MEDIUM ACCESS CONTROL IN VEHICULAR NETWORKS BASED ON THE UPCOMING IEEE 802.11P STANDARD

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

[†]Centre for Research on Embedded Systems, Halmstad University, Sweden
[§] Department of Signals and Systems, Chalmers University of Technology, Sweden
[‡]Volvo Technology Corporation, Transport, Information and Communication, Sweden

{katrin.bilstrup, elisabeth.uhlemann}@hh.se, erik.strom@chalmers.se

ABSTRACT

In this paper, initial simulations are presented showing that the upcoming IEEE 802.11p standard is not suitable for traffic safety applications requiring reliable, low-delay communication between vehicles. The medium access control procedure is one of the most important parts in the design of delay-constrained communication systems, and emerging vehicle safety applications put new stringent demands on timely and reliable delivery of data packets. The medium access procedure used in 802.11p is carrier sense multiple access, which is inherently unsuitable for time-critical data traffic since it is contention-based and cannot provide a finite upper bound on the time to channel access. The simulation results indicate that with IEEE 802.11p, channel access cannot be granted in a manner that is sufficiently predictable to support reliable, low-delay communications between vehicles on a highway.

KEYWORDS: IEEE 802.11p, MAC, V2V, vehicular communication

INTRODUCTION

Traffic safety systems, where vehicles communicate with each other and with roadside stations to enable higher safety for passengers, is a new application area within the intelligent transportation systems (ITS) sphere. Typical examples include pre-crash warning, communicating slippery road conditions, emergency vehicle routing, etc. Such applications are considered by for example the American Intelligent Vehicle Initiative (IVI) (1) and the European eSafety group (2). These emerging traffic safety systems put high concurrent demands on timely and reliable delivery of data packets. Some applications also have additional demands on very low latency and therefore require direct communication between vehicles without the use of communications infrastructure, so-called vehicle-to-vehicle (V2V) communications. Further, all communication involving moving vehicles needs to be wireless and since wireless channels are subject to interference and signal fading, they are inherently unreliable. The high mobility of vehicular networks further complicates matters, since it rejects the use of traditional stable network topologies (3).

This work was funded in part by the Knowledge Foundation, www.kks.se. The authors would also like to acknowledge COST2100 SIG C for fruitful discussions, www.cost2100.org.

The data communication typically generated by traffic safety applications is characterized by short event-driven control messages that have to be received without errors in time. In addition, traffic safety systems often contain periodic messages that regularly provide information about the position, speed, direction, etc of vehicles. These messages are the foundation for a plethora of applications within ITS. Both the periodic (time-triggered) and the aperiodic (event-driven) messages require timely delivery. All messages sent will have a deadline or a best-before-date implying that if a message arrives late it is of little or no use. It is of essence that the aperiodic messages are delivered before the event takes place and further, the periodic messages are perishables as the vehicles are usually moving and more updated messages will become availabe. A traffic safety system can therefore be categorized as a critical real-time communication system (4). Real-time communication implies that there is an upper bound on the communication delay such that if the correct data does not reach its intended recipient before a certain deadline, it is more or less useless and this will potentially have severe consequences for the system performance. This problem has also been pointed out in (5). Communicating real-time messages does not necessarily require a high transmission rate, or a low delay, but it does require that the message is delivered before the deadline. Obviously, high transfer rates and low average delays are beneficial features also in real-time communication systems, but even more important is the ability to predict worst cases of system behaviour.

One of the most important things in a communication system in order to support real-time communication is the medium access control (MAC) method. This method decides who has the right to transmit when on the channel. To guarantee timely delivery such that time-critical communication tasks meet their deadlines, the MAC scheme must provide a finite *worst case access time to the channel*. Once channel access is a fact, different coding strategies, diversity techniques and retransmission schemes can be used to achieve a sufficiently reliable transmission. However, if the MAC scheme does not provide an upper bound on the maximum time before channel access, it is not possible to give any guarantees about meeting deadlines. In the upcoming vehicular communications standard IEEE 802.11p a contention-based MAC method, carrier sense multiple access (CSMA), is used. This implies that it is not possible to provide a finite upper bound on the time to channel access. However, as long as the system load is not too heavy, CSMA usually behaves satisfactory. Much attention within standardization for vehicle communication systems has therefore been devoted to enhance this MAC method by providing different quality of service (QoS) classes for traffic with different priorities (6, 7), which helps balancing the system load. However, the main problem of unpredictable delays in CSMA remains. It is therefore of essence to find out how severe this problem is when a typical traffic safety scenario is considered and to evaluate the boundaries when the system load becomes too heavy. Consequently, in this paper a MAC layer simulation of IEEE 802.11p is presented and an initial evaluation of its suitability for traffic safety application using V2V communication is made. First, an introduction to MAC methods for vehicular networks is given. Next, the IEEE 802.11p standard is explained in more detail and the paper is concluded with simulation results of the IEEE 802.11p standard.

MEDIUM ACCESS CONTROL FOR VEHICULAR COMMUNICATIONS

All communication systems have a protocol stack which is more or less complex depending on the task of the communication system (e.g., general web surfing, industrial control loops, mobile telephone systems). The MAC layer is a sublayer of the data link layer of the OSI reference protocol stack (8), and it is present in most communication networks; wireline as well as wireless. The MAC protocol is responsible for determining who has the right to send on the channel for the moment. There exists many different MAC protocols and we have chosen to

classify them here as being either contention based or conflict-free protocols (9). Conflict-free protocols ensure that a transmission is not interfered by any other transmissions, i.e., no overlap occurs in time, frequency, or space between transmitters and thus no collisions arise. Examples of conflict-free protocols are time division multiple access (TDMA) and frequency division multiple access (FDMA). TDMA divides time into slots, where the total available frequency spectrum may be used in each slot and a user will get exclusive right to send in one time slot. FDMA, on the other hand, divides the frequency band into narrower subchannels where each user is allotted a subchannel and thereafter always has the ability to send at any point in time in the subchannel. The drawback with these protocols in their original design is that they generally require a central mechanism such as a base station or an access point that can share the resources among the users (i.e., allot time slots or frequency bands to users). A combination of TDMA and FDMA is used in the GSM mobile system which duly has a centralized network topology. With contention based protocols, on the other hand, the user is not guaranteed an exclusive right to send (using the assigned resources in a predetermined way) and hence collisions can occur. Contention based protocols provide mechanisms for taking care of the collisions such that a transmission eventually should be possible. There are two large groups of contention based protocols; Aloha and CSMA. In the simplest Aloha protocol, each transmitter sends its packet as soon as it is locally generated. CSMA is an improved Aloha protocol where the transmitter starts by sensing the channel before the transmission is initiated and only transmits if the channel is free, i.e., "listen before talk." In order to reduce the probability that several transmitters starts sending immediately when the channel becomes free, each transmitter randomizes a backoff time during which it defers channel access. These two protocols are very popular, since they are easily deployed. The drawback is that there is a possibility that two or more transmissions collide and continues to collide infinitely many times and hence packets may suffer unbounded delays. This drawback is especially severe in a real-time system intended for traffic safety applications where a worst case access time is a must.

Vehicular networks could be roughly divided into *ad hoc* networks and infrastructure-based networks. The latter contains some sort of communications infrastructure, such as a base station, an access point, or a roadside station which controls the channel resources, and enables the deployment of a deterministic MAC method. *We define a deterministic MAC method to be a scheme for which the time from channel access request to actual channel access has a finite upper bound*. MAC methods that are inherently deterministic are the ones contained in the group of conflict-free protocols; e.g., TDMA and FDMA. All the communication within an infrastructure-based network must go through the centralized unit as opposed to a vehicular *ad hoc* network (VANET) with direct communication between vehicles, i.e., V2V. In a VANET a deterministic MAC scheme is harder to implement since no central entity is present.

The MAC schemes in the literature that are targeting VANETs are either based on CSMA or TDMA. CSMA has the drawback of not being deterministic and it is generally not possible to make adjustments or additions to make it deterministic. However, enhancements providing different priority levels (10, 11), such that packets with higher priorities wait a shorter time period before channel access, has been made. This is a way of reducing and controlling the network load. However, despite these enhancements collisions may still occur and when they do, a transmitter with higher priority data traffic will randomize a shorter backoff time than transmitters with lower priority traffic. This way, unbounded delays are reduced for higher priority data traffic – but not removed. This type of prioritization mechanism is also found in the standard IEEE 802.11e which will be used by the upcoming IEEE 802.11p standard. In

(10) an additional feature is considered, where a potential transmitter sends a busy tone using a reserved frequency in order to get the attention from the intended recipient, which will then poll the transmitter.

The TDMA-based protocols in (12, 13, 14, 15) use time slots to achieve collision-free transmission of data. The difference between these TDMA protocols lies in how they assign the time slots. In (12, 13) space division multiplexing (SDM) is used, where the road is first divided into subspaces, and within each subspace a TDMA scheme is applied. Each vehicle will use different time slots depending on where it is currently situated. In (14), the 3G radio interface UMTS terrestrial radio access time division duplex (UTRA TDD) is used as physical layer, and at the MAC level, the available time is divided into slots. To achieve a transmission slot in this TDMA scheme, a random access channel (i.e., CSMA) is deployed. This approach with a contention based protocol for time slot reservation requests is also used in the ADHOC MAC (15) proposal.

The drawback with almost all the MAC protocols (10, 11, 14, 15) proposed for vehicular environments is that they do not incorporate the dynamics of the network and therefore, they are still only applicable to slow moving objects and ordinary mobile *ad hoc* networks. Further, some MAC methods, such as (10, 11) prioritize packets, but the presence of collisions still results in that there is no upper bound on when channel access can take place (theoretically nodes can keep colliding forever). The *ad hoc* mode and the prioritization do decrease the average delay, but the worst case collision scenario is still the same. In (12, 13) the schemes are dependent both on a tight synchronization and on exact space awareness, something that is not easily obtained in a highly mobile VANET.

WAVE AND IEEE 802.11P

Wireless access in vehicular environment (WAVE) is IEEE's proposal to a vehicular communication system standard. WAVE is a protocol stack (6) that has support for TCP/IP traffic as well as simpler transport, network and application protocols, Figure 1. Besides the TCP/IP part, it consists of, IEEE 1609.1, IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, and IEEE 802.11p, where 802.11p is the only part which has not yet been ratified.

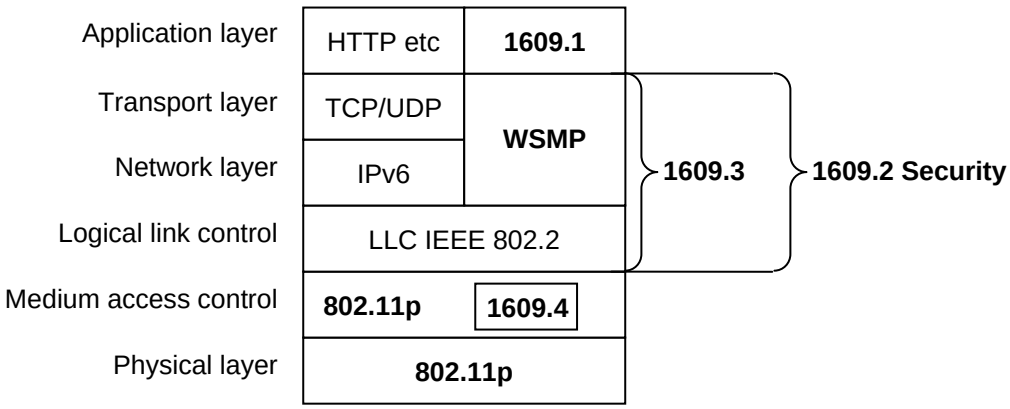

Figure 1. Overview of the WAVE protocol stack.

WAVE short message protocol (WSMP) is a transport and network layer protocol which is described in 1609.3. This provides the application layer protocol 1609.1 with the ability to determine physical layer characteristics such as channel number and output power. The

1609.1 protocol is a resource manager that multiplexes communication between one sender and multiple receivers. A WAVE compliant station must support a control channel (CCH) and multiple service channels (SCH) as defined in 1609.4. This approach is totally different from the one used in the original WLAN standard of IEEE 802.11, which instead has a cellular approach. Exactly how this new channel strategy is used is decided by 802.11p. The 1609.2 protocol adds security which is very important in this kind of networks.

The network topology in 802.11p will be a loose form of independent basic service set (IBSS) called WAVE BSS (WBSS). IBSS is the *ad hoc* mode of 802.11 where all nodes are peers. In an infrastructure-based 802.11 network, an AP is responsible for sending beacons and thereby also providing the synchronization of the network. In an 802.11 network using IBSS this beaconing is distributed among the nodes in the IBSS network. However, in an 802.11p network no beaconing exists and instead the network synchronization depends on a global time reference, such as the coordinated universal time (UTC). This can be provided by a global navigation satellite system, e.g., GPS or Galileo. It is sufficient for a node to receive the UTC information through a management frame sent in the 802.11p network. The 802.11p standard is derived from the original standard of IEEE 802.11 that was released already in 1997. 802.11p will use parts from the original standard together with the MAC amendment 802.11e for QoS support and the physical (PHY) layer supplement of 802.11a, as seen in Figure 2.

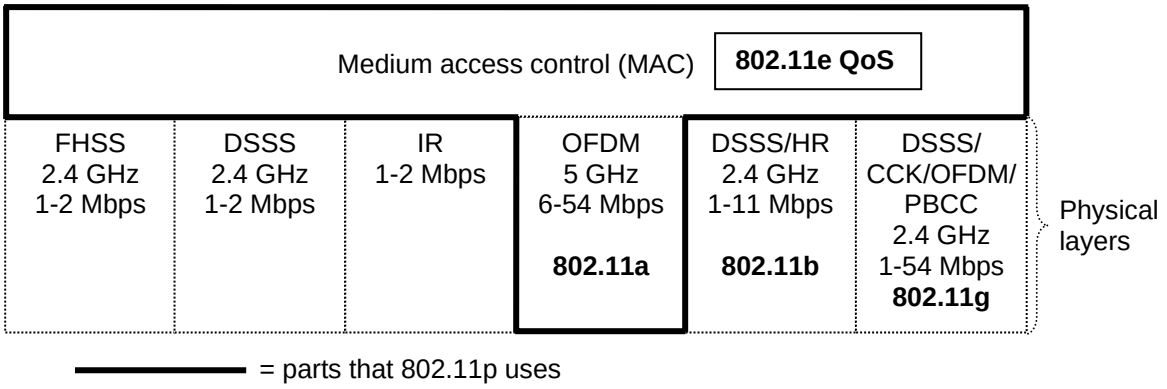

Figure 2. An overview of which part of the IEEE 802.11 that the 802.11p will use.

The WAVE protocols including 802.11p are specifically designed for the allocated frequency band in the US at 5.850-5.925 GHz called the intelligent transportation systems radio service (ITS-RS). This 75 MHz band will be divided into one CCH and six SCH. The IEEE 802.11a, uses orthogonal frequency division multiplexing (OFDM), where the basic idea is to divide the available frequency spectrum into narrower subchannels. The high-rate data stream is split into a number of lower-rate data streams transmitted simultaneously over a number of subcarriers. The 802.11p will use 10 MHz wide channels as compared to 802.11a using 20 MHz and will therefore have half the transfer rates of 802.11a namely 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps. The different transfer rates are obtained by changing modulation and coding rates.

Medium Access Control within 802.11p

The MAC layer of 802.11p (16) will use the enhanced distributed channel access (EDCA) procedure derived from the IEEE 802.11e QoS amendment. This mechanism is based on the basic CSMA with collisions avoidance (CSMA/CA), which is also known as the distributed coordination function (DCF) in 802.11. In the DCF mode all stations must compete for access to the channel (best effort system). When a station wants to send a packet, it starts by listening to the channel, an activity referred to as the physical carrier sense part of the protocol. If the

channel is free for a certain time, known as the distributed interframe spacing (*DIFS*) time, the station will start sending immediately. The 802.11 standard also specifies a virtual carrier sense mechanism called the network allocation vector (*NAV*) which is a value that indicates the amount of time before the channel will become free again. Every packet sent in the network contains information about the duration (i.e., the *NAV* time) of its transmission and all stations must update their *NAV* values according to the traffic in the network. The *NAV* value hence indicates whether the medium is busy even when the channel appears to be free as sensed by the physical carrier sense. These two carrier sense mechanisms constitute the collision avoidance part in the protocol. If a station senses that the medium is busy, either virtually or physically, it must randomize a backoff time before a transmission can be initiated anew. The backoff time is based on a specific slot time multiplied by a random number, which is uniformly distributed in the interval [0, *CW*] where *CW* stands for contention window. *CW* is doubled for every attempt to retransmit a particular packet from its initial value, CW_{min}, up to its maximum value CW_{max}. Increasing *CW* is useful during high utilization periods, when several stations want to access the channel. With a large value of *CW* there will be a greater spread of the randomized backoff times for the stations and thus collisions will decrease. After a successful packet transmission the *CW* will be set to its initial value again. The randomized backoff time is decremented only when the channel is free and once it reaches zero the station starts sending immediately.

The MAC method of 802.11 further uses a stop-and-wait protocol where the sender waits for an acknowledgement (*ACK*) from the recipient, Figure 3, and if the transmitted packet disappears for some reason, the sender must perform a backoff and try to resend the same packet.

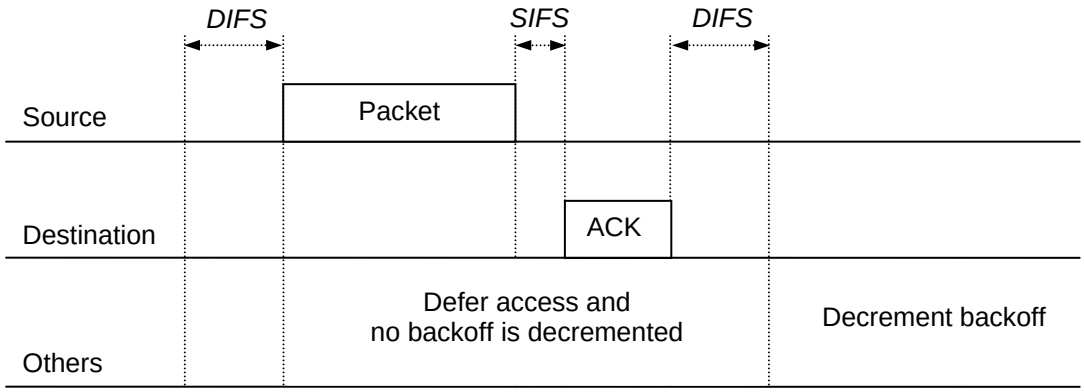

Figure 3. A packet exchange in IEEE 802.11. SIFS stands for short interframe space.

A backoff procedure can be invoked for two reasons; (*i*) a station wanting to send senses a physical or virtual carrier during its mandatory *DIFS* listening period or (*ii*) a station has managed to send its packet but never received an *ACK* packet in return. A station that is in backoff mode is not allowed to decrement the backoff value while the channel is busy, which includes the *DIFS* period that follows a transmission (Figure 3). However, once a backoff value reaches zero the station can start to send immediately.

The EDCA MAC method introduces improved features such as prioritized access to the channel by means of several queues with different *DIFS* values, although *DIFS* are instead called arbitration interframe space (*AIFS*) in EDCA. There are four queues which represent different levels of priority (called access categories/ACs in 802.11e); background, best effort, video and voice traffic, where voice has the highest priority, Table 1.

Table 1. The parameters from the 802.11e used in the 802.11p.

Designation	AC in 802.11e	AIFSN	CW_{min}	CW_{max}
Background	AC_BK	7	aCWmin	aCWmax
Best effort	AC_BE	3	aCWmin	aCWmax
Video	AC_VI	2	aCWmin/2	aCWmax
Voice	AC_VO	2	aCWmin/4	aCWmax/2

Every terminal in an 802.11p network contains these four queues and the queue with the highest priority will wait the shortest time (the shortest *AIFS*) before its transmission can start. This way, different priorities are enforced and stations having lower priority traffic will lose the race for the channel when competing with a station having higher priority traffic. However, collisions between packets of the same priority can still occur and these are handled with a backoff procedure. In WAVE, the different queues have different *CW*s such that high priority traffic will have shorter backoff times than low priority traffic. Each queue contends for the channel in the same way as with the basic access method DCF with the difference of how long they will listen before starting to send (the AIFS). The AIFS for an AC/queue is calculated as follows $AIFS[AC] = AIFSN[AC] \times aSlotTime + SIFS$. The default values of the *AIFSN* are found in Table 1. When the PHY of 802.11p is used, the *AIFS* for voice packets will be 34 μs which should be compared to 41 μs for a DIFS in the 802.11a standard. When a collision occurs within the station, the queue with the highest priority will win the contention and therefore access the channel. The other colliding queue must then randomize a backoff time and try anew.

SIMULATION STUDY OF THE MAC METHOD IN 802.11P

We have developed a simulator in a computer using Matlab and our scenario is a highway with three lanes in each direction where the vehicles arrive according to a Poisson process as is customary for many traffic systems. The scenario chosen can be assumed to be the most stressful situation for the MAC scheme since here the highest relative vehicular speeds are found. The inter-arrival times between the vehicles in each lane are modeled as independent identically distributed exponential random variables with a mean of 3 seconds (consistent with the 3-second-rule applied in Sweden, which recommends drivers to maintain a 3 second space to the vehicle in front). The speed of each vehicle is a random variable with a Gaussian distribution with mean values different for each lane; 23 m/s (~83 km/h), 30 m/s (~108 km/h) and 37 m/s (~133 km/h), and a standard deviation of 1 m/s. The speeds were chosen with the Swedish highway speed regulations in mind, i.e., trucks are allowed to have a maximum speed of 90 km/h, cars 120 km/h at certain places otherwise 110 km/h, cars with a trailer 70 km/h, etc. The vehicles regularly broadcast data messages containing information about their speed, position, direction etc., according to a predetermined rate of 10 Hz (one new packet every 100 ms) and there is no other data traffic. The messages are broadcast messages and therefore no one will send an *ACK* in response.

All vehicles use the MAC method of 802.11p as described above, and each vehicle must listen before sending during an *AIFS* and backoff if the channel is, or becomes, busy during the *AIFS*. Since all the data traffic is of the same priority, i.e., everyone broadcasts position messages, only the highest priority is used. In a real implementation where data traffic from different applications must share the same communication channel, these position messages would probably have a lower priority than messages containing, e.g., collision avoidance data.

If we had chosen a lower priority in our simulation scenario this would have had the implication that fewer messages would fit into the same time frame and thus the network load would increase and the simulation results would show a reduced performance. Note that the only time a backoff procedure is invoked is when a physical or virtual carrier is detected during the *AIFS*. Consequently, the case with a missing *ACK*, as described above, will not appear since all traffic is broadcasted and there is no specific intended recipient. Instead all nodes within sensing range are recipients. With this in mind, the transmitter will never make more than two attempts to access the channel in order to try to send a packet. If a carrier is detected in the first access attempt, the transmitter randomizes a backoff time. The transmitter is then only allowed to decrement the backoff time when the channel is detected as free and an *AIFS* period has passed, see Figure 3. When the backoff counter has reached zero, the vehicle will send immediately. In Table 2, all parameters used in the simulation are listed.

Table 2. IEEE 802.11p parameters used in the simulation.

Parameter	**Value**
Slot time	9 µs
SIFS	16 µs
AC in 802.11e	AC_VO (Voice)
AIFSN	2
AIFS for voice	34 µs
CW_{min}	aCWmin/4 = 16/4, $\Rightarrow CW \in \{0,1,2,3\}$
CW_{max}	Will never be used due to broadcast
Transfer rate	3 Mbps

All vehicles have the same data traffic type to send, and therefore all transmitters will have the same *AIFS* value of 34 µs. The contention window will never be doubled since only one failed channel access attempt is made. The backoff time is a random number resulting from a multiplication between the slot time and a discrete random number uniformly distributed in the interval [0, 3] and stations will only randomize between four different values in this simulation; 0, 9, 18, and 27 µs, respectively.

The channel model is a simple circular sensing range model, Figure 4. We assume that every node within the assumed sensing area receives the message perfectly (i.e., without errors). Note that a node could be exposed to a second transmission by a so-called hidden terminal, Figure 4, where transmitters Tx_1 and Tx_2 are sending at the same time because they cannot hear each other, and the receivers Rx_1, Rx_2, Rx_3 and Rx_4, will experience collisions of the two ongoing transmissions. However, since the focus of this simulation is to determine the delay before a transmitter will get a channel access, the hidden terminal problem is not considered.

To avoid the edge effects in the simulation, statistics are only collected from the middle part of the highway and only when the highway has been filled with traffic. The nodes will start to transmit as soon as they enter the highway at an initial random delay between 0-100 ms. The simulation has been carried out with three different packet lengths; 100, 300, and 500 bytes and three different sensing ranges, 300, 500, and 1000 meters. The chosen sensing ranges have its origin in the project authorization request (PAR), i.e., the project proposal, for IEEE 802.11p (17), which states that communication ranges of up to 1000 m should be supported by the standard. Even though 802.11p has support for up to eight different transfer rates, a transfer rate of 3 Mbps without link adaptation has been used. This is due to the fact that this

is a broadcast system that requires high reliability and we want as many nodes as possible to hear each transmission correctly. The lowest transfer rate has the most robust modulation scheme together with the lowest coding rate and is therefore a reasonable choice.

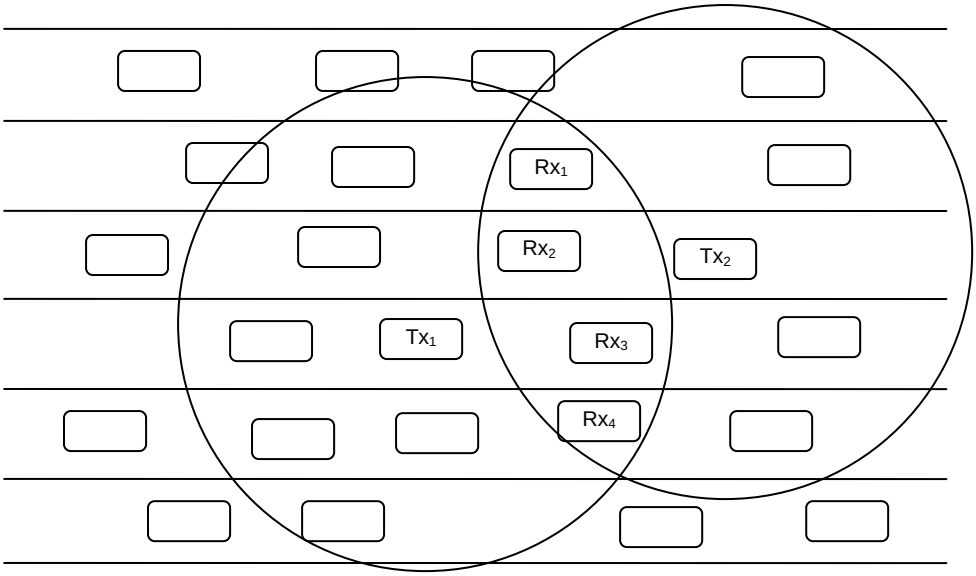

Figure 4. Simulation set-up

Figure 5 depicts the cumulative distribution functions (CDF) for the channel access delay for different sensing ranges and 300 byte packets. The channel access delay is defined as the time it takes from when a packet arrives at the MAC layer in a node to when the channel is accessed, i.e., the delay between channel request to channel usage. Hence, the CDF curves show the probability that channel is accessed within a certain delay. For example, it can be concluded from Figure 5 that, for a 1000 m long sensing range, the channel access delay will be less than 20 ms with a probability of about 90%. The delay is never less than 34 μs because of the *AIFS* value, and it will never exceed 100 ms because when a new packet arrives at the MAC layer from the application layer, the old one that is still waiting for channel access will be thrown away, i.e., the packet is dropped.

For each sensing range, the CDF includes all channel access attempts made by all vehicles, i.e., around 15-18 million access attempts. The average number of possible recipients for the different sensing ranges are as follows; 300 m ~ 34-36 nodes, 500 m ~ 58-60 nodes, and 1000 m ~116-118 nodes. Consequently, this is also the average number of nodes that will compete for channel access. When the CDF reaches 1, this means that no node has been forced to drop any packets, i.e., all packets generated at each node were sent. In Figure 5 it is shown that approximately 5% of the packets were dropped for a sensing range of 1000 meters. Theoretically, 117 nodes could fit into a system having 300 byte long packets if the transmissions were perfectly scheduled (100 ms divided by the transmission time for a 300 byte long packet plus the *AIFS*). This explains why nodes start to drop packets when the sensing range reaches 1000 m.

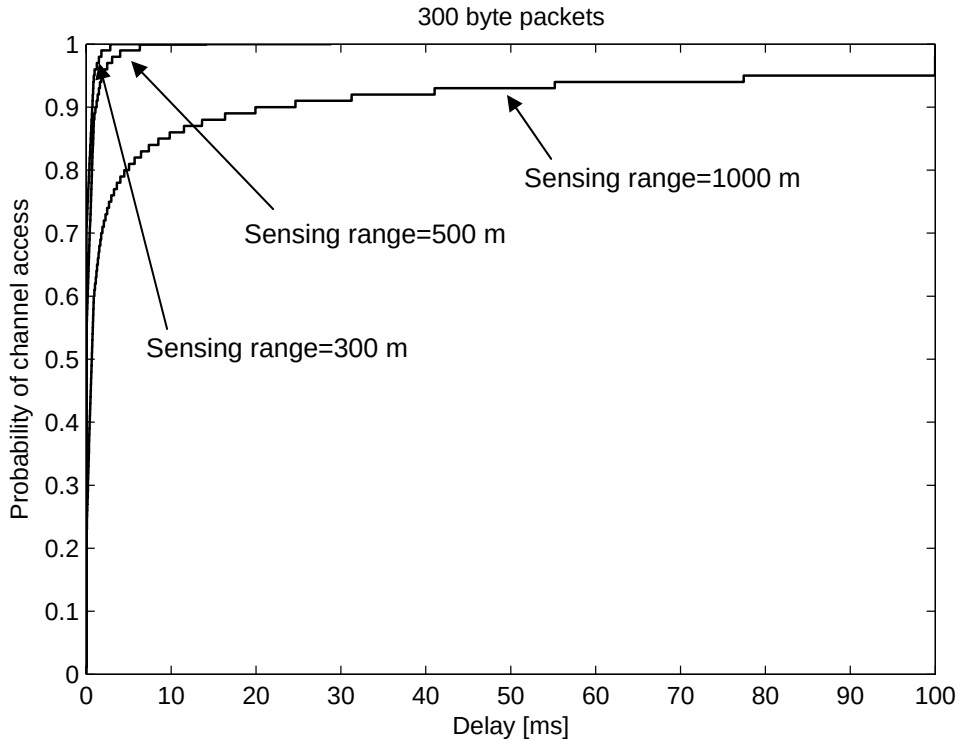

Figure 5. The CDF of the channel access delay for 300 byte packets and different sensing ranges.

In Figure 6, the CDF for the channel access delay for 500 byte packets is shown for different sensing ranges. Here, it can be seen that also vehicles having a sensing range of 500 meter starts dropping packets.

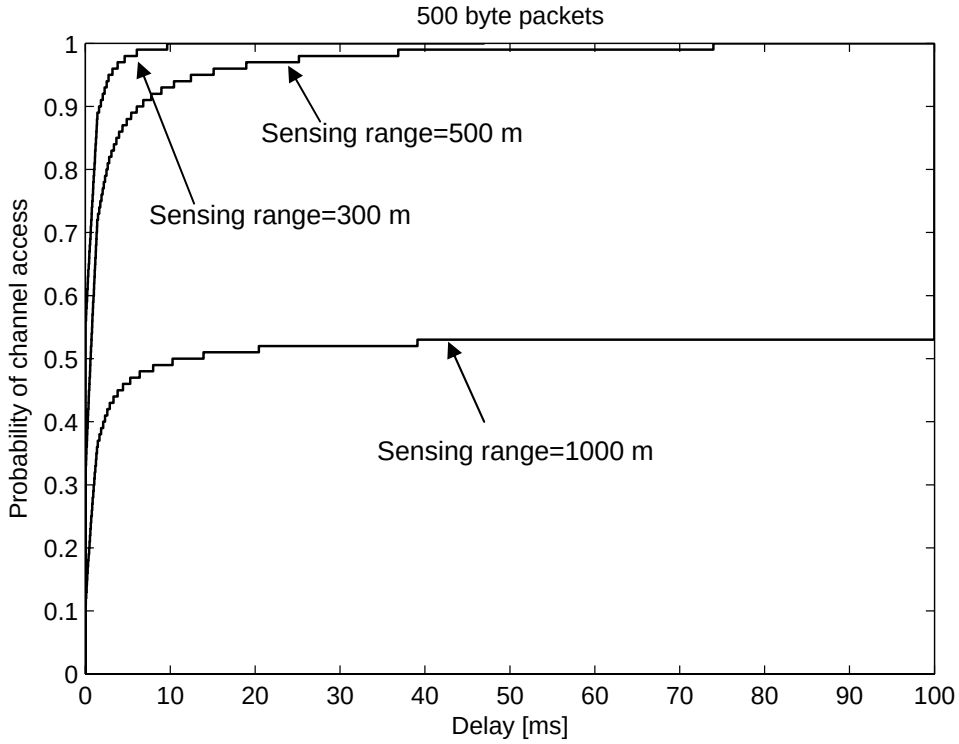

Figure 6. The CDF of the channel access delay for 500 byte packets and different sensing ranges.

When the packet length is increased, every node keeps the channel busy for a longer time period and with a greater sensing range more nodes are blocked, i.e., they must defer their own channel access due to an occupied channel. In Figure 6, stations having a sensing range of 1000 meter will drop around 45% of their packets. A packet drop could also be interpreted as a node that never succeeded to decrement its backoff value to zero. Since the nodes only randomize between the backoff values; 0, 9, 18, and 27 μs, the channel was never free for these times during the 100 ms period before a new packet arrived at the MAC layer.. Note that the theoretical number of nodes that fits into a sensing range of 1000 meter when sending 500 byte long packets is 72 (100 ms divided by the transmission time for a 500 byte long packet plus the *AIFS*). This is the reason for packet drops occurring when the sensing range is increased from 500 meter to 1000 meter. Simulations with shorter packets than 300 byte were also conducted, but they did not suffer from any packet drops and are therefore not shown here.

CONCLUSION

We have classified future traffic safety systems as being critical real-time systems thus requiring a deterministic MAC method, i.e., a MAC method for which *the time from channel access request to actual channel access has a finite upper bound*. Conflict-free MAC methods (e.g., TDMA, and FDMA) are inherently deterministic, but usually require a centralized network structure for distributing the channel resources among the nodes. These methods are unsuitable for VANETs. Many emerging traffic safety systems will require low latency and thereby need direct V2V communication, and the only standard currently supporting this is the upcoming IEEE 802.11p. The 802.11p standard will use contention-based CSMA as MAC method, implying that there is no upper bound on the delay before channel access (i.e., non-deterministic) which makes it unsuitable for critical real-time communication. The 802.11p will use the 802.11e QoS amendment, but this will only decrease the average delay for high priority packets when the data traffic types are mixed and contain traffic from all ACs. However, if the nodes in the network all have the same type of traffic, the QoS amendment is of no use. We will still have the problem with unbounded delays when the network load increases.

Our initial simulation results of the MAC method for IEEE 802.11p show increasing delays for longer packets and greater sensing ranges. Moreover, the probability of dropping packets is alarmingly high for certain simulation points, e.g., for a sensing range of 1000 meters (which is supported by the upcoming 802.11p stated in its project proposal, i.e., the PAR). The question is what range is needed by a typical application and what do we need to know about other vehicles in the vicinity? This must be studied in more detail, in order to determine how severe the consequences are. For example, if packets are dropped in bursts for a certain node; this implies that a vehicle could be invisible to all other vehicles in the vicinity. It can be concluded that even though IEEE 802.11 works well in our offices and homes, more detailed studies of the 802.11p standard are needed before time critical applications at vehicular speeds can be considered. Since the MAC protocol does not have an upper bound on when access to the channel occur it is unsuitable for critical real-time communication especially in a highly dynamic environment as required by future vehicle safety applications.

REFERENCES

(1) Intelligent Vehicle Initiative, http://www.its.dot.gov/ivi/ivi.htm.
(2) eSafety, http://www.esafetysupport.org/.
(3) K. Bilstrup *et al*., "Vehicle alert system," in *Proc. of the 14th World Congress on Intelligent Transport Systems*, Beijing, China, Oct. 2007.
(4) C. M. Krishna and K. G. Shin, *Real-Time Systems*, McGraw-Hill, New York, 1997.
(5) J. J. Blum, A. Eskandarian, and L. J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE Trans. on ITS*, vol. 5, no.4, pp. 347-351, Dec. 2004.
(6) K. Bilstrup, "A Survey Regarding Wireless Communication Standards Intended for a High-Speed Vehicle Environment," *Technical Report IDE 0712*, Halmstad University, Sweden, Feb. 2007.
(7) Z. Kong, D. H. K. Tsang, B. Bensaou and D. Gao, "Performance analysis of IEEE 802.11e contention-based channel access," *IEEE J. Sel. Areas in Com.*, vol. 22, no. 10, pp. 2095-2106, Dec. 2004.
(8) A. S. Tanenbaum, *Computer Networks*, Prentice Hall, U.S., 2003.
(9) R. Rom and M. Sidi, *Multiple Access Protocols: Performance and Analysis*, Springer-Verlag, New York, 1990.
(10) S. Yang, H. H. Refai, and X. Ma, "CSMA based inter-vehicle communication using distributed and polling coordination," in *Proc. IEEE Int. Conf. on ITS*, Vienna, Austria, Sept. 2005, pp. 167-171.
(11) A. Pal, A. Dogan, F. Özgüner, and Ü. Özgüner, "A MAC layer protocol for real-time inter-vehicle communication," in *Proc. of the IEEE Int. Conf. on ITS*, Singapore, Sept. 2002, pp. 353-358.
(12) S. V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks," in *Proc. of the IEEE Int. Conf. on ITS*, Oakland, CA, Aug. 2001, pp. 962-968.
(13) J. J. Blum and A. Eskandarian, "A reliable link-layer protocol for robust and scalable intervehicle communication," *IEEE Trans. on ITS*, vol. 8, no. 1, pp. 4-13, Mar. 2007.
(14) M. Lott, R. Halfmann, E. Schulz, and M. Radimirsch, "Medium access and radio resource management for ad hoc networks based on UTRA TDD," in *Proc. of ACM Symp. on Mobile Ad Hoc Networking and Computing*, Long Beach, CA, Oct. 2001, pp. 76-86.
(15) F. Borgonova, L. Campelli, M. Cesana, and L. Coletti, "MAC for ad-hoc inter-vehicle network: services and performance," in *Proc. of the IEEE Int. Vehicular Technology Conference*, Orlando, FL, Oct. 2003, pp. 2789-2793.
(16) IEEE P802.11p/D3.0, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specification: Amendment: Wireless Access in Vehicular Environment (WAVE)*, Draft 3.0, July 2007.
(17) The PAR for IEEE 802.11p, http://www.ieee802.org/11/PARs/index.html#Active