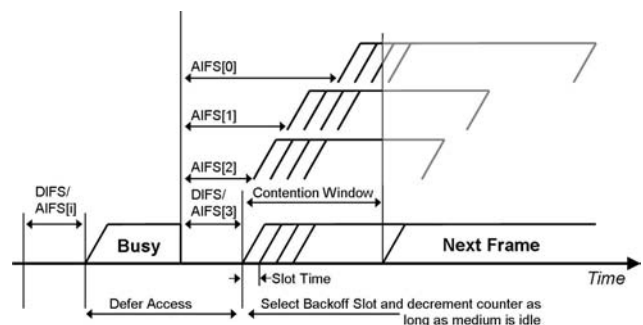
Fig. 2   Interframe Spaces and Contention Window as specified in IEEE 802.11 [12].

For broadcast communication, there is no error-handling as there are no acknowledgments and hence no exponential backoff growth. As the contention window size is not increased, CW_{min} always defines the upper limit for the backoff counter. This limits the prioritization and even increases the likeliness of

Fig. 1   Communication range, detection range and interference range of a transmitting vehicle.

---

1   The length of each backoff slot represents the MAC-layer end-to-end delay. It is dominated by the signal propagation and processing time and is between 9 to 16 µs.
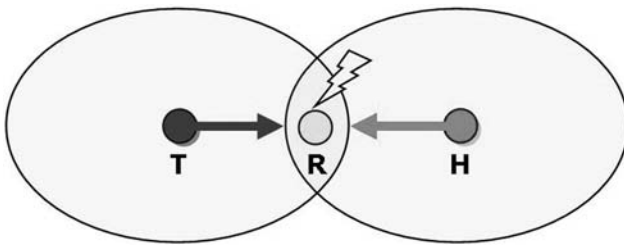
Fig. 3   Transmission from T is not successful at receiver R due to a colliding transmission from Hidden Station H.

packet collisions. In case there are two (or more) stations selecting the same backoff counter, they will start the transmission at the same time resulting in a packet collision. For an idle medium, which also covers the case where all stations wait the DIFS time, a station having a new packet shall not back off (as "the medium is not determined to be busy" [12]). This fact increases the probability of packet collisions.

Packet collisions can not be fully prevented by the DCF approach. It is still possible that there are two or more stations starting a transmission at the same time. In this case, the carrier sensing would not provide the correct channel assessment as the signals need some time to propagate. However, this propagation time is very low as signals at 5.9 GHz travel at a velocity of the speed of light. As the intended communication range lies in the order of some 100 meters, the propagation delay is in the range of some microseconds and hence the probability of such a packet collision is low. Nevertheless, the medium access mechanism fails to avoid a collision. Even worse, it fails when the received signal is too weak to be detected but is sufficiently high to result in a packet collision at some receivers in-between.

Situations where there are two concurrent transmission are often described using the term Hidden Station. Fig. 3 displays the typical view on the constellation of three stations *T, R, H*. Station *T* starts communication with station *R*. As station *H* does not hear the transmission of *T*, it is hidden to *T*. Once, it also starts transmission, *T*'s and *H*'s packets collide. In MANETs, this problem is addressed by the four-way RTS/CTS/DATA/ACK handshake. A station *T* that is willing to start a transmission to one particular station initializes this handshake procedure by sending a Ready-to-Send (RTS) message. The recipient *R* responds with a Clear-to-Send (CTS) message addressed to *T*. Once, *T* got the CTS message it is allowed to send DATA packets comprising the actual information that *T* wants to provide to *R*. *R* in turn acknowledges each DATA packet with an ACK message. Summarizing this procedure, each station in the surrounding of *T* and *R* knows of their communication and refrains from accessing the medium concurrently.

The main application for this procedure is Wireless LAN communication between access point and station or in ad-hoc mode between two stations. Unfortunately, it does not apply for inter-vehicle (safety) communication. Not having unicast communication is one reason. Each vehicle always conducts a local broadcast of its status information. Another reason is that the RTS/CTS approach needs stable conditions, e.g. positions of the nodes and a stable communication link. Furthermore, handshakes cause additional message overhead. So, RTS/CTS is reasonable if the actual amount of data to be transmitted is much higher than the overhead. Also, in contrast to MANETs,

the transmitting vehicle is not able to detect packet loss and thus will not repeat a transmission in case of a collision.

4   REASONS FOR PACKET LOSSES

The last section has introduced the protocol mechanisms of IEEE 802.11 that will be applied in VANETs. Medium access will follow a best-effort strategy with limited packet prioritization elements. It is already clear that in high-load situations a significant number of packet collisions may occur. In this section, we summarize the reasons of packet loss that are obvious from protocol and signal propagation point of view. We then formulate questions on the significance of the problem and dependability on particular parameters which our simulation study in Section 5.

As explained in Section 3, the hidden station effect is commonly seen as one of the main reasons for packet loss in mobile ad-hoc communication, i.e. two overlapping transmissions. Yielding a packet loss is not always the result. So, a packet collision is not equal to a packet loss. Only if there is a too low SINR for the strongest signal, this transmission can not be decoded.

Again considering the SINR, the location of the hidden station may be only within interference range to the receiver. The received power from the hidden station might be enough to interfere with a weak signal from the focused transmitter. When we take multiple far-distance hidden stations into account whose interferences accumulate, this effect may lead to significant packet loss.

The former discussion focused on the hidden station effect from a spatial point of view. A second part of the hidden station effect is in the time domain. The transmission of two stations may be hidden to each other as both start their transmission within the same time slot. As we know from the discussion of the HCF in Section 3 the maximum number of backoff slots is limited to 15. It is easily imaginable that VANETs can experience situations with much more vehicles than available backoff slots. Hence, a significant packet loss probability may arise. An evaluation on this problem can be found in [5]. There, an analytical model is built using Markov chains to compute the packet collision probability.

The Exposed-Station Effect is another effect responsible for implicit packet loss in MANETs which means that packets are lost within the station, due to a packet drop in the message queue, instead of a packet loss on the air. For RTS/CTS communication this effect is known for unnecessarily blocking a communication between two nodes C and D, if C heard a successful RTS/CTS-dialog between two nodes A and B. Although C's communication partner D may be out of range of A and B, C's transmission of the CTS would interfere. So, in case C receives a RTS from D, it will not respond as long as the communication between A and B persists.

As RTS/CTS can not be realized for safety communication as it is always a local broadcast, this effect does not apply exactly as stated before. But it is worth mentioning that vehicles may be exposed in high load scenarios where the carrier is nearly all the time found busy. The connection to packet loss here is that for the exposed vehicles the local message queue becomes full. In the worst case, not even one message can be sent. Such a situation can be described as local message congestion. Packet loss then occurs depending on the message dropping stra-

tegy. In case of time-critical information like the vehicle's status messages only the newest one may be of interest for other vehicles. The packet loss in this case would concern all packets except for the newest one[2].

If we now consider highly varying node densities this consideration also reveals that even in locally low densities stations may be exposed if there are high densities within carrier sensing range. In this case, some nodes would be blocked from transmission unnecessarily.

To sum up this discussion, we have identified the following sources of packet loss[3] and hence transmission range degradation:

— *Fully Interfered Receiver:* The SINR at the receiver is too low already from the beginning of transmission. The receiver may not even be able to sense the packet. Many stations within interference range can together cause sufficiently high accumulated interference even if they are far away. This high interference level may also result from nearby stations transmitting on an adjacent channels
— *Classic Hidden Station:* During the reception, the SINR deteriorates due to a colliding transmission. Packet loss occurs if the minimum SINR is not given anymore.
— *Hidden Station in Time Domain:* Regardless of the distance between two transmitters, a collision can occur if at least two stations have the currently lowest backoff slot. Hence, they start the transmission at the same time. This also allows for two colliding transmissions within receiving range of each other which is in contrast to the classic hidden station. We will call this effect Simultaneous Sending in the following.
— *Exposed Station:* Packet loss implicitly occurs due to local message congestion if the medium can not be accessed in high-load situations.

With this discussion in mind, we want to investigate the problem in a typical VANET scenario. Besides the analysis of each packet loss source, we measure the efficiency of the communication using the metric *reliable transmission range*. We assume a range is reliable if at all locations in-between, the packet error rate per second is below 10 %. It is assumed that the beacon rate is chosen by the applications, as low as possible. So, if there is some information missing due to packet loss, applications do not work properly. We account this by assuming that 10 % is a significant but tolerable loss. Following, we formulate questions to the simulation study based on the above discussion:

— What is the packet-loss-dominating factor?
— Is total offered load in general, or are particular parameters dominating, like the beacon rate or the packet size?
— As the packet size is currently not fixed and as the discussion covers a wide range of packet sizes: What is better, larger or smaller packets? Does the sending of few large or many small packets lead to a better reliable transmission range?

5 SIMULATION STUDY

To evaluate the different reasons for packet loss in VANETs, we have performed a simulation study. In this section we describe the VANET scenario and our simulation model. The key observations from the simulation study and its conclusions are discussed in the last part of this section.

Table 2 Simulation parameters overview

Fixed Parameter	Value
Simulation time	85 seconds
Number of runs	20
Signal propagation Friis'	Transmission Equation
Transmit Power	16 dBm
Rx Sensitivity	—91dBm
CCA Threshold	—65dBm
Carrier/Receiver SINR	5/8 dB
Noise/Interference model	Thermal/Accumulative avg power
Maximum communication range	960 meters
Link-/MAC-Layer Protocol	IEEE P802.11p 5.0
Data rate	6 MBit/s
AIFS (Best Effort)	6
Contention Window	7 … 15
Maximum vehicle velocity	120 km/h
Number of lanes	3
Number of vehicles	100
Length of traffic jam	~2100 meters
Meters per vehicle	~21 meters
Variable Parameter	**Values**
Message length	50, 200, 1000 Bytes
Message rate	2-200 Msgs/sec

5.1 Scenario Description

For our study, we want to take into account the special characteristics of VANETs when designing the road/traffic scenario. For the efficiency of ad-hoc communication, very low and very high node density can cause significant difficulties. As we explain in the following, our road scenario connects both extreme situations and considers a safety application.

The scenario starts with one vehicle driving on a three-lane autobahn at constant speed. Thus, the node density per kilometer is very low. Then, the node density increases strongly as the vehicle approaches a traffic jam with other vehicles standing still on all lanes. For the sake of simplicity we neglect oncoming traffic.

The question that we investigate in this scenario is what happens to the communication efficiency during the transition between low and high node density. In our scenario this is between the time at which the tail-end vehicle in the traffic is within theoretical communication range and the time at which the approaching vehicle has reached the traffic jam. In other words, what happens to the warning lead-time where car-tocar communica-

---

2 If the strategy is *drop all old beacons*.
3 For the sake of completeness, the reader is referred to [19] which describes receiver capabilities to receive the strongest of the colliding packets.

tion can provide a gain of knowledge about upcoming road traffic events?

The road traffic scenario is one part of an overall VANET scenario, the other part is the communication pattern. We assume that all vehicles send a constant number of status messages (beacons) per second. Each message has a fixed length and it is sent with the same transmit parameters, e.g. transmit power, antenna configuration, etc.). In the road traffic scenario above, this leads to a significant increase of offered messages from the approaching vehicle's point of view. This could be the scenario for safety application like the "Notification of an Approaching Emergency Vehicle" [1]. Assuming an emergency vehicle approaching, this application would inform all drivers within the traffic jam to be alerted and even to inform particular vehicles to clear a lane for that emergency vehicle to pass through. The investigation of transmission range degradation focuses on the (broadcast) communication between the Emergency Vehicle (EV) and the last vehicle at the end of the traffic jam, i.e. the Upstream Vehicle (UV). At the UV we measure the number of packets per second received from the EV.

5.2 Simulation Setup

For our simulation study we use JiST/SWANS [4], [3] with the extensions from the University of Ulm. The additional STRAW-package offers a integrated mobility model, enabling the simulated network nodes to move on streets. With the additional STRAW-package, vehicular movement is simulated. Therewith, we set up our road scenario: A traffic jam is built by setting the nodes velocity to zero, the approaching vehicle behaves normal.

During the simulation run, every node sends its beacon messages frequently. For the data rate, we select 6 MBit/s which has been shown to be very efficient [15]. On the physical layer, the path loss between transmitter and receiver is determined according to Friis' transmission equation. Though, there exist a number of sophisticated path loss models, we intentionally chose the simple Friis' formula 2.1. We are aware that this model does not model signal propagation realistically as some attenuation aspects are not considered due to simplicity. But this simplicity allows us to show the general problem of transmission range degradation due to interference. The same effects will occur when using more realistic propagation models.

As a result of the parameter and model selection, each vehicle achieves a maximum transmission range of 960 meters which is roughly in line with some experiments presented in [9]. All important parameters are listed in Table 2.

The only environmental noise on the channel is the thermal noise at —104dBm. All other interference contributing to the SINR value is self-induced noise by the network. For every transmission the simulator calculates the SINR at the receivers where the signal is stronger than the thermal noise. As a result, proper reception is possible or not. In case the interference level changes throughout the transmission, each time the SINR is checked again. If it becomes to low, the packet reception is canceled.

In the study, we vary two parameters: message length and the message frequency. For the message length, we cover three values, i.e. 50; 200 and 1000 Byte. Similarly, we vary the message frequency in a range from 2 Hz to 200 Hz.

5.3 Simulation Results

Following, we study the impact of two different channel load scenarios in the first part. We identify each scenario by its *offered load* given to the system. The offered load denotes the total amount of data per second that is offered by all vehicles to the communication channel. Each offered load scenario consists of different parameters for beacon rate and message size.

In the second part, we investigate the difference in packet loss using small packets with 50 Byte and large packets with 1000 Byte at different beacon rates. We compare the two offered load scenarios that we introduce in Section 5.3.1 and highlight the reasons for packet loss. We focus our study on explicit packet loss on the wireless medium. The exposed station effect will not be considered for two reasons: First, it is not clear which strategy for queue management will be applied and rule for message drop will be applied. Second, we carefully choose the offered load so that the channel capacity is not exceeded. As there are no acknowledgments and retransmissions, there will be no additional offered load in the system.

5.3.1 Total Offered Load

The total amount of data to be transmitted to other nodes can not exceed the channel capacity. The channel capacity, in turn, is given by the specified data rate set on the physical layer. For our study, we assume a data rate of 6 MBit/s. This translates to about 750 KByte/s of data that can be transmitted. Clearly, the actual amount of data that can be transmitted will be lower, as the Phy/MAC protocol demands parts of this channel capacity in terms of interframe spaces and additional fields to create the MAC frame, e.g. the preamble and PLCP header.

Table 3 Overview on offered load setups a) and b).

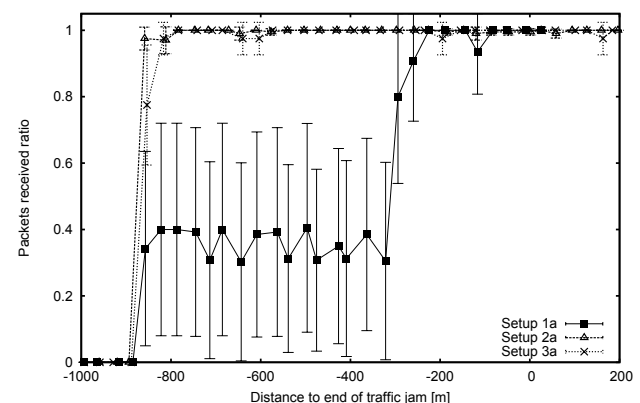| Setup a) — Offered Load 0.2 MByte/sec			
1	40 Hz	100 vehicles	50 Byte
2	10 Hz	100 vehicles	200 Byte
3	2 Hz	100 vehicles	1000 Byte
Setup b) — Offered Load 1 MByte/sec			
1	200 Hz	100 vehicles	50 Byte
2	50 Hz	100 vehicles	200 Byte
3	10 Hz	100 vehicles	1000 Byte

Fig. 4   Packet loss for setups with offered load a)

Note that the mentioned data rate must be shared by all ve- hic- les within carrier sensing range as they share the same channel. The other way round, vehicles that do not hear each other, may occupy the wireless medium simultaneously. This is called spatial reuse of the medium.

In the following experiment, we use two offered load setups which do not exceed the channel capacity, summarized in Table 3. Each offered load will be simulated with varying parameters, i.e. message size and beacon rate. Note that they do not directly represent the channel load. The vehicles' separation as described in Table 2 allows them to simultaneously use the communication medium. So, this offered load is distributed over the whole area but not the load at one particular point.

— a) Lower offered load: 0.2 MByte/sec
— b) Higher offered load: 1 MByte/sec

For this offered load, the protocol overhead should be noted. For small packets, the ratio of this overhead and the payload is quite high. For large packets with 1000 Byte, the packet airtime, i.e. the time where the channel is busy, is still relatively low with about 1:3 milliseconds. So, as we see in Fig. 4, the performance for the same offered load but with lower packet size is degraded (setup 1a). Obviously, the offered load is relatively low but nevertheless there is a high number of beacons per second. As a result, the last upstream vehicle (UV) does not receive all (small) packets from the emergency vehicle (EV) from the theoretic maximum transmission range at about 960 meters at the given beacon rate. This, in turn, is the case for the other two setups (2a and 3a) with medium and high message lengths. Looking at the confidence intervals also reveals the fluctuation of packet loss. For small packets (setup 1a) there is some kind of plateau with large confidence intervals that display a large fluctuation of packet loss in this area. The reason for that is that the average of packets received is influenced by two extreme cases: In some cases, nearly all packets are lost where in some other cases, only few packet loss is experienced. Large size packets (setup 3a) with 1000 Byte show a higher fluctuation only at the very end of the theoretic transmission range. A closer look into the results shows that the classic hidden station situation is mainly responsible here. Before going into deeper analysis of the reasons for the packet loss for small packets, we compare these observations with the high offered load scenario.
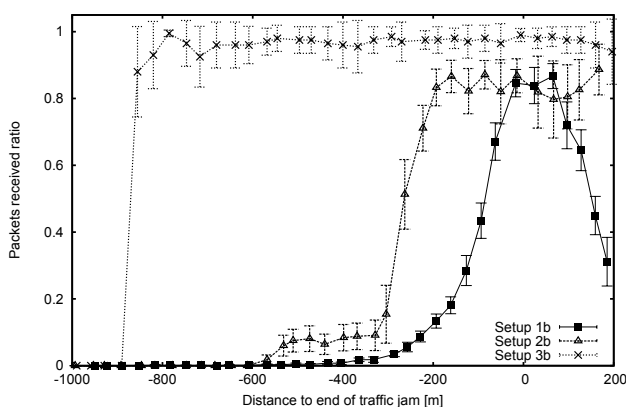

Fig. 5   Packet loss for setups with offered load b).

In Fig. 5, the packet loss for small packets (setup 1b) deteriorates with a remarkable degradation of the reliable transmission

range down to 100 meters. As mentioned before, this tendency was expected as this setup comes close to the channel capacity. The mentioned protocol overhead and channel access delays, interframe-spaces, contribute to an increased channel utilization. This difference to larger packets is supported by the results for medium and high message lengths. The degradation of transmission range for medium size packets (setup 2b) is in the order of 250 meters which means that the it is reduced to a quarter. For large packets (setup 3b) it seems that there is still no influence. Note for setup 1b the degradation is symmetric as the EV passes the UV at $x = 0$. So, the reliable transmission range degrades again at 100 meters after the UV has been passed.

Next, we go into detail with extreme situations for small and large packets where we investigate the impact of the beacon rate further.

5.3.2 Large packet size

From the observations presented in the last subsection, there was no significant packet loss found for large packets. Now, we increase the offered load per vehicle in terms of the beacon rate. Starting at the beacon rate of 15 beacons per second, we had no significant impact on the packet loss. When increasing the rate further, i.e. from 15 to 18 Hz, suddenly the packet loss increased. Fig. 6 depicts this situation.

For 15 beacons per second, the packet loss in far distances slightly increases as well as its fluctuation. Now, for 18 beacons per second, the performance strongly drops. A similar drop is observed for 20 beacons per second. The reliable transmission range decrease to about 300 meters. It finally deteriorates, for 40 beacons per second, to a value of 150 meters. Again, this sudden drop and successive behavior is remarkable.

Before drawing conclusions of these observations, we need to discuss also the same effect for small packets.

5.3.3 Small packet size

In Fig. 7, the situation for small packets is shown. In contrast to large packets, the mentioned sudden performance drop occurs in a different way. As the figure displays, the packet loss in far distances strongly occurs whereas the area of no loss remains quite stable. Starting from 19 up to 40 beacons per second, we also see a sort of plateau where the average packet loss fluctuates. This behavior is different to large packets where a linear but stable packet loss was observed. However, when further increasing the beacon rate to 100 or even 200, the situation converges similarly as for large packets, with a reliable transmission range of 100 meters or 50 meters. It is also worth noting that for these extreme setups, a high reliability of 90 % is never reached. As for a brief conclusion for small packets, it seems that there are three areas with respect to the offered load: First, a stable area, with up to 15 beacons per second. Second, a transient area from 20 to 40 beacons per second with highly varying packet error rates at far-distances. And third, the transmission range becomes more stable but strongly degraded, starting from about 50 beacons per second.
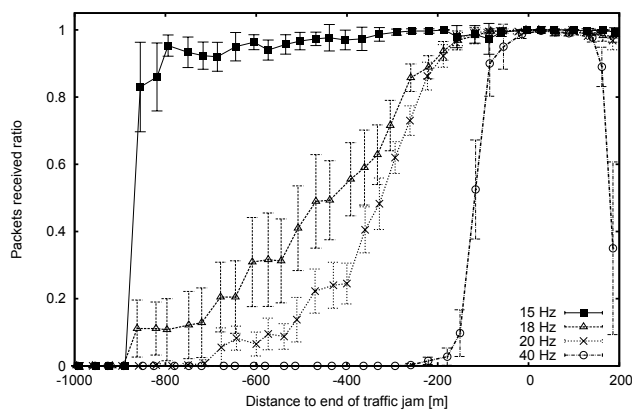
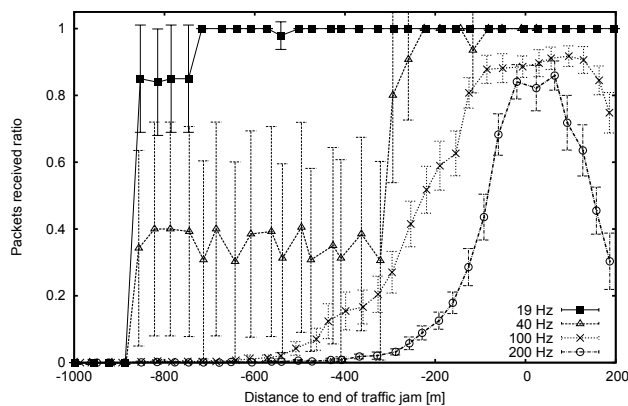*Fig. 6   Packet loss for large packets, i.e. 1000 Bytes.*

Fig. 7   Packet loss for small packets, i.e. 50 Bytes.

5.4 Discussion

The simulations have shown that the total offered load as the sum of all messages from all vehicles within an area is not the only important parameter for packet loss. Most severe is the impact of the beacon rate, especially beacon rates above 20 Hz in our experiments.

Via the simulations, we found that at some point when increasing the load, there is a sudden increase of packet loss and hence a significant decrease of the reliable transmission range. We suspect that at these transitions, some sort of chain-reaction occurs where the interference influences the clear channel assessment. That is, even though the preamble and PLCP are modulated with the more robust BPSK scheme and hence needs a lower SINR, vehicles become more and more unable to decode that the carrier is busy. The carrier sensing range hence may also strongly decrease.

Packet loss due to interference of other vehicles is the most dominating factor. This cause basically comprehends two of our identified packet loss reasons in Section 4: The Fully Interfered Receiver and the Classic Hidden Station. This means, mostly the SINR at the receiver is already too low as the existing interference prevents sensing the packet, i.e. decoding the preamble and PLCP header. The second cause with the same severity is the Hidden Station effect. The UV is able to start receiving the packet from the EV but does not finish as the SINR falls below the minimum threshold which results in packet loss.

We observed that due to simultaneous sending the mentioned reliable inner core of the transmission range is slightly degraded. This effect becomes significant especially in very high load situations where the beacon frequency is very high (e.g. 40 Hz). In contrast to the Hidden Station effect, the number of packet collisions due to this effect remains nearly constant as the EV approaches the UV. Similarly, we expect that the interference from adjacent channels affects this inner core, too. Nearby vehicles transmitting on an adjacent channel lead to packet loss or at least to an increase of the SINR at the receiver.

Concluding, the transmission range can be significantly degraded in high-load scenarios, especially at high distances between transmitter and receiver. Packets from far away vehicles are received with a high packet error rate as the received signal is relatively low compared to the existing interference at the receiver. At closer distances, only low packet loss occurs. The SINR is relatively high as the path loss for the focused signal is low. In our scenario, this means that the EV will not be heard at the end of a traffic jam if it is far away (but within theoretical transmission range). As it approaches the traffic jam, the probability increases that it will be heard even when there is a high interference level from transmissions within the traffic jam. The total reduction of the transmission range depends on the communication scenario and can be as high as 90 %. In the experiment, this was a reduction from 960 meters to something around 100 meters. Such a strong degradation of a potential warning lead-time may limit the benefit of this application. The vehicle driver would not be able to react appropriately.

6 RELATED WORK

Packet loss in VANETs has been analyzed from different perspectives and with different scenarios. Jiang et al. [14] showed the reduction of transmission range in scenarios with homogeneous and non-homogeneous vehicle densities. Vehicles are traveling along a circular road with 8 lanes. In nonhomogeneous scenarios, vehicles belong to groups with different densities and transmission ranges. Based on these results, they identify the optimal data rate for inter-vehicle communication in [15]. We have applied the resulting data rate to our study of a VANET-specific scenario. In their study on the average packet reception rate depending on the distance between transmitter and receiver they show a similar trend as in our study. The packet error rate in some distances increases linearly with a high gradient. Like in our results, this is the case at distances of half of the original transmission range. Unfortunately, the fluctuation by means of confidence intervals is not shown and discussed which we found for small packets. The packet size was also always fixed to 200 Byte. Chen et al. [6] also evaluated the reduction of transmission range in an experiment with three homogeneous VANET setups. The high-load scenario with 1000 vehicles presents also a strong decrease of the reliable transmission range. However, the lower density setup with 133 vehicles shows a different increase of packet loss with respect to the distance of transmitter and receiver, compared to our study. But, the reduction of the reliable transmission range is also in a high percentage, roughly 70 %. Also, the fluctuation is not shown. We assume that it is quite low as the vehicle setup is homogeneous and hence the average packet loss is, too. Similarly to [15], they also assumed a maximum transmission range of 250 meters. In the results of their experiment, they haven't discussed the different reasons for packet loss in a quantitative way.

This is done conceptually, in order to overhaul the physical layer model of their network simulator. In line with our discussion, they also distinguish between selfcaused packet loss by starting a transmission regardless of the receive state, and packet loss by external causes, e.g. a receive signal that is too weak or a noise level that is too high. Furthermore, Chen et al. point out the relation between the SINR and the Bit-Error-Rate. They describe that with decreasing SINR not all packets are lost but the probability of packet errors increases. Even with a very low SINR a receiver might be able to decode a packet due to error correction redundancy and advanced receive filters. Preliminary to our simulation study, we also briefly investigated different SINR levels for reception. We decided to fix the SINR threshold for reception as variation causes only slight changes in the results. The general trend of transmission range degradation remains the same.

Schmidt-Eisenlohr et al. [18] evaluated the transmission range and the influence of different offered loads produced by the periodic beaconing in highway scenarios with varying traffic densities. They show how the average packet reception, channel busy time and channel access time behave in dependence of distance between sender and receiver for different packet generation rates. They confirm that the communication range is significantly reduced in all high message load scenarios. Briefly summarized, the beacon rate for all 802 simulated vehicles was in the range of 2 to 14 packets per second, each having 500 Bytes, and the theoretic transmission ranges from 100 to 1000 meters. An interesting conclusion of their experiment is that "a higher number of received packets is achieved while increasing the packet generation rate." It is noted that this however may not be a solution as the offered load is increased. As we also see in our specific experiment, the beacon rate should be kept as low as possible in particular situations.

Schmidt-Eisenlohr et al. are also in line with Ware et al. [19] that the packet capture feature allows receivers to recover a fair amount of colliding packets if there is a stronger signal which can be decoded potentially. The reliable transmission range converges to an "inner core", a much smaller part of the original transmission range. As we found out, this inner core is already present without capturing functionality. However, it does not cope with simultaneous sending where the delay between two approaching transmissions is within microseconds. We assume that within such a short period, i.e. where the training sequence is sent, capturing is not possible. Also, it does not prevent interference from nearby vehicles on adjacent channels.

Eichler [7] has evaluated the prioritization mechanism (Hybrid Coordination Function, HCF) that is adapted in IEEE P802.11p. He also studied dense high-load scenarios. The focus here is to show the performance of the four access categories and hence the performance of message prioritization. In addition packet collisions are briefly studied. He mainly focuses on collisions due to simultaneous sending, depending on access category and number of vehicles. According to his considerations, the total collision probability for 19 vehicles with a contention window of 15 slots is around 50 %. Compared to our study, the probability of collision between two arbitrary vehicles is analyzed but not for particular vehicles. Also, it should be noted that a channel switching scheme is applied according to the IEEE 1609.2 protocol which limits the comparability of results.

7 CONCLUSIONS AND FUTURE WORK

Inter-vehicle communication must be reliable to ensure a benefit for passengers' safety. In this paper, we analyzed the current state-of-the-art MAC protocol draft IEEE P802.11p which will be used in VANETs. We studied the reasons for 8 packet loss and identified multiple causes belonging to both protocol and signal propagation issues. By an analytical discussion we pointed out the most severe ones. Afterwards, in a simulation study we have conducted a quantitative analysis and evaluated the problem in dependence of particular parameters, i.e. beacon rate and packet size. The design of the scenario that we use in the simulation was guided by a concrete application background: An emergency vehicle that approaches a traffic jam. Our special interest in the study is on the communication between the emergency vehicle, e.g. an emergency vehicle and the vehicles at the upstream of the traffic jam, i.e. the vehicles with which the emergency vehicle gets in contact first.

Interference of other vehicles has been found to be the main reason for packet loss in our study. In situations where there is a high message load the reliable transmission range is reduced by up to 90 %. We have also shown that the transition between stable communication to high packet loss occurs at particular slight increases of the offered load. The significance of this problem is obvious: A reduction of transmission range, especially from an emergency vehicle results in a degradation of application performance. The lead time for a warning to driver is strongly reduced and hence is the benefit of such an application.

Our future work will comprise a deeper analysis of the transition between stable and unstable communication. We will therefor also consider other scenarios on the one hand. On the other hand, we will look at heterogeneous communication setting, e.g. multi-hop, multi-channel communication with different transceiver characteristics. In general, a better understanding of the parameters is needed to understand the situations where the channel conditions suddenly result in high packet error rates.

8 ACKNOWLEDGMENTS

REFERENCES

[1]   Car to Car Communication Consortium Manifesto —Overview of the C2C-CC System. Technical report, C2C-CC, Aug. 2007.

[2]   A. Banchs and L. Vollero: Throughput analysis and optimal configuration of 802.11e edca. IEEE Computer Networks, 50 (11): 1749-1768, 2006.

[3]   R. Barr: Java in Simulation Time (JiST), Mar. 2004.

[4]   R. Barr: Scalable Wireless Ad-hoc Network Simulator (SWANS), Mar. 2004.

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

[6]   Q. Chen; F. Schmidt-Eisenlohr; D. Jiang; M. Torrent-Moreno; L. Delgrossi; and H. Hartenstein: Overhaul of ieee 802.11 modeling and simulation in ns-2. In: MSWiM '07: Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems, pages 159-168, New York, NY, USA, 2007. ACM.

[7] S. Eichler: Performance evaluation of the ieee 802.11p wave communication standard. In: 1st IEEE International Symposium on Wireless Vehicular Communications (WiVeC), Baltimore, USA, September 2007.

[8] H.T. Friis: A note on a simple transmission formula. Proceedings of the IRE, 34 (5): 254-256, 1946.

[9] B. Gallagher; H. Akalsuka; and H. Suzuki: Wireless communications for vehicle safety: Radio link performance and wireless connectivity methods. IEEE Vehicular Technology Magazine, 1 (4): 4-24, 2006.

[10] L.C. Godara: Handbook of Antennas in Wireless Communications. CRC Press, Inc., Boca Raton, FL, USA, 2001.

[11] Institute of Electrical and Electronics Engineers: IEEE Std 802.11e, November 2005.

[12] Institute of Electrical and Electronics Engineers: IEEE Std 802.11-2007, June 2007.

[13] Institute of Electrical and Electronics Engineers: IEEE P802.11p/ D5.0, September 2008. Draft 5.0.

[14] D. Jiang; Q. Chen; and L. Delgrossi: Communication density: A channel load metric for vehicular communications research. IEEE Conference on Mobile Adhoc and Sensor Systems, 2007. MASS 2007, pages 1-8, Oct. 2007.

[15] D. Jiang; Q. Chen; and L. Delgrossi: Optimal data rate selection for vehicle safety communications. In: VANET '08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, pages 30-38, New York, NY, USA, 2008. ACM.

[16] S. Moser; F. Kargl; and A. Keller: Interactive Realistic Simulation of Wireless Networks. In: IEEE/EG Symposium on Interactive Ray Tracing (RT '07), Ulm, Germany, Sept. 2007. IEEE, IEEE.

[17] T.S. Rappaport: Wireless Communications: Principles and Practice (2nd Edition). Prentice Hall PTR, December 2001.

[18] F. Schmidt-Eisenlohr; M. Torrent-Moreno; J. Mittag; and H. Hartenstein: Simulation platform for inter-vehicle communications and analysis of periodic information exchange. In: Proceedings of the 4th Annual IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS), Jan. 2007.

[19] C. Ware; J. Chicharo; and T. Wysocki: Simulation of capture behaviour in ieee 802.11 radio modems. In: IEEE Vehicular Technical Conference (VTC) Fall, volume 3, pages 1393-1397, September 2001.

[20] Y. Zhang; I.L. Tan; C. Chun; K. Laberteaux; and A. Bahai: A differential ofdm approach to coherence time mitigation in dsrc. In: VANET '08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, pages 1-6, New York, NY, USA, 2008. ACM.