How Severe is the Hidden Terminal Problem in VANETs when Using CSMA and STDMA?

Katrin Sjöberg [†,§], Elisabeth Uhlemann[†], and Erik G. Ström[§,†]

[†]Centre for Research on Embedded Systems
Halmstad University
Box 823, SE-301 18 Halmstad, Sweden

[§]Department of Signals and Systems
Chalmers University of Technology
SE-412 96 Göteborg, Sweden

Email: Katrin.Sjoberg@hh.se, Elisabeth.Uhlemann@hh.se and Erik.Strom@chalmers.se

Abstract – **The hidden terminal problem is often said to be the major limiting performance factor in vehicular *ad hoc* networks. In this article we propose a definition of the hidden terminal problem suitable for broadcast transmissions and proceed with a case study to find how the packet reception probability is affected by the presence of hidden terminals. Two different medium access control methods; carrier sense multiple access (CSMA) from IEEE 802.11p and self-organizing time division multiple access (STDMA), are subject of investigation through computer simulations of a highway scenario with a Nakagami fading channel model. The results reveal that the presence of hidden terminals does not significantly affect the performance of the two MAC protocols. STDMA shows a higher packet reception probability for all settings due to the synchronized packet transmissions.**

I. Introduction

The first generation of road traffic safety systems based on short-range wireless communications will deploy IEEE 802.11p [1]. One major difference between IEEE 802.11p and the legacy 802.11[2] is the removal of the access point (AP) functionality in the former, implying that there is only support for *ad hoc* networking and all nodes are peers. IEEE 802.11 is using carrier sense multiple access (CSMA) as its medium access control (MAC) method, where all nodes perform a carrier sensing operation before initiating transmissions, and if the channel is sensed busy during the carrier sensing operation, the node must perform a backoff procedure and defer its transmission. In a network containing APs, this kind of MAC method gives rise to the well-known hidden terminal problem. The problem occurs because a node may sense that the channel is free even though another node which is out of radio range (but associated to the same AP) has an ongoing transmission. This in turn leads to overlapping or partially overlapping transmissions. With CSMA, overlapping transmissions can also occur if two nodes within radio range start sensing the channel simultaneously or select the same random backoff value. When an AP is present, all data traffic must traverse the AP, implying that unicast transmissions are made between individual nodes and the AP and all nodes must contend for access. To combat the hidden terminal problem in AP based networks request-to-send (RTS) and clear-to-send (CTS) packets can be used. The RTS is transmitted by the sending node preceding its transmission of a longer data packet, and if the AP responds with CTS, overlapping transmissions are avoided as all other nodes will be notified about the upcoming transmission even if they are hidden from the sending node.

In vehicular *ad hoc* networks (VANET) the hidden terminal problem is not as straight forward to define. The applications that are proposed for VANETs using 802.11p technology are mostly based on broadcast communication, i.e., one transmitter and many receivers. All vehicles in the network will regularly (1-10 Hz) broadcast position messages (also called beacons) containing the speed, heading and position of the vehicle. These messages will be the foundation for a range of road traffic safety applications. The goal of the broadcasting node in this context is to reach as many of the vehicles in its vicinity as possible. However, the sending node does not actually know if its transmissions are successful since acknowledgments (ACK) cannot be used in broadcast situations. In unicast transmissions, a sending node awaits an ACK in response and if that is missing, the sending node knows reception has failed and it may for example retransmit the packet. With applications based on unicast, the hidden node situation can be more severe since there is only one specific receiver for each transmission and several transmitters potentially contend for the same receiver. In a broadcast situation there are typically many receivers of which the majority could still receive the packet even though there is a hidden terminal situation. This complicates not only the definition of the hidden terminal problem but also the ability to mitigate the effects of the problem. In this paper we investigate the impact of hidden terminal transmissions in a VANET where all nodes solely use broadcast communication. The packet reception probability is used for measuring and capturing the impact of hidden terminal transmissions on the overall performance. The study is conducted using computer simulation of a multi-lane highway scenario with a Nakagami channel model. CSMA of 802.11p is compared to another MAC method proposed for VANETs: self-organizing time division multiple access (STDMA).

II. Hidden Terminal Problem

In Figure 1, transmitter TX1 and transmitter TX2 are out of radio range of each other, i.e., they are hidden to one another. Therefore they may access the medium at the same time, making the receivers RX1-RX3 experience a data collision, i.e.,

This work was funded in part by the Knowledge Foundation, www.kks.se. E. Uhlemann is partly funded by the Swedish Governmental Agency for Innovation Systems, Vinnova, through the VINNMER program, www.vinnova.se.

being unable to decode any of the two packets. This phenomenon is termed the *hidden terminal* problem and in wireless *ad hoc* networks, it can occur regardless of MAC method.

Pioneering work on CSMA and the hidden terminal problem was made by Kleinrock and Tobagi in their two well-known articles from 1975 [3, 4], where Part I is about CSMA in general and Part II analyzes the performance degradation that the hidden terminals introduce in a network containing many transmitters and one receiver. In 2000, Bianchi presented an analytical model of CSMA as deployed in an infrastructure-based IEEE 802.11 network [5], which has served as the basis for much research since then. In [6, 7] Bianchi's work was extended to account for hidden terminals in networks containing AP and mesh networks, respectively, i.e., implying unicast investigations. The unicast transmission case containing hidden terminals is thus quite well investigated in contrast to the broadcast environment. Several research articles considering performance evaluation of VANETs are mentioning the hidden terminal problem and states that it is a problem but they fail to show to what extent the problem impacts performance in broadcast situations. In [8] the authors investigate the impact of different deterministic and statistical channel models on the performance of VANETs where vehicles use 802.11p. They mention the hidden terminal problem, but they do not state or evaluate how severe the problem is. One major problem with determining the effects of the hidden terminal problem in VANETs is that there is no common definition for the problem when a broadcast *ad hoc* network is considered. Moreover signals undergo fading in a real system and therefore it is hard to define "communication range" and when two nodes are "out of radio range". Using an application perspective, which is relevant for road traffic safety applications, we propose a definition of hidden terminals in VANETs.

Definition 1

Consider a transmission of a particular packet p from node k, and let $\mathcal{R}_k$ denote the set of intended receivers of p. Let node $l \in \mathcal{R}_k$. A node n is said to be a *hidden node with respect to the transmission of packet p from node k and the receiver node l* if the following four conditions are satisfied:

(i) k is transmitting packet p

(ii) n is transmitting a packet during the time p is transmitted

(iii) l is an intended receiver of n and k, i.e., $l \in \mathcal{R}_k \cap \mathcal{R}_n$

(iv) n is not an intended receiver of k, i.e., $n \notin \mathcal{R}_k$

We note that the set of intended receivers, $\mathcal{R}_k$, is essentially determined by the (road traffic safety) application. We can define a communication range which is associated with $\mathcal{R}_k$ as the smallest radius R_c around node k that encloses all intended receivers. Hence, the communication range R_c is also requirement from the application and is not necessarily connected to the ability to decode packets, as this would be unreasonable for real radio channels. Hence, nodes outside a circle of radius R_c centered around node k are not necessarily unable to decode a transmission from node k or, vice versa, nodes inside the circle are not necessarily able to decode the message. Furthermore, we note that all nodes inside R_c are not necessarily intended receiver. In other words, the definitions above allow for non-circular regions of interest since a road traffic safety transmission might, e.g., be intended only for receivers behind the transmitter. However, for simplicity, we assume in the following that all transmissions from all nodes have the same intended communication range and circular regions of interest, i.e.,

$$\mathcal{R}_k = \{ i : \|\mathbf{x}_i - \mathbf{x}_k\| \le R_c \},$$

where $\mathbf{x}_i$ and $\mathbf{x}_k$ are the positions of nodes i and k respectively. The above definition of hidden terminals is inspired by research work conducted for the unicast case with the difference that we now consider a set of receivers instead of one single receiver. This definition of hidden terminals in a VANET is used when analyzing the results in the case study below.

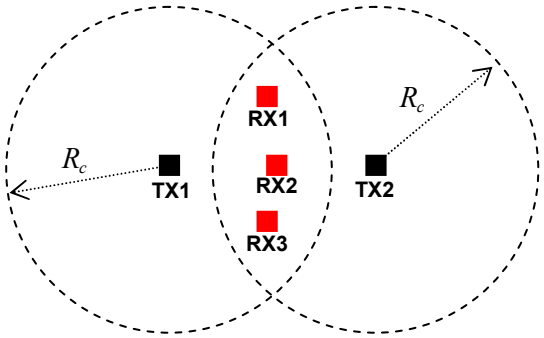

Figure 1. The hidden terminal problem

III. Medium Access Control

Providing access to the shared medium while at the same time providing the Quality of Service (QoS) in terms of, e.g., delay and reliability, requested by the application, is an important and challenging task of the MAC layer. Although, the reliability is mostly addressed in the physical layer, the MAC protocol can minimize simultaneous channel access attempts in an effort to decrease the interference and thereby increase reliability. The broadcast nature of messages in VANETs excludes traditional automatic repeat request (ARQ) strategies at the link layer found in unicast communication, which implies that important messages have to rely on e.g., repeated broadcasts of the same message in an effort to increase reliability.

In this article we compare how two different MAC protocols cope with the hidden terminal problem: the CSMA protocol as specified in 802.11p and the time-slotted STDMA protocol which is also proposed for the vehicular environment. Time-slotted MAC approaches such as STDMA requires synchronization and one packet fits into one slot, i.e., fixed packet lengths. CSMA does not require synchronization and supports variable packet lengths. Below is a brief description of the

channel access procedure of CSMA and STDMA. For further protocol details see [1, 2] for CSMA and [9, 10] for STDMA.

In CSMA of 802.11p, each node initiates a transmission by listening to the channel, i.e., performs a carrier sense operation, during a predetermined listening/sensing period called the arbitration interframe space (AIFS), T_{AIFS}. If the sensing is successful, i.e., no channel activity is detected, the node transmits directly. If the channel is occupied or becomes occupied during the T_{AIFS}, the node must perform a backoff procedure, i.e., it has to defer its access for a randomized time period. Nodes are only allowed to decrement their backoff values while the channel is free. Therefore, they must defer their backoff decrementation whenever the channel is busy and they must listen a T_{AIFS} after a busy channel becomes free, before decrementation of the backoff value can resume. When a backoff value of 0 is reached, the node transmits directly.

In STDMA the time is divided into time slots constituting a frame. The frame is seen as a ring buffer and all nodes have their own frame start. Hence, the nodes are slot synchronized, but not frame synchronized. The synchronization is done through GPS. The major difference between STDMA and other self-organizing TDMA schemes is the lack of a random access channel for slot assignment. Instead, STDMA uses the information contained in broadcasted position messages, which for VANETs are already present in the system. Nodes in STDMA listen to the channel during one frame and then select a number of free slots for transmission. If all slots are occupied; the node will choose the same slot as another node located furthest away from itself, based on its knowledge of positions. This way channel access is always granted regardless of the number of nodes within communication range and the distance between two concurrently transmitting nodes is maximized. To cater for network topology changes, the same slot assignment is not kept for long. When a new slot has been selected the node will also attach a random integer, $a = \{3,...,8\}$, to it, which determines for how many frames this particular slot will be used. This random number is different for each assigned slot in the frame. When a specific slot has been used its predetermined number of frames, the node must find a new slot and attach a new random number to it.

IV. Case Study: Hidden Terminals

The hidden terminal problem in VANETs is evaluated through computer simulations of a highway scenario with 10 lanes (five in each direction). The vehicles appear Poisson distributed with two different inter-vehicle arrival rates, depending on the investigated vehicle density. Every vehicle broadcasts position messages periodically, and the start of the period for each vehicle is independent and randomly selected. The vehicle speeds are independently Gaussian distributed with a standard deviation of 1 m/s, but with different mean values (23 m/s, 30 m/s and 37 m/s) depending on lane. The vehicles maintain the same speed as long as they are on the highway.

Two types of simulations have been conducted: the vehicles use either STDMA or CSMA as channel access method. Two different packet lengths, B, and update frequencies, f_p, are used, Table 1. The two data traffic settings are selected based on discussions in Europe within ETSI and in the US within IEEE, respectively. The messages are transmitted using the highest priority in CSMA, implying a T_{AIFS} of 58 μs and the CW set to 3. The bandwidth requirements for each node based on the data traffic settings and the number of slots in the STDMA frame for each model are also found in Table 1. The frame size in STDMA is 1 second. Both MAC methods use the same physical layer of 802.11p, i.e., orthogonal frequency division multiplexing (OFDM). The chosen transfer rate for the vehicles' position messages is R = 6 Mbps (QPSK, r =1/2).

Table 1. Data traffic settings.

	B [byte]	f_p [Hz]	Bandwidth req. [kbps]	No of slots/ frame
Data traffic model Europe	800	2	12.8	904
Data traffic model USA	300	10	24	2283

The channel model in the simulator is based on an outdoor channel sounding measurement campaign performed at 5.9 GHz, measuring communications between vehicles [11]. The collected data has served as a foundation to find a suitable statistical model and its parameter setting. The small-scale and the large-scale fading are both represented by the Nakagami m model [12], which has been pointed out earlier to be a suitable candidate for vehicular channel modeling [13]. The fading intensities, represented by the m parameter of the Nakagami distribution, are different depending on the distance between transmitter and receiver [11]. The average received power, P_r, is assumed to follow a dual-slope model as suggested in [11]. All numerical values of the channel model are found in [11] and data set 2 has been used. Simulations have been conducted with an output power, $P_{t,dB}$, of 20 dBm (100 mW). The carrier sense threshold for CSMA is −96 dBm [14]. The resulting signal-to-interference-plus-noise (SINR) ratio at the receiver is calculated using the following formula:

$$SINR = \frac{P_r}{P_n + \sum_k P_{i,k}}, \quad (1)$$

where P_r is the power of the desired signal, $P_{i,k}$ is the received power from the k-th interferer, and P_n is the noise power set to −99 dBm. We assume that the application sets the intended communication range, R_c, to 400 m. The transmit power level is adjusted to support this in the following sense: a transmission affected by path loss only and no fading or interference, will reach at most 400 m. However, as fading is also present, a packet can be decoded successfully beyond R_c as well as unsuccessfully within R_c. We assume that the physical layer requires a $SINR_{dB} > 6$ dB to successfully decode a packet. In CSMA, $SINR_{dB}$ can vary during the packet due to overlapping transmissions and consequently the $SINR_{dB}$ at the end of the packet is used to determine if a packet is successfully decoded.

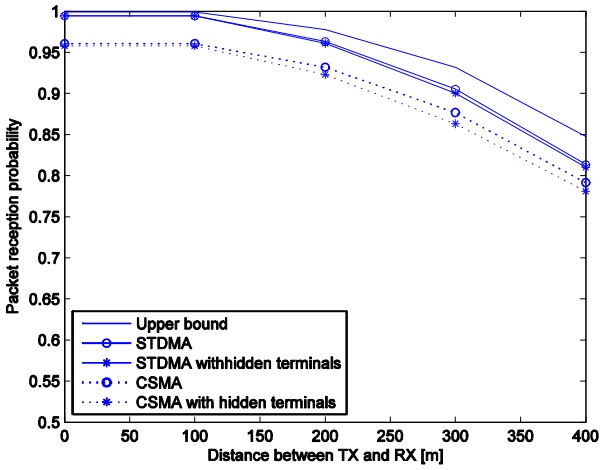

Figure 2. Packet reception probability for 2 Hz and 800 bytes with $P_{t,dB}$ =20 dBm and vehicle density 10 vehicles/lane/km.

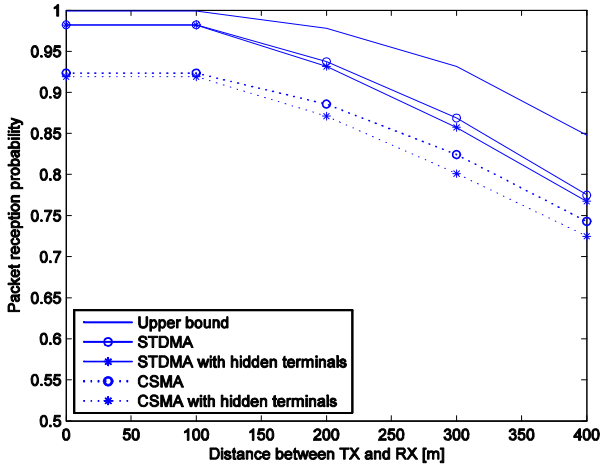

Figure 3. Packet reception probability for 2 Hz and 800 bytes with $P_{t,dB}$ =20 dBm with vehicle density 20 vehicles/lane/km.

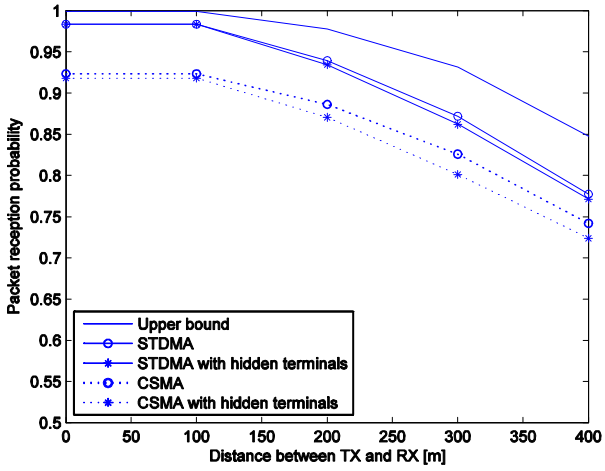

Figure 4. Packet reception probability for 10 Hz and 300 bytes with $P_{t,dB}$ =20 dBm and vehicle density 10 vehicles/lane/km.

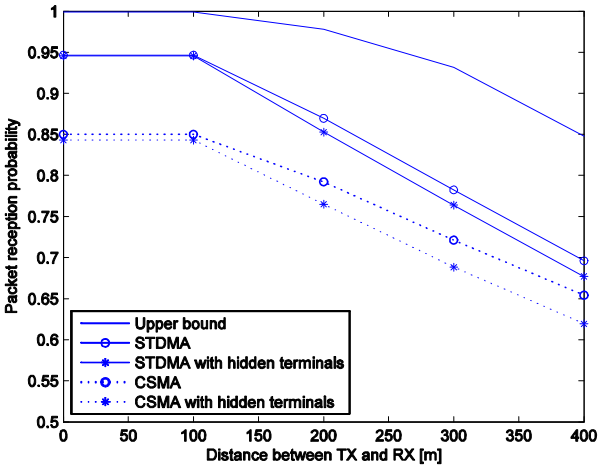

Figure 5. Packet reception probability for 10 Hz and 300 bytes with $P_{t,dB}$ =20 dBm and vehicle density 20 vehicles/lane/km.

In Fig. 2-5 the packet reception probability averaged over all RXs within a certain maximum distance from a TX is depicted. In Fig. 2-3, the vehicles broadcast with an f_p of 2 Hz and packet length of 800 bytes and in Fig. 4-5 with 10 Hz and 300 bytes. In Fig. 2 and 4, a vehicle density of 10 vehicles/lane/km has been used and in Fig. 3 and 5, a vehicle density of 20 vehicles/lane/km is depicted. The upper bound shows the packet reception probability for a system with no interference, i.e., no other transmissions are ongoing at any place in the network. This is the best performance that can be achieved with the chosen channel model and therefore, this is called upper bound in the figures. There are two graphs for each MAC method, one containing all transmissions, including those from the hidden terminal transmissions as defined earlier, and one without the hidden terminals. This implies that for the latter case, with an R_c of 400 meters, all simultaneous transmissions performed by terminals located between 400-800 meters apart *are not included*, i.e., hidden terminal transmissions are removed. If the two TXs are more than 800 meter apart, the set of common receivers is empty and if they are less than 400 meters apart, they are within the intended communication range and consequently not hidden.

The superior performance for STDMA compared to CSMA for all settings is partly due to that STDMA schedules transmissions in space to minimize interference and partly due to the synchronization mechanism used by STDMA. Since STDMA also broadcasts its future intended slot use, this information can be used to determine that a slot is occupied, even if fading makes it appear to be free. Further, transmissions in CSMA are unsynchronized, resulting in many transmissions that partially overlap in time when nodes are hidden, whereas in STDMA transmissions are either fully overlapping or not at all, implying that fewer transmissions are affected. The synchronization consequently contributes to a better protection against interference in general, including the hidden terminal transmissions. In a fading environment all nodes are potential interferers, but, as can be seen in the figures, the interferers we classify to be hidden terminals are only responsible for a minor part of the performance degradation. Hence, it is the other interferers that contribute the most of the interference level in the system. Therefore, it is important to decrease the overall interference level in the system especially in the

CSMA case since the synchronization between nodes is lacking. The decrease of the interference level could be achieved through power and/or congestion control methods as suggested in [15]. We have also run simulations with a lower output power for different vehicle densities and the hidden terminal problem is still present even though the output power is reduced. The only difference is that fewer RX are reached and the fading becomes a more dominant part of the performance degradation. However, since VANETs are supposed to support road safety applications there is of course a tradeoff between the number of nodes in range and how far the generated data should propagate. Depending on the situation and road traffic safety application in question an intended communication range of 400 meters is not at all an impossible requirement. Then an output power of 20 dBm would be needed in order to reach nodes at 400 m with a certain packet reception probability. As seen from our simulations with lower output power the packet reception probability drops drastically after a couple of hundred meters due to the low power.

V. Conclusions

The hidden terminal problem is often said to be the major limiting performance factor in vehicular *ad hoc* networks without any firm support for that statement or any strict definition of what constitutes a hidden terminal in a broadcast scenario. In this paper, we have made a formal definition of the hidden terminal problem for broadcasting in *ad hoc* networks. We have compared the impact of hidden terminals on two different MAC protocols suggested for use in VANETs. The performance measure of our evaluations of a highway scenario is the packet reception probability with and without the presence of hidden terminal transmissions. An upper bound on the packet reception probability where only one transmitter is sending at a time served as a benchmark. We can conclude that the hidden terminal problem is not a major limiting factor for VANETs using any of the considered MAC protocols. Further, we have found that STDMA performs better than CSMA regardless of the presence of hidden terminals. In the simulator setting with 800 byte packets transmitted with an update rate of 2 Hz; STDMA performs close to the upper bound for receivers located close to the transmitter. CSMA experience partially overlapping transmissions from hidden terminals and other interferers due to the lack of synchronization. The synchronization consequently contributes to a better protection against interference in general – including the hidden terminal transmissions. From our results and findings on the hidden terminal problem, we can conclude that the interference generated by transmitters that are not hidden accounts for most of the performance degradation. The impact of these interferers could be reduced with, e.g., power control methods, but the balancing act between output power and number of intended receivers is difficult.

References

[1] IEEE 802.11p *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 7: Wireless Access in Vehicular Environment*, July 2010.

[2] IEEE 802.11 *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007.

[3] L. Kleinrock, and F. Tobagi, "Packet switching in radio channels: Part I - carrier sense multiple access modes and their throughput characteristics," *IEEE Trans. Communications,* vol. 23, no. 12, pp. 1400-1416, Dec. 1975.

[4] F. Tobagi, and L. Kleinrock, "Packet switching in radio channels: Part II - the hidden terminal problem in carrier sense multiple access and the busy tone solution," *IEEE Trans. Communications,* vol. 23, no. 12, pp. 1417-1433, Dec. 1975.

[5] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Selected Areas in Communications,* vol. 18, no. 3, pp. 535-547, Mar. 2000.

[6] A. Tsertou, and D. I. Laurenson, "Insights into the hidden node problem," in Proc. *Conf. Wireless Communications and Mobile Computing*, Vancouver, Canada, Jul. 2006, pp. 767-772.

[7] O. Ekici, and A. Yongacglu, "IEEE 802.11a throughput performance with hidden nodes," *IEEE Communications Letters,* vol. 12, no. 6, pp. 465-467, Jun. 2008.

[8] M. Torrent-Moreno, S. Corroy, F. Schmidt-Eisenlohr, and H. Hartenstein, "IEEE 802.11-based one-hop broadcast communications: understanding transmission success and failure under different radio propagation environments," in Proc. *9th ACM Int. Symp. on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM06)*, Malaga, Spain, Oct. 2006, pp. 68-77.

[9] Recommendations ITU-R M.1371-1, *Technical characteristics for universal shipborne automatic identification system using timed division multiple access in the VHF maritime mobile band*, Apr. 2001.

[10] K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, "On the ability of the 802.11p MAC method and STDMA to support real-time vehicle-to-vehicle communications," *EURASIP J. Wireless Communications and Networking,* vol. 2009, Article ID 902414, 2009.

[11] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band," *IEEE J. Selected Areas in Communications,* vol. 25, no. 8, pp. 1501-1516, Oct. 2007.

[12] M. Nakagami, *The m-distribution, a general formula of intensity distribution of the rapid fading*, Oxford, England, Pergamon, 1960.

[13] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta, "Empirical determination of channel characteristics for DSRC vehicle-to-vehicle communication," in Proc. *ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, Philadelphia, PA, USA, Oct. 2004, pp. 88-88.

[14] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: fair transmit power control for safety-critical information," *IEEE Trans. Vehicular Technology,* vol. 58, no. 7, pp. 3684-3703, Sep. 2009.

[15] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: fair transmit power control for safety-critical Information," *IEEE Trans. Vehicular Technology,* vol. 25, no. 8, pp. 3684-3703, Oct. 2009.