Thesis for the degree of Licentiate of Engineering

Predictable and Scalable Medium Access Control for Vehicular Ad Hoc Networks

Katrin Sjöberg Bilstrup

Department of Signals and Systems

CHALMERS UNIVERSITY OF TECHNOLOGY

School of Information Science, Computer and Electrical Engineering

HALMSTAD UNIVERSITY

Göteborg, Sweden, 2009

Predictable and Scalable Medium Access Control for Vehicular Ad Hoc Networks

Katrin Sjöberg Bilstrup

Technical Report No. R016/2009
ISSN 1403-266X

Department of Signals and Systems
CHALMERS UNIVERSITY OF TECHNOLOGY
Hörsalsvägen 11
SE-412 96 Göteborg
Sweden
Telephone: +46 - (0)31 - 772 10 00
Fax: +46 - (0)31 - 772 36 63

Contact Information:
Katrin Sjöberg
School of Information Science, Computer and Electrical Engineering
HALMSTAD UNIVERSITY
SE-301 18 Halmstad
Sweden

Telephone: +46 - (0)35 - 16 71 00
Fax: +46 - (0)35 - 12 03 48
Email: Katrin.Sjoberg@hh.se

Printed in Sweden
Chalmers Reproservice
Göteborg, Sweden, 2009

Predictable and Scalable Medium Access Control for Vehicular Ad Hoc Networks

KATRIN SJÖBERG BILSTRUP
School of Information Science, Computer and Electrical Engineering, Halmstad University
Department of Signals and Systems, Chalmers University of Technology

Thesis for the degree of Licentiate of Engineering

Abstract

This licentiate thesis work investigates two medium access control (MAC) methods, when used in traffic safety applications over vehicular *ad hoc* networks (VANETs). The MAC methods are carrier sense multiple access (CSMA), as specified by the leading standard for VANETs IEEE 802.11p, and self-organizing time-division multiple access (STDMA) as used by the leading standard for transponders on ships. All vehicles in traffic safety applications periodically broadcast cooperative awareness messages (CAMs). The CAM based data traffic implies requirements on a predictable, fair and scalable medium access mechanism. The investigated performance measures are *channel access delay*, *number of consecutive packet drops* and the *distance between concurrently transmitting nodes*. Performance is evaluated by computer simulations of a highway scenario in which all vehicles broadcast CAMs with different update rates and packet lengths. The obtained results show that nodes in a CSMA system can experience *unbounded channel access delays* and further that there is a significant difference between the best case and worst case channel access delay that a node could experience. In addition, with CSMA there is a very high probability that several *concurrently transmitting nodes are located close to each other*. This occurs when nodes start their listening periods at the same time or when nodes choose the same backoff value, which results in nodes starting to transmit at the same time instant. The CSMA algorithm is therefore both *unpredictable* and *unfair* besides the fact that it *scales badly* for broadcasted CAMs. STDMA, on the other hand, will always grant channel access for all packets before a predetermined time, regardless of the number of competing nodes. Therefore, the STDMA algorithm is *predictable and fair*. STDMA, using parameter settings that have been adapted to the vehicular environment, is shown to outperform CSMA when considering the performance measure *distance between concurrently transmitting nodes*. In CSMA the distance between concurrent transmissions is random, whereas STDMA uses the side information from the CAMs to properly schedule concurrent transmissions in space. The price paid for the superior performance of STDMA is the required network synchronization through a global navigation satellite system, e.g., GPS. That aside since STDMA was shown to be scalable, predictable and fair; it is an excellent candidate for use in VANETs when complex communication requirements from traffic safety applications should be met.

Keywords: CSMA, self-organizing TDMA, STDMA, medium access control, MAC, vehicular ad hoc networks, VANET, vehicle-to-vehicle communications, V2V, V2X, IEEE 802.11p, WAVE, DSRC, ETSI ITS-G5, ISO CALM M5, real-time communications, scalability, traffic safety, cooperative system

Acknowledgement

The first part of my doctoral studies is finished with this licentiate thesis and it has been astonishing years. Never in my wildest dreams could I have imagined that this work could be so interesting. I have during my first years gotten to know many great people that have inspired me to continue and to “keep up the good work”.

First I would like to thank Dr. Elisabeth Uhlemann, Halmstad University and Volvo Technology, and Prof. Erik G. Ström, Chalmers University of Technology, who are two excellent supervisors (ok, I have nothing to compare with but they are really great!). I have had a really nice time with you! If I fail to turn my licentiate degree into a doctor’s degree it is totally my own fault. My next thanks go to Dr. Urban Bilstrup, SAAB, who actually led me into the research world and all of its winding roads from the beginning. He has been my “background supervisor” and I am grateful to him for many reasons and our vivid, in depth technical discussions especially. Prof. Bertil Svensson, Halmstad University, has also been a source of inspiration and support. I am grateful to my fellow workers at CC-lab at Halmstad University as well as ComSys at Chalmers. I do not want to mention any particular persons at the different departments because almost everyone has played a role in one way or another through my studies. No one mentioned and no one forgotten… ☺

I have had the opportunity and the pleasure to work in close collaboration with people in the industry and they have showed much interest in my work, which demonstrates how important research is for companies. Here my thanks go to Pelle Wiberg, Free2Move, Niclas Nygren, Volvo Technology, Knut Evensen, Q-Free, Runar Søråsen, Q-Free, and Peter Bergljung, SAAB TransponderTech.

Everything is not just about research. There is always much administrative stuff competing for attention and the several persons involved in this at Halmstad University have made many things a lot easier for me. Thanks to Roland Thörner CC-lab, Niklas Sjöberg and Johan Persson at the IT department, and, last but not least, all the secretaries at the School of IDE at Halmstad University, Ulla Johansson, Eva Strid-Andersson, Eva Nestius, Jessika Rosenberg and her stand-in Christer Svensson, and Marie-Louise Lunder.

At last I would like to thank my friends and family who have always been there for me when I have made my decisions through life. Thanks to Linda “Silbergskan”, Cissi, Solveig, Pernilla, Cinna, Sofia, Jessicka, Maria and Cia. And my lovely family – my parents Margareta and Stig, my brothers Niklas and Lasse, and my two sons Sixten and Nils, forcing me to think about other things that are much more important than research such as playing with Lego or toy cars….

This work was mainly funded by the Knowledge Foundation through the profile Center for Research on Embedded Systems (CERES), Halmstad University.

List of appended papers

[Paper A] 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 communication,” in *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 902414, 13 pages, doi:10.1155/2009/902414.

[Paper B] K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, “On the ability of IEEE 802.11p and STDMA to provide predictable channel access,” in *Proc. of 16th World Congress on ITS*, Stockholm, Sweden, Sept. 2009.

[Paper C] K. Sjöberg Bilstrup, E. Uhlemann, and E. G. Ström, “Scalability issues for the MAC methods STDMA and CSMA/CA of IEEE 802.11p when used in VANETs,” submitted to *IEEE International Conference on Communications, ICC2010*, Cape Town, South Africa, May 2010.

Related publications

K. Sjöberg Bilstrup, E. Uhlemann, and E. G. Ström, ”Performance of IEEE 802.11p and STDMA for vehicular cooperative awareness applications,” presented at *9th COST2100 Meeting*, TD(09)938, Vienna, Austria, Sept. 2009.

K. Bilstrup, E. Uhlemann, and E. G. Ström, “Medium access control in vehicular networks based on the upcoming IEEE 802.11p standard”, in *Proc. of the 15th World Congress on Intelligent Transport Systems*, New York, US, Nov. 2008.

K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, “Evaluation of the IEEE 802.11p MAC method for vehicle-to-vehicle communication,” in *Proc. of the 2nd IEEE Int. Symp. on Wireless Vehicular Communications*, Calgary, Canada, Sept. 2008.

K. Bilstrup, A. Böhm, K. Lidström, M. Jonsson, T. Larsson, L. Strandén and H. Zakizadeh, ”Vehicle alert system,” in *Proc. of the 14th World Congress on Intelligent Transport Systems*, Beijing, China, Oct. 2007.

K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, ”Medium access control schemes intended for vehicle communication,” presented at *3rd COST2100 Meeting*, TD(07)369, Duisburg, Germany, Sept. 2007.

K. Bilstrup, “A survey regarding wireless communication standards intended for a high-speed vehicle environment,” Technical Report IDE0712, Halmstad University, Sweden, Feb. 2007.

Table of contents

Abbreviations

ACK	ACKnowledgment
AIS	Automatic Identification System
ASTM	American Society for Testing and Materials
C2C-CC	Car-to-Car Communication Consortium
CALM	Communication Access/Architecture for Land Mobiles
CAM	Cooperative Awareness Messages
CAN	Controller Are Network
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA with Collision Avoidance
CVIS	Cooperative Vehicle-Infrastructure Systems
DAB	Digital Audio Broadcast
DCC	Distributed Congestion Control
DSRC	Dedicated Short-Range Communications
DNM	Decentralized Notification Messages
EDCA	Enhanced Distributed Channel Access
ETC	Electronic Toll Collection
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FOT	Field Operational Test
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
LDM	Local Dynamic Map
MAC	Medium Access Control
OFDM	Orthogonal Frequency Division Multipexing
PHY	Physical layer
RFID	Radio Frequency Identification
RTTT	Road Transport and Traffic Telematics
STDMA	Self-organizing Time Division Multiple Access
STF	Specialist Task Force
TC	Technical Committee
TPC	Transmit Power Control
TDMA	Time Division Multiple Access
WAVE	Wireless Access in Vehicular Environments
WG	Working Group
WLAN	Wireless Local Area Networks

PART I

This licentiate thesis is divided into two parts. The first part gives an introduction to the topic treated in this thesis, namely medium access control for vehicular ad hoc networks, to provide a background to the contributions presented in the second part of the thesis. Section 1 of Part I outlines the big picture around vehicular communications including ongoing standardization activities. The second section describes how cooperative systems based on vehicle communications are intended to increase traffic safety. Vehicular *ad hoc* networks are discussed together with the communication requirements that are set through certain traffic safety applications and appropriate metrics to evaluate them. In Section 3 the medium access control algorithms scrutinized in this thesis are detailed. Part I is concluded with the research motivation, problem description and the future directions of this thesis work. In Part II the appended papers are found.

1 Introduction

Vehicles, cooperating to increase traffic safety, are soon to be a reality. What previously seemed to be utopia is now assuming a more and more definite shape. In the beginning of the 90s there was a frantic research activity on vehicular communications, especially in Germany. However, after the efforts made in the projects PROMETHEUS and PReVENT [1], the activity around vehicular communications diminished for several reasons. One factor was the lack of cost efficient wireless technologies that could enable the proposed applications, and another was that the car manufacturers were not ready or did not see the potential benefits that communication between vehicles could establish. There were still many things within passive safety that could be done individually by the car manufacturers to gain market advantages.

However, in 1999 the activities relating to vehicular communications took off again, when the Federal Communications Commission (FCC) in the US allocated a 75 MHz band at 5.850-5.925 GHz especially intended for intelligent transportation systems (ITS): “to improve traveller safety, decrease traffic congestion, facilitate the reduction of air pollution, and help to conserve vital fossil fuels” [2]. The American Society for Testing and Materials (ASTM) was commissioned to bring forward a standard and they did so by emanating from the Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 for wireless local area network (WLAN) [3] and made some minor changes to fit high-speed vehicular environments. The ASTM standard [4] made use of a simple mailbox application layer [5] and the resulting protocol stack contained only three layers: application, data link and physical. The standard was termed dedicated short-range communications (DSRC), which is somewhat misleading, since the term DSRC since the 80s has referred to application specific vehicular communication systems such as electronic toll collection (ETC), traffic traveller information, automatic vehicle identification etc., in Europe and Japan. These types of application specific systems can be classified as radio frequency identification systems (RFID) since their applications are fairly simple, the communication technology is intended for hotspots without networking (i.e., single hop where no routing is necessary) and the transmission takes place between vehicles and roadside units (i.e., transponders and readers). Consequently, and slightly confusing, DSRC refers to a type of RFID system in Europe and Japan, whereas in the US it refers to a type of WLAN system.

Much has happened in the last decade and a standard supporting *ad hoc* communications between vehicles is now under development within IEEE. This is based on the work carried out by ASTM in 2003, but IEEE is developing a whole protocol stack including application, network and transport layers called wireless access in vehicular environment (WAVE) [6, 7, 8, 9], where the draft standard 802.11p constitute one part [10]. IEEE 802.11p will amend 802.11 both at the physical (PHY) layer and the medium access control (MAC) layer. IEEE 802.11p is intended for the frequency band allocated in the US, which is a 75 MHz band divided into one control channel and six service channels located at 5.850-5.925 GHz. The WAVE specification 1609.4 [9] describes exactly how the frequency channels are utilized and what types of messages that are admitted or prohibited on what channels. As might be recalled, the first version of IEEE 802.11 was released in 1997. It contained a MAC layer and three different PHY layers sharing the same MAC. After this release there has been several amendments and supplements made to the original standard, e.g., 802.11a a new PHY layer, 802.11b a new PHY layer, and 802.11e Quality of Service (QoS) support. At regular intervals the IEEE makes so-called roll-ups where ratified amendments and supplements up to a given date are included in the base standard and the amendment letters are dropped. There have been two major roll-ups of the 802.11 standard since the release in 1997 and the last one was in 2007. The draft standard IEEE 802.11p intended for the vehicular environment will probably be ratified in June 2010 and the next roll-up is planned to 2012. Currently, there is no other competing standard for *ad hoc* communications between vehicles. Instead, standardization organizations have now agreed to cooperate to achieve a globally interoperable standard based on IEEE 802.11p.

The International Organization for Standardization (ISO) is developing a more general specification of 802.11p under its framework called Communication Architecture for Land Mobiles (CALM) and has coined this standard to CALM M5 [11]. The idea with CALM is to use all types of already existing wireless access technologies such as 2G/3G/LTE, wireless broadband access (e.g., WiMAX), WLAN, CALM M5, DSRC (as defined in Europe and Japan), to provide seamless wireless connection to the end users. In the protocol stack above the different wireless carriers, the internet protocol version 6 (IPv6) is found, gluing together all different access technologies. A future vision in CALM is also to integrate access technologies within the vehicle, wired as well as wireless, e.g., Bluetooth, IEEE 802.15.x (wireless personal area networks), controller area network (CAN), receiver for digital audio broadcast (DAB) etc.

In Europe it was not possible to use the same frequency band as in the US due to different current frequency allocations in some European countries. However, the frequency regulators in Europe have managed to set aside 30 MHz in a first step towards a harmonized frequency band for ITS applications. The frequency band in Europe, 5.875-5.905 GHz, is currently divided into two service channels and one control channel, solely intended for safety related ITS applications. The band just below, 5.855-5.875 GHz will probably in the future be used for non-safety ITS applications. A third band is also being considered for use of ITS applications as a whole, namely 5.470-5.725 GHz. In Europe there is also a previously allocated band called Road Transport and Traffic Telematics (RTTT) at 5.795-5.805 GHz dedicated for the European DSRC, i.e., used for ETC. The European Telecommunications Standards Institute (ETSI) in Europe is bringing forward a profile of 802.11p tailored for the 30 MHz allocated in Europe [12]. The technical committee (TC) on ITS within ETSI was formed in December 2007. It is divided into five working groups (WG). WG1 deals with user and application requirements, specifying amongst other things the different message types. They have identified two types of messages needed – decentralized notification messages (DNM) and cooperative awareness messages (CAM). The former is a response to an event and the packet size is variable depending on what application that triggered the creation of a DNM. The CAMs are time-triggered messages containing information about a vehicle's position, speed, heading etc. These messages are broadcasted periodically by all nodes and will probably have an update rate of 2 Hz and a packet length of 800 byte. The US has another approach, where the CAMs are shorter, in the order of 100-300 bytes with a frequency of 10 Hz. This is due to packets having less security and applications requiring a higher update rate. In Europe the longer packet sizes is caused by the security overhead. WG2 takes a holistic view, trying to find a common architecture for ITS stations and it also deals with cross-layer issues. Geonetworking and IPv6 are central concepts in the work conducted by WG3, which handles transport and network layers issues as a whole. WG4 is the group developing a profile of the 802.11p suited for the 30 MHz band in Europe, together with transmit power control (TPC) algorithms and decentralized congestion control (DCC) mechanisms to enhance the performance of 802.11p. Security is a very important and crucial issue in cooperative systems and it is dealt with in WG5. The first ETSI ITS related standards are to be ratified in the end of 2009.

2 Cooperative systems for traffic safety

There exists a plethora of different ITS applications, ranging from conventional web browsing to collision avoidance applications. The main motivation for using vehicular communications to form cooperative systems is to decrease the number of traffic accidents by introducing traffic safety applications, but also to reduce congestion, travel-time and pollution through traffic efficiency applications. In addition, other types of services may be offered to facilitate system introduction and provide sustainable business and operation models. Mainly three types of applications are considered: *traffic safety*, *traffic efficiency* and *value-added services*. These applications will use different wireless access technologies to meet the diverse set of communication requirements. *The main focus of this thesis work is traffic safety applications since the communication requirements of these applications notably differ from those of most existing applications relying on wireless communications.* Emergency electronic brake lights, wrong way driving warning, collision risk warning, traffic and jam detection are all examples of traffic safety applications with stringent communication requirements.

Cooperative systems for enhancing traffic safety both for in-vehicle passengers as well as other road-users are under intensive investigation and development throughout the world for the moment. In Europe there are several large EC funded projects investigating cooperative systems; Cooperative Vehicle-Infrastructure Systems (CVIS), Safe Cooperative Driving – Smart Vehicles on Smart Roads (SAFESPOT), Cooperative Systems for Intelligent Road Safety (COOPERS), and Preparation for Driving Implementation and Evaluation of C2X Communication Technology (Pre-Drive C2X). There is also a Specific Support Action termed Communications for eSafety [13] (COMeSafety) as well as a well-established consortium called the Car-2-Car Communication Consortium (C2C-CC). CVIS [14] is a project consisting of over 60 partners from academia, industry, society and research institutes. The focus of the project is on communications architecture with traffic efficiency applications in mind. Examples are journey planning to avoid congested areas, pre-booking of parking space etc. CVIS will use CALM in an open architecture platform for continuous connectivity. SAFESPOT [15] on the other hand focuses more on traffic safety related applications aiming to increase the horizon of awareness of the driver. This project is of approximately the same size as CVIS. One of the main contributions from SAFESPOT is an ITS facility called local dynamic map (LDM), where a map with several layers is built up dynamically starting with a standard static road map at the bottom. Next follows a layer containing landmarks for referencing, which for example could be road signs. Semi-dynamic information, such as recent traffic accidents or road construction sites is presented in the third layer, whereas the final layer is made up of position messages broadcasted periodically by all surrounding vehicles, i.e., the CAMs. This LDM facility is the basis for many traffic safety applications such as collision avoidance, lane merge assistance etc. and the work in SAFESPOT is used for standardization within ETSI TC ITS. The COOPERS project considers telematics applications from the road operators' point of view with the long term goal of cooperative traffic management. Pre-Drive C2X [16] with approximately 25 partners prepares a large-scale field operational test (FOT) and aims to test the findings from other projects. A common European ITS communications architecture is described in "the COMeSafety document", in which results from several European projects are gathered [17]. The document is also used within ETSI standardization as well as in Pre-Drive C2X for implementation. C2C-CC [18] was from the beginning a German initiative involving car manufacturers, suppliers and other interested parties. They want to create an open industrial standard based on IEEE 802.11 together with deployment strategies. Both C2C-CC as well as the EC funded projects are involved in the European standardization activities within ETSI TC ITS with the goal to ensure total interoperability between different vehicle manufacturers.

2.1 Vehicular Ad Hoc Networks

Many of the traffic safety applications being proposed both in the US and in Europe will rely on *ad hoc* communications, i.e., direct vehicle-to-vehicle communications, using the upcoming IEEE 802.11p standard. A typical vehicular *ad hoc* network (VANET) is a spontaneous network with no central mechanism controlling the network resources [19, 20, 21]. This is an advantage for traffic safety applications, since then they do not have to rely on coverage by access points or base stations to function. However, the lack of a central control mechanism implies higher requirements on the distributed, self-organizing algorithms in the nodes, such that they are stable enough to handle all different situations that could arise in the VANET [22]. The VANET, as applied in 802.11p, must self-organize, have support for distributed channel access, use a common frequency channel for communication, and have support for all nodes within radio range. The common frequency channel, here termed control channel, is needed so that every node can follow the data traffic and adapt accordingly. Obviously, more than one communication channel is typically available in a VANET, but the announcement of services on another communication channels is done through the common control channel. Therefore, all nodes must periodically return to the control channel to listen for new messages. This means that the control channel and timely access to it is crucial. In Europe, the control channel will carry the periodic time-triggered position messages, i.e., CAMs, as well as event-driven data traffic such as DNMs.

A VANET provides *ad hoc* communications and thereby potentially lower average delay than centralized networks, since communication takes place directly in-between end nodes. This is an advantage when it comes to traffic safety applications. However, the low average delay should also be maintained even when the network load increases, since the number of participating nodes in a VANET using 802.11p is impossible to predict. For example, a crash on a highway with many lanes could result in a rapidly increasing amount of nodes within radio range in just a couple of seconds. There are different techniques to handle this *scalability* issue in decentralized networks. One way is to use power control: when the nodes “hear” too many other nodes, they can decrease their output power and thus reducing the congestion in the air. On the contrary, if (too) few nodes are heard, an increase in the output power could be made. Note that this requires careful design of the TPC algorithm [23, 24], otherwise the network may start oscillating, i.e., nodes continuously decrease and increase their output power. Another way to handle scalability is to restrict the data traffic injected into the network [25], i.e., cross-layer information is used to inform the application about a detected overloaded situation in the network thereby limiting the data traffic that needs to be communicated to the absolute minimum.

2.2 Communication Requirements

Cooperative ITS applications have diverse communication requirements, especially regarding *reliability* and *delay*. Reliability is coupled with the error probability of packets. Data originating from a phone call can tolerate a lower reliability, implying a higher tolerance for packet loss, but is instead very delay sensitive. Delays larger than 150 ms one way makes the conversation hard to follow. Emailing requires high reliability, and thus packets must be received correctly, but it has less stringent delay requirements, i.e., the email needs not to be delivered before a strict deadline, but rather as soon as possible (best effort), which means retransmissions can be used to increase the reliability. Most wireless technologies have been designed with specific applications in mind and consequently also to meet specific application requirements. For example, mobile telephony has traditionally been developed for voice whereas WLAN is developed with Internet browsing in mind which functions well even for unpredictable delays.

Traffic safety applications, however, differ from most existing applications using wireless communications in that *reliability* and *predictable delay* is now required concurrently. By predictable delay is meant that a message needs to be delivered to the receiver before a predefined deadline. This deadline dependent communications is sometimes termed real-time communications. Basically all traffic safety applications have real-time requirements. Either it is critical that a message reaches its intended recipient before a particular time instant, e.g., before a traffic accident as with event-driven DNMs, or the deadline simply tells us that the message is now expired and no longer of interest, possibly because a newer version is available, as with time-triggered periodic CAMs. Note that besides predictable delay, some traffic safety applications also require a low delay, which further increases the complexity of the problem. Achieving high data reliability in vehicular networks is particularly difficult due to several reasons, e.g., the low heights of the antennas and the high relative speeds [26, 27]. In a VANET where data traffic often is broadcasted, the data reliability is also harder to predict due to the lack of acknowledgment (ACK) messages. This implies higher requirements on the MAC scheme to carefully schedule the transmissions and their power levels to keep the interference in the system as low as possible or alternatively requirements on the applications to adapt the data traffic accordingly.

Scalability is a key concept of cooperative systems and, as mentioned above, it is even more crucial when decentralized vehicular *ad hoc* networks are used [28]. By scalable means that a VANET must support a varying number of nodes without collapsing [29]. In the early stages of ITS introduction, the applications must function even at low penetration rates. Conversely, when the penetration rate, i.e., the number of ITS equipped vehicles, increases the applications must scale without collapsing. The broadcast nature of many ITS realizations together with the highly distributed systems makes the problem even more prominent.

2.3 Performance metrics

A mentioned above, traffic safety applications based on cooperative systems can be classified as real-time communication systems [30], implying demands on *predictable delay* for delivery of messages, i.e., the messages should reach its or their intended recipient(s) before a deadline and with certain *reliability* (error probability). Traditional performance measures generally found in networking, such as throughput [31], are of less importance in a real-time system. This is due to the fact that communicating real-time messages does not necessarily require a high transmission rate or a low delay, but it does require a predictable delay such that the message can be delivered before the deadline with the required error probability. Depending on the application, a missed deadline could potentially have severe consequences for the system or lead to temporarily performance degradation. The *worst case behaviour* is important in real-time communications and therefore the *deadline miss ratio* is a central performance measure. A missed deadline in a wireless broadcast communication system seen from the MAC layer perspective can mainly be caused by two things – the packet was never transmitted or the packet was not received correctly. The deadline miss ratio is consequently the probability that a packet received by the MAC layer from the layer above it does not reach its destination before the deadline expires. Therefore, the deadline miss ratio is closely coupled to the *channel access delay*, i.e., the time it takes from channel access request to actual channel access at the MAC layer. The *worst case channel access delay* is essential and should not exceed the message deadline.

The interference in the wireless systems is one reason for not receiving a packet successfully. The MAC scheme is responsible for scheduling the transmissions to minimize the interference and therefore is the *distance between concurrently transmitting nodes* an important performance measure. The closer two transmitting nodes are in space the higher interference level will be experienced in that area.

Based on ongoing standardization activities, broadcasted periodic position messages, i.e., CAMs, will be of utmost importance for a range of different traffic safety applications. If a channel access request for a CAM never results in actual channel access before the next CAM is generated, the former CAM is thrown away since more recent information is available, i.e., it is dropped at the sending node, and we say that the deadline is missed. Missing a CAM deadline does not necessarily have severe consequences for the application, but merely implies temporary performance degradation. However, if the same node is forced to drop many consecutive packets due to continuously being denied channel access, this can turn into a major problem. When there are few ITS equipped vehicles, there will be many "inherently invisible" vehicles, but as the penetration increases, invisibility due to packet drops turns into a problem. The distributed algorithm that provides channel access therefore needs to be fair, so that potential packet drops affect all network members evenly. Consequently, *fairness* and *scalability* are central properties in a VANET, and therefore e.g., *consecutive deadline misses* (packet drops) from the same node should be considered.

Even though a channel access attempt is successful, the deadline can still be missed due to the unreliable wireless communication channel, i.e., the packet was never successfully decoded at the receiver because of a noisy channel. When considering the receiver side, the traditional performance measure *deadline miss ratio,* derived from the real-time systems area, needs to be redefined for vehicular networks due to the broadcast nature for both event-driven and time-triggered realizations. Successful message reception is a function of the number of vehicles in interest range for the particular traffic safety applications and diverse applications require different interest ranges. The communication range and the interest range do not necessarily coincide, as certain applications require larger interest range than the communication can offer. This problem is often solved using multi-hop schemes, however, this is out of scope of this thesis work.

3 Medium Access Control

The most important component for achieving predictable delays in a communication system is the MAC algorithm, determining who has the right to transmit next on the shared communication channel. The MAC scheme must provide a worst case channel access delay, i.e., the medium access must be predictable. The MAC scheme must also be scalable, such that if a dangerous traffic situation arises and is detected by many vehicles, all DNMs can be sent. Hence, the MAC must be capable of coping with periods of overload while remaining fair. In other words, the MAC scheme is responsible for scheduling all channel access while keeping the interference as low as possible at any transmission moment. The MAC scheme intended for use in VANETs aiming at enhancing traffic safety must be *scalable*, *fair* and *predictable*.

This thesis work explores and investigates two different MAC schemes for vehicular *ad hoc* networks, namely CSMA/CA as defined in IEEE 802.11 [3, 10] and a promising alternative called self-organizing time division multiple access (STDMA). STDMA as outlined in the automatic identification system (AIS) [32] standard is of interest because it is decentralized, predictable, fair and potentially also scalable.

3.1 CSMA of IEEE 802.11p

CSMA is a MAC method that dates back to the 70s and it is an enhanced version of the Aloha protocol [33] from 1970. The Aloha protocol was developed at Hawaii University with the purpose of connecting remote users wirelessly to the university on-campus main frame. In an Aloha network a node sends its data packet as soon as it is generated. The node expects an ACK in return and if this is missing, the node will resend the packet again after it has been waiting for a randomly selected time. Aloha was developed for bursty data traffic, where the reliability was more important than the delay of data packets and therefore a higher reliability was achieved by using retransmissions. The data traffic in ordinary computer networks is bursty and hence random access protocols such as Aloha and its successor CSMA is well suited for this.

In 1973 Robert Metcalfe at Xerox presented the first CSMA algorithm used for wired networks. He dubbed this invention Ethernet. In 1975 Kleinrock and Tobagi [34, 35] made the first thoroughly analysis of the CSMA algorithm for wireless networks. CSMA is an improved Aloha protocol where the transmitter starts by sensing the channel before the transmission is initiated, i.e., “listen before talk”. If the sensing is successful, i.e., no channel activity is detected, the node transmits directly. If the channel becomes occupied during the sensing, the node must perform a backoff procedure. The node does so by randomizing a time that it has to wait before a new sensing is allowed.

The MAC method of the upcoming vehicular communication standard IEEE 802.11p is CSMA/CA derived from the 802.11. The 802.11p will use the QoS amendment 802.11e together with the PHY layer of 802.11a, which is based on orthogonal frequency division multiplexing (OFDM), with some minor changes to fit the high-speed vehicular environment. The 802.11p is designed for 10 MHz wide channels instead of 20 MHz as it is in the original 802.11a. Due to this, the transfer rates will be halved in 802.11p as compared to 802.11a, implying transfer rates of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps. The different transfer rates are obtained through changing modulation scheme and channel code rate. Another major difference in the 802.11p compared to the original 802.11 is that there is no difference between the nodes in the network, i.e., all nodes including roadside units are peers. There exists no access point functionality in 802.11p even though the vehicular network will contain roadside units at certain locations. The roadside units are instead defined at the application layer.

Officially the MAC method of IEEE 802.11p is called enhanced distributed channel access (EDCA), which is the enhanced version of the basic access mechanism in 802.11 using

QoS. This is based on CSMA/CA, meaning that the station starts by listening to the channel, and if it is free for a certain time period, called an arbitration interframe space (AIFS), the sender can transmit directly. If the channel is busy or becomes occupied during the AIFS, the station must perform a backoff, i.e., it has to defer its access for a randomized time period. The QoS in EDCA is obtained by placing the data traffic within each node into four different priority queues. These queues have different AIFS and backoff parameters, i.e., the higher priority, the shorter AIFS and the smaller contention window (*CW*). The backoff procedure in 802.11 works as follows: (*i*) draw an integer from a uniform distribution [0,*CW*], (*ii*) multiply this integer with the *slot time* derived from the PHY layer in use, and set this as the backoff value (*iii*) decrease the backoff value only when the channel is sensed free, (*iv*) upon reaching a backoff value of 0, send immediately. The MAC protocol of 802.11 is a stop-and-wait protocol, and the sender will wait for an ACK. If no ACK is received by the sender for some reason (that the transmitted packet never reached the recipient, the packet was incorrect at reception, or the ACK never reached the sender), a backoff procedure must also be invoked before a retransmission is allowed. For every attempt to send a specific packet, the size of the contention window, *CW*, will be doubled from its initial value (CW_{min}) until it reaches a maximum value (CW_{max}). This is done since during high utilization periods it is convenient to distribute the nodes that want to send over a longer time period. After a successful transmission or when the packet had to be thrown away because the maximum number of retransmission attempts was reached, the *CW* will be set to its initial value again, i.e., $CW=CW_{min}$. In Table 1, default parameter settings for the different queues in 802.11p are found together with the *CW* setting. In a broadcast situation, the receiving nodes will not send ACKs. Therefore, a sender never knows if anyone has received the transmitted packet correctly or not. Due to this, the sender will perform at most one backoff, which occurs when the initial channel access attempt senses a busy channel. Hence, broadcast packets will never experience multiple backoffs, and the contention window will always be CW_{min}. In Figure 1a, a flow diagram presents the CSMA procedure in the broadcast situation with periodic data traffic, i.e., CAMs.

Table 1. Default parameter setting in 802.11p for the EDCA mechanism.

	Queue #1	Queue #2	Queue #3	Queue #4
Priority	Highest		→	Lowest
AIFS	58 *μs*	58 *μs*	71 *μs*	123 *μs*
CW_{min}	3	7	15	15
CW_{max}	511	1023	1023	1023

3.2 STDMA of AIS

The STDMA algorithm presented in this thesis is found in the AIS standard for the shipping industry [32]. There are international regulations saying that ships larger than 300 gross ton must use AIS, which is a transponder technique. Every ship will transmit messages containing information about its position, heading etc., at a predetermined heartbeat rate. The AIS system is used for identifying ships in the vicinity and it is of great help in, e.g., bad weather situation since false radar images are problematic. With AIS, each ship will build its own surveillance picture about the neighbourhood using the messages received from other ships. Ships all over the world can meet and track each other through this system. AIS divides the time into 1 minute frames where each frame contains 2250 time slots and a transfer rate of 9.6 kbps is supported. Two different frequency channels; 161 MHz and 162 MHz, are used for communication and the ships will divide its messages between these two channels (called channel A and channel B). A message is 256 bits long and it fits into one time slot.

STDMA as used in AIS is a decentralized scheme where the network members themselves are responsible for sharing the communication channel. Due to the decentralized network topology, the synchronization among the nodes is done through a global navigation satellite system such as GPS or Galileo. The MAC algorithm is dependent on that all nodes in the network regularly send messages containing information about their own position. The STDMA algorithm will use this position information when choosing transmission slots in the frame. All network members start by determining a report rate, i.e., how many position messages that will be sent during one frame, which translates into the number of slots required in each frame. When a node is turned on, it will follow four different phases; *initialization, network entry, first frame,* and *continuous operation*.

During the *initialization*, the node will listen for the channel activity during one frame to determine the current slot assignments, i.e., listen to the position messages sent in each slot and, by using these, the node builds its own slot map. The position messages contain besides the node's speed, heading, position, also information about the node's future slot allocations.

In the *network entry* phase, the node determines its own slots to use for transmission of position messages within each frame according to the following rules: (*i*) calculate a nominal increment, *NI*, by dividing the number of time slots with the report rate, (*ii*) randomly select a nominal start slot (NSS) drawn from the current slot up to the *NI*, (*iii*) determine a selection interval (SI) of slots as 20% of the *NI* and put this around the NSS, (*iv*) now the first actual transmission slot is determined by picking a slot randomly within SI that is not currently occupied by someone else and this will be the nominal transmission slot (NTS). If all slots within the SI are occupied, the slot used by a station located furthest away from oneself will be chosen.

Upon reaching the first chosen NTS, the station will enter the *first frame* phase where the rest of the transmission slots (NTS), according to the report rate are determined (e.g., a report rate of 10 messages/frame implies 10 NTSs). A *NI* is added to the NSS and a new SI area is made available to choose a slot from. This is repeated until an entire frame has elapsed and all position messages are assigned to a transmission slot. Every node has one NSS and it is used to keep track of when the frame starts for this particular node, i.e., all nodes have their own frame start and they look at the frame as a ring buffer with end followed by start. Modulo operations are used to avoid static numbering of slots. The parameters NSS, NS, SI, and *NI*, are kept constant as long as the node is up and running. However, if the report rate is changed during operation (an increase or a decrease in the number of position messages per frame for some reason) the parameters will be changed since *NI* is dependent on the report rate.

When all slots within one frame duration have been selected, the station will enter the *continuous operation* phase, using the NTSs decided during the *first frame* phase for transmission. However, during the *first frame* phase, the node will also draw a random integer $n \in \{3,...,8\}$ for each NTS. After the NTS has been used for the *n* frames, a new NTS will be allocated in the same SI as the original NTS. This procedure of changing slots after a certain number of frames is done to cater for network changes, i.e., two nodes that use the same NTS which were not in radio range of each other when the NTS was chosen could now have come closer and will then interfere if the NTS allocation was not changed. In Fig. 1b the continuous operation phase of STDMA is depicted. The interested reader is referred to [36, Paper A] for more information about the STDMA algorithm.

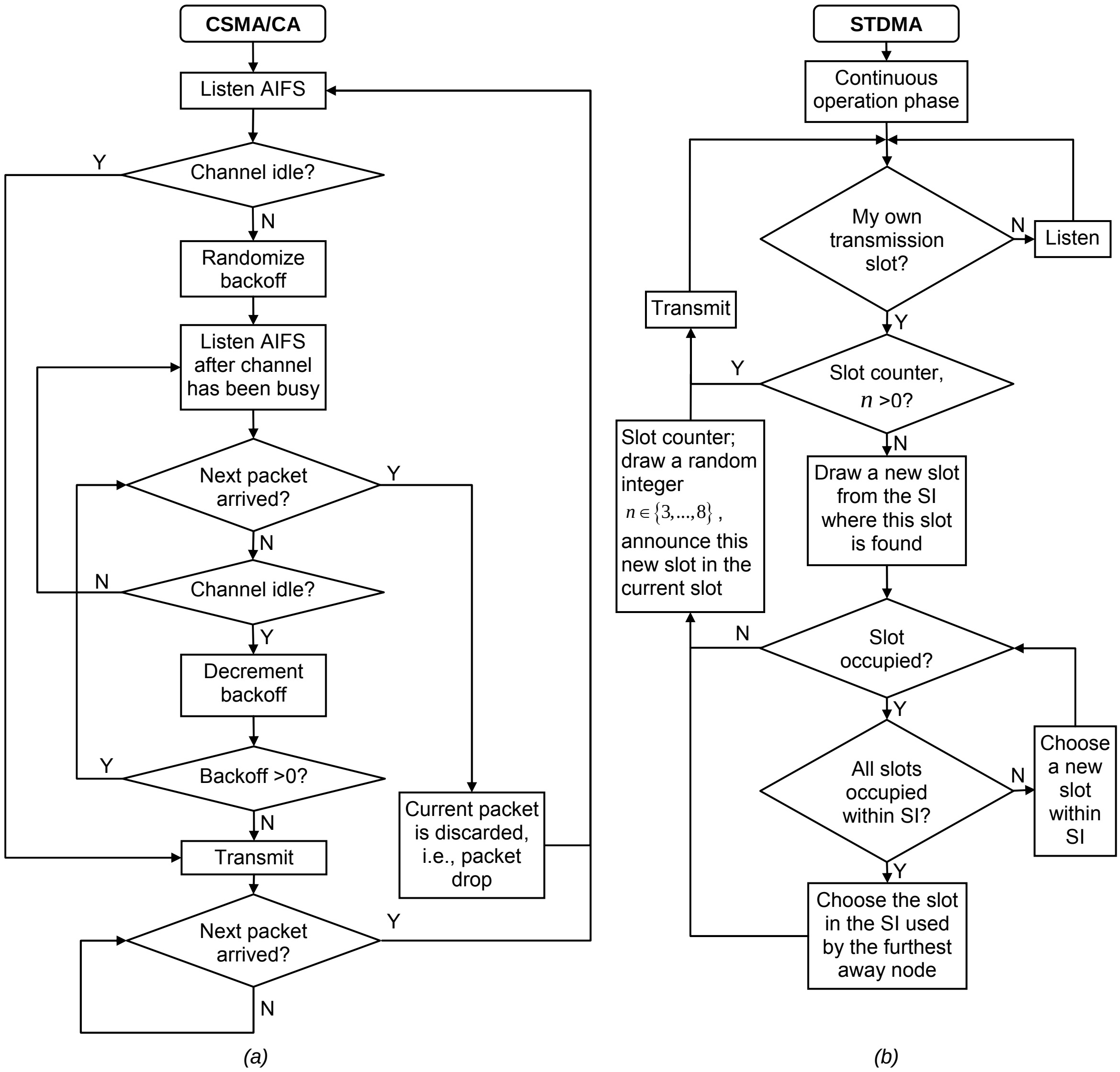

Figure 1. The two MAC procedures examined in this thesis work using a data traffic model with broadcasted time-driven messages at predetermined heartbeat rates; (a) the CSMA procedure according to 802.11p and (b) continuous operation phase of STDMA

4 Motivation, Problem Description and Contributions

Cooperative systems will enhance traffic safety, both for in-vehicle passengers as well as other road-users, through a diverse set of applications. Vehicular communications is considered to be of great importance both in the US, Europe and in Japan, to decrease the number of traffic accidents costing the society an enormous amount of grief and money each year. According to ongoing standardization, several traffic safety applications will rely on the upcoming vehicular communication standard IEEE 802.11p. This standard is based on a vehicular *ad hoc* network lacking a central mechanism for controlling the network resources, and thereby implying distributed channel access and self-organization of nodes. CAMs, broadcasted periodically by every vehicle, will be the foundation for many traffic safety applications in Europe. The CAMs have strict timing requirements, i.e., they must be delivered before a specific deadline (the next updated CAM) otherwise they are of no use. In addition, all vehicles need fair access to the channel to transmit their CAM in order not to become invisible to the vehicles in the vicinity.

Traffic safety applications can be classified as a real-time communication system, having requirements on *predictable delay* but also on high *reliability*. The broadcast nature of traffic safety applications implies requirements on *fairness* and good *scalability*. The MAC method is a key component to grant fair and predictable channel access as well as to provide scalability in decentralized network topologies. The 802.11p uses CSMA/CA as channel access mechanism, which is an inherently *unpredictable* protocol due to the potential random backoff procedure which may lead to *unbounded channel access delays*. In addition, the carrier sensing mechanism preceding each packet transmission implies that there is a competition for the resource, causing problems with *fairness* and *scalability*, e.g., when many nodes simultaneously try to access the wireless channel, some nodes may have to *drop several consecutive packets* since they never got access to the channel before the deadline, whereas other nodes drop none or only very few packets. This problem becomes more severe in heavily loaded networks. Finally, when the channel is busy, the nodes in CSMA must perform a backoff procedure and during high utilization periods this mechanism can cause several nodes within radio range of each other, to transmit concurrently due to the limited discrete random numbers to choose from in the backoff procedure. This also implies problem with *scalability*. In addition, the concurrent transmissions by nodes located closely together decreases the *reliability* of the communications since the interference is not controlled. If channel access cannot be granted in a fair and predictable fashion, the whole idea with cooperative systems for traffic safety fails.

This licentiate thesis work considers communications requirements from traffic safety applications based on VANETs. Based on these requirements, it is concluded that the MAC protocol needs to be decentralized, predictable, fair and scalable. A central contribution of this thesis is therefore the evaluation of the performance of the MAC method of IEEE 802.11p in terms of *channel access delay*, *consecutive packet drops* and *distance between concurrently transmitting nodes*. A computer simulator has been developed to perform the evaluation in terms of scalability, delay and fairness. The chosen scenario is a multi-lane highway since this is believed to be one of the most demanding scenarios for the MAC method. The high dynamics of the network imply that the high relative speeds (up to 300 km/h) will cause vehicles to rapidly move in and out of radio range of each other.

Another key contribution of this thesis work is the suggestion to use STDMA as a remedy to the scalability and predictability problems experienced with CSMA. Regardless of the number of nodes competing for channel access with STDMA, all nodes will always get access within a bounded delay. When two nodes are forced to transmit in the same time slot with STDMA, their transmissions are scheduled so that the concurrently transmitting nodes are separated as far as possible in space, thereby trying to control and minimize the interference in the system. Using STDMA solves the problems with predictability, fairness and scalability found in CSMA. STDMA has been adjusted in this thesis from the AIS setting to the needs of the vehicular environment.

CSMA has been evaluated for VANETs before through computer simulations – but from an average performance viewpoint [37, 38, 39] rather than considering the worst case behaviour. This is mainly due to the fact that CSMA has been considered primarily for applications requiring a good average throughput, rather than predictable delay and fairness among users. This is why the simulator is such an important contribution of this licentiate work. It uses a data traffic model based on CAMs as defined by ETSI and a message arrival rate of the CAMs that is based not only on the period of the actual CAM, but also on a vehicle arrival rate being Poisson distributed. In addition, both MAC methods have been evaluated using the parameters and PHY layer attributes found in 802.11p. An equally important contribution of this thesis is the considered performance metrics: channel access delay, consecutive packet drops and distance between concurrently transmitting nodes which aims to evaluate predictability, fairness and scalability of the system, rather than the throughput. Finally, STDMA has, to the best of the author's knowledge, not previously been considered for, or adapted to the vehicular environment.

4.1 Paper A

In Paper A the simulator is presented and used to evaluate channel access delay on the transmitter side. The simulations have been conducted for a saturated network comparing the MAC method of IEEE 802.11 to the STDMA algorithm in a highway scenario with five lanes in each direction. The results in Paper A show that some of the nodes using CSMA as MAC method can drop up to 80% of the generated packets on the transmitter side (since no channel access was possible for the current packet before a new one appeared at the MAC layer). The node that experienced the highest number of successful channel access attempts drops about 22 % of its packets, so it is quite a big difference between what a node using CSMA could experience in the best and the worst case. Some of the worst affected nodes also dropped more than 100 *consecutive* packets when a heartbeat frequency of 10 Hz was used, implying that those nodes were invisible to their neighbourhood during ten seconds. The conclusion that can be drawn from this is that nodes in a CSMA system can experience *unbounded channel access delay* and that the CSMA algorithm is *not fair* between the nodes since some nodes are punished harder than others. In STDMA all channel access requests result in actual channel access. Therefore, the STDMA algorithm is *predictable and fair*. To compare the two MAC schemes, a new performance measure was introduced: *distance between two concurrently transmitting nodes*. This showed that the probability that two nodes located close to each other would transmit at the same time was considerably higher for CSMA than for STDMA. It can be concluded that the STDMA algorithm is a highly interesting alternative for VANETs since all nodes always get channel access before a predetermined time, regardless of the number of competing nodes.

4.2 Paper B

In Paper B the results from Paper A are used as a starting point when trying to tweak the parameters of the two MAC protocols CSMA and STDMA to improve their respective performance for traffic safety applications. The IEEE 802.11p has support for QoS by means of prioritizing the data traffic in queues within each node. Depending on the priority, the data traffic is put into one of four different queues, where each queue has a different listening period and a different backoff window setting. In Paper A the highest priority was used all the time, implying the shortest listening period and the smallest contention window, but also fewer discrete backoff values to choose from. In Paper B the aim was to improve the fairness of CSMA by adjusting the parameters found in the standard. Simulations were performed with all the different priorities to determine if the performance in terms of *consecutive packet drops* and *channel access time* is affected by this. However, it could be concluded that the priorities do not have much effect when the network is overloaded. An algorithm to enhance the fairness of the CSMA algorithm was then proposed, where nodes receive a higher or lower priority on the current packet depending on if the previous channel access request was successful or not. This algorithm was shown to *enhance the overall fairness of the system* such that the difference between the best case and the worst case channel access delay was reduced and thereby the worst case consecutive packet drops decreased. However, regardless of the parameter settings, CSMA still suffers from unbounded channel access delays and frequent medium access collisions. The performance of STDMA was improved in terms of reduced interference by decreasing the number of consecutive frames that an STDMA node is allowed to use a specific allocated time slot such that the *distance between two concurrently transmitting nodes* was reduced. It was concluded that STDMA has even more to offer if properly adapted to the specific application in question.

4.3 Paper C

In Paper A and Paper B the network was overloaded in terms of nodes and data traffic. In Paper C simulations were instead conducted comparing STDMA with CSMA of IEEE 802.11p *for a network that is not saturated*. Two different CAM packet sizes and update frequencies have been used, inspired by the current proposals for CAMs in Europe (2 Hz, 800 byte) and the heartbeat messages in the US (10 Hz, 300 byte). First we determine the maximum number of vehicles that can be supported for each CAM setting and for each MAC method and term this 100 % network load. Next, we examine the *scalability* of STDMA and CSMA in terms of how far away from the theoretical maximum constituting the 100% that the simulated results are. STDMA being a time slotted method can be expected to handle all data traffic regardless of message arrival distributions. For CSMA to support its 100 % network load, i.e., all deadlines on the CAMs are met, the message arrivals from all nodes need to be uniformly distributed. If all time-triggered messages start at the same time instant, CSMA performance is at its worst from a concurrent transmission point of view. At a network load of 80% CSMA resolves all channel access requests to channel access, however, up to 10% of the transmissions take place concurrently. With CSMA there is a very high probability that concurrently transmitting nodes are located close to each other. This is due to nodes starting their listening periods at the same time and thereby transmitting at the same time, or nodes choosing the same backoff value which also results in transmitting at the same time instant. This does not happen with STDMA and thus also in not saturated networks STDMA outperforms CSMA when considering the performance measure *the distance between concurrently transmitting nodes*. In an attempt to reduce the amount of concurrently transmitting nodes in CSMA, simulations have been conducted with an increased backoff window. This results in slightly more packet drops at the sending side, but fewer concurrent transmissions. For a moderately loaded network packet drops with CSMA is scarce and therefore there is almost the same amount of transmissions in the air for both the CSMA and STDMA. The major difference therefore lies in where in space concurrent transmissions take place – in CSMA it is random and in STDMA it is properly scheduled due to the side information from the position messages.

5 Discussion and Outlook

A considerable amount of work therefore remains before the launch of truly *predictable*, *reliable* and *scalable* traffic safety applications is a reality. As the IEEE 802.11p is designed today, there are no restrictions regarding the amount of generated data traffic or the number of nodes constituting the VANET. To partly overcome the drawbacks of CSMA as identified in this thesis work, there is a proposal in Europe within ETSI TC ITS not to load the control channel with more than 25% data traffic. Any node detecting that the control channel is occupied during periods that amount to more than 25% has to decrease its output power and/or generated data traffic, i.e., TPC and DCC mechanisms.

The first generation of VANETs currently being standardized will be based on IEEE 802.11p. It is likely to function satisfactorily since the penetration rate will be low in the beginning and the MAC method of 802.11 was originally designed for such lightly loaded networks. As the penetration increases the scalability issue will turn into a major problem. One interesting continuation of the work carried out in this thesis would therefore be to study a migration path from CSMA to STDMA for VANETs. STDMA can handle overloaded situations but requires a tighter synchronization through GPS or Galileo. This requirement in STDMA has not yet been studied for the vehicular environment. The worst thing that could happen in STDMA is to lose the synchronization, but then the STDMA system could fallback to become a CSMA system and thus would never perform worse than this. Based on the results presented in this thesis, ETSI TC ITS has proposed to create a specialist task force (STF) for further investigations of STDMA for traffic safety applications.

The next step in this work is to study the performance measures on the receiving side by adding a realistic channel model based on real measurements to the simulator. The channel models for centralized networks are well studied and there exist many really good models when one of the two communicating parties is stationary with medium and high antenna heights. However, when two moving nodes communicate is harder to study due to, e.g., the quite low antenna heights and all possible vehicular scenarios that exist. The existing performance measure for the receiving side must be further investigated and defined to suit the broadcast nature of VANETs, where different safety applications have different interest range.

The use of STDMA solves the problems with predictability, fairness and scalability with CSMA – by reliability remains. The periodic nature of the CAMs implies that the report rate could simply be increased when an increased reliability is needed, but this is not necessarily the case for DNM that are broadcasted only in the event of a hazard. Retransmission schemes are traditionally used in unicast transmissions as a tool to increase the reliability, however, this is a less tractable option in broadcast scenario. Therefore other methods must be used to increase the reliability. One way is of course to use a fair and predictable MAC scheme such as STDMA that schedules transmissions as far apart as possible resulting in increased reliability for the nodes situated closest to the transmitter. However, to further enhance the reliability cooperative communications could be used and supported at the MAC layer.

References

[1] Ian Catling ed., *Advanced Technology for Road Transport: IVHS and ATT*, Artech House, US, 1994.

[2] FCC homepage, http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1999/fcc99305

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

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

[5] IEEE Std. 1455-1999, *IEEE Standard for Message Sets for Vehicle/Roadside Communications*, 1999.

[6] IEEE Std. 1609.1-2006, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment (WAVE) – Resource Manager*, 2006.

[7] IEEE Std. 1609.2-2006, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment (WAVE) – Security Services for Applications and Management Messages*, 2006.

[8] IEEE Std. 1609.3-2007, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment (WAVE) – Networking Services*, 2007.

[9] IEEE Std. 1609.4-2006, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment (WAVE) – Multi-channel Operation*, 2006.

[10] IEEE 802.11p/D7.0, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 7: Wireless Access in Vehicular Environment*, Draft 7.0, May 2009.

[11] CALM homepage, http://www.calm.hu

[12] ETSI homepage, http://www.etsi.org

[13] COMeSafety project, http://www.comesafety.org

[14] CVIS homepage, http://www.cvisproject.org

[15] Safespot's homepage, http://www.safespot-eu.org

[16] Pre-Drive C2X, http://www.pre-drive-c2x.org

[17] COMeSafety document, http://www.comesafety.org/uploads/media/COMeSafety_DEL_D31_EuropeanITSCommunicationArchitecture_v2.0_01.pdf

[18] Car-to-car communication consortium, http//www.car-to-car.org

[19] H. Füssler, S. Schnaufer, M. Transier, and W. Effelsberg, "Vehicular ad hoc networks: from vision to reality and back," in *Proc. of the 4th annual Conf. on Wireless on Demand Network Systems and Services*, Obergurgl, Austria, pp. 80-83, Jan. 2007.

[20] H. Hartenstein and K. P. Lamberteaux, “A tutorial survey on vehicular ad hoc networks,”, in *IEEE Communications Magazine*, vol. 46, no. 6, June 2008, pp. 164-171.

[21] S. Yousefi, M. S. Mousavi, and M. Fathy, “Vehiuclar ad hoc networks (VANETs): challenges and perspective,” in *Proc. of the 6th Int. Conf. on ITS Telecommunications*, Chengdu, China, pp. 761-766, June 2006.

[22] J. J. Blum, A. Eskandrian, and L. J. Huffman, ”Challenges of intervehicle ad hoc networks,” in *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, 2004, pp. 347-351.

[23] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, “Fair sharing of bandwidth in VANETs,” in *Proc. of the 2nd ACM Int. Workshop on Vehicular Ad Hoc networks*, Cologne, Germany, pp. 49-58, Sept. 2005.

[24] M. Artimy, W. Robertson, and W. Phillips, “Assignment of dynamic transmission range based on the estimation of vehicle density,” in *Proc. of the 2nd ACM Int. Workshop on Vehicular Ad Hoc networks*, Cologne, Germany, pp. 40-48, Sept. 2005.

[25] L. Wischhof and H. Rohling, “Congestion control in vehicular ad hoc networks,” in *Proc. of the IEEE Int. Conf. on Vehicular Electronics and Safety*, Xian, China, pp. 58-63, Oct. 2005.

[26] A. Molisch, F. Tufvesson, J. Kåredal, and C. Mecklenbräuker, ”Propagation aspects of vehicle-to-vehicle communications – an overview,” in *Proc. of IEEE Radio and Wireless Symposium*, San Deigo, CA, US, pp. 179-182, Jan. 2009.

[27] A. Thiel and O. Klemp, “Initial results of multielement antenna performance in 5.85 GHz vehicle-to-vehicle scenarios,” in *Proc. of the 2008 European Conf. on Wireless technology*, Amsterdam, Netherlands, Oct. 2008.

[28] T. Kosch, C. J. Adler, S. Eichler, C. Schroth, and M. Strassberger, “The scalability problem of vehicular ad hoc networks and how to solve it,” in *IEEE Wireless Communications*, vol. 13, no. 5, Oct. 2006, pp. 22-28.

[29] B. Clifford Neumann, “Readings in distributed computing systems,” in chapter *Scale in Distributed*, IEEE Computer Society, Los Alamitos, CA, 1994, pp. 463-489.

[30] C. M. Krishna and K. G. Shin, *Real-time Systems*, McGraw-Hill, New York, 1997.

[31] A. S. Tannenbaum, *Computer Networks*, 4th ed., Pearson Education Int., New Jersey, US, 2003.

[32] Recommendations ITU-R M.1371-1, *Technical Characteristics for Universal Shipborne Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Band*, 2001.

[33] N. Abramson, “The Aloha system – another alternative for computer communications,” in *Proc. AFIPS Joint Computer Conferences*, Houston, Texas, US, Nov. 1975, pp. 281-285.

[34] L. Kleinrock and F. A. Tobagi, “Packet switching in radio channels: part I - carrier sense multiple access modes and their throughput-delay characteristics,” in

IEEE Transaction on Communications, vol.23, no. 12, pp. 1400-1416, Dec. 1975.

[35] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: part II – the hidden node terminal problem in carrier sense multiple access and busy tone solutions," in *IEEE Transactions on Communications*, vol. 23, no. 12, pp. 1417-1433, Dec. 1975.

[36] R. Kjellberg, *Capacity and Throughput Using Self Organized Time Division Multiple Access VHF Data Link in Surveillance Applications*, Master's Thesis, The Royal Institute of Technology, Stockholm, Sweden, April 1998.

[37] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proc. of the 66th IEEE Vehicular Technology Conference*, pp. 2199-2203, Baltimore, MD, US, Sept-Oct 2007.

[38] M. Torrent-Moreno, *Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment*, PhD dissertation, University of Karlsruhe, Germany, 2007.

[39] M. Wellens, B. Westphal, and P. Mähönen, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios," in *Proc. of the 65th IEEE Vehicular Technology Conference*, pp. 1167-1171, Dublin, Ireland, April 2007.

Part II

In Part II the following appended papers are found.

[Paper A] 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 communication,” in *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 902414, 13 pages, doi:10.1155/2009/902414.

[Paper B] K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, “On the ability of IEEE 802.11p and STDMA to provide predictable channel access,” in *Proc. of 16th World Congress on ITS,* Stockholm, Sweden, Sept. 2009.

[Paper C] K. Sjöberg Bilstrup, E. Uhlemann, and E. G. Ström, “Scalability issues for the MAC methods STDMA and CSMA/CA of IEEE 802.11p when used in VANETs,” submitted to *IEEE International Conference on Communications, ICC2010*, Cape Town, South Africa, May 2010.

Paper A

Katrin Bilstrup, Elisabeth Uhlemann, Erik G. Ström, and Urban Bilstrup

On the ability of the 802.11p MAC method and STDMA to support real-time vehicle-to-vehicle communication

EURASIP Journal on Wireless Communications and Networking

Vol. 2009, Article ID 902414, 13 pages

Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 902414, 13 pages
doi:10.1155/2009/902414

Research Article

On the Ability of the 802.11p MAC Method and STDMA to Support Real-Time Vehicle-to-Vehicle Communication

Katrin Bilstrup,[1,2] Elisabeth Uhlemann,[1,3] Erik G. Ström,[1,2] and Urban Bilstrup[1]

[1] *Centre for Research on Embedded Systems, Halmstad University, P.O. Box 823, 301 18 Halmstad, Sweden*
[2] *Department of Signals and Systems, Chalmers University of Technology, 412 96 Göteborg, Sweden*
[3] *Transport, Information and Communication M1.6, Volvo Technology Corporation, 405 08 Göteborg, Sweden*

Correspondence should be addressed to Katrin Bilstrup, katrin.bilstrup@hh.se

Received 1 May 2008; Revised 17 October 2008; Accepted 7 December 2008

Recommended by Onur Altintas

Traffic safety applications using vehicle-to-vehicle (V2V) communication is an emerging and promising area within the intelligent transportation systems (ITS) sphere. Many of these new applications require real-time communication with high reliability, meaning that packets must be successfully delivered before a certain deadline. Applications with early deadlines are expected to require direct V2V communications, and the only standard currently supporting this is the upcoming IEEE 802.11p, included in the wireless access in vehicular environment (WAVE) stack. To meet a real-time deadline, timely and predictable access to the channel is paramount. However, the medium access method used in 802.11p, carrier sense multiple access with collision avoidance (CSMA/CA), does not guarantee channel access before a finite deadline. In this paper, we analyze the communication requirements introduced by traffic safety applications, namely, low delay, reliable, real-time communications. We show by simulation of a simple, but realistic, highway scenario, that vehicles using CSMA/CA can experience unacceptable channel access delays and, therefore, 802.11p does not support real-time communications. In addition, we present a potential remedy for this problem, namely, the use of self-organizing time division multiple access (STDMA). The real-time properties of STDMA are investigated by means of the same highway simulation scenario, with promising results.

1. Introduction

Some of the new, emerging applications for enhancing traffic safety found within the intelligent transportation systems (ITS) sphere can be classified as real-time systems, that is, the transmitted messages have deadlines. In addition, requirements on high reliability and low delay are imposed on the wireless communication systems in use. For example, it is vital that an event-driven message reaches its intended recipient(s) before a particular time instant, for example, before a traffic accident. Information that is delivered correctly, but after the deadline in a real-time communication system, is not only useless, but can also have severe consequences for the traffic safety system. This problem has been pointed out also in [1–3]. In most cases, the extremely low delays required by traffic safety applications imply the need for ad hoc network architectures, supporting direct vehicle-to-vehicle (V2V) communication in peer-to-peer mode. The IEEE 802.11p draft standard, intended for V2V ad hoc communication in high-speed vehicular environments, has received a lot of attention since its project authorization request (PAR) was approved by IEEE [4], which states amongst other things that multiple data exchanges should be completed within 50 milliseconds time frames.

The original IEEE 802.11, intended for wireless local area networking (WLAN), has two well-known drawbacks within its medium access control (MAC) technique carrier sense multiple access (CSMA): it can cause unbounded delays before channel access as well as collisions on the channel. The MAC protocol decides who has the right to transmit next on the shared communication channel. In a carrier sense system, such as CSMA, the node first listens to the channel and if the channel has been free for a certain time period, the node transmits directly with the implication that another node can have conducted the exact same procedure, resulting in a collision on the channel. Moreover, a node can experience very long channel access delays due to the risk of the channel being busy during its listening period. These two phenomena occur primarily during high utilization periods in the network. CSMA is used by the whole IEEE 802.11 family as well as its wired counterpart IEEE 802.3 Ethernet. One of the reasons for the success of both WLAN and Ethernet is the straightforward implementation of the standard resulting in reasonably priced equipment. Due to this WLANs and Ethernet are often applied to other domains than they originally were designed for. Even though CSMA is unsuitable for real-time communication because of the unbounded channel access delays, Ethernet has paved its way into the industrial communication scene where many real-time systems are found. However, the problems with the MAC method can be solved here by introducing more network equipment, such as switches and routers, and thereby reducing the number of nodes competing for the shared channels, that is, breaking up collision domains. In the wireless domain, however, there is no such easy solution since the wireless channel has to be shared by all users. Further, when the CSMA algorithm is applied in the wireless domain, an interferer could easily jam a geographical area, intentionally or unintentionally, and the nodes in this area would defer their access even though there is no “real” data traffic present. A wireless carrier sense system is thus more susceptible to interference since no access will occur as long as activity is detected on the channel.

The upcoming standard IEEE 802.11p, intended for vehicular ad hoc networks (VANET), will use CSMA as its MAC method, despite its inability to support real-time deadlines. The argument is that the problems with CSMA are most pronounced at high network loads, and traffic smoothing can be introduced to keep the data traffic at an acceptable level. However, traffic smoothing is typically used in centrally controlled networks or networks in restricted geographical areas. A VANET is neither a restricted geographical area, nor can it be made predictable by a central controller due to its highly dynamic characteristics and requirements on low delay. In addition, traffic smoothing only reduces the average delay, and the main problem with unbounded worst case delay remains. A remedy to the problem with potentially unbounded channel access delays when using CSMA could be to use a self-organizing time division multiple access (STDMA), a decentralized, yet predictable, MAC method with a finite channel access delay, making it suitable for real-time ad hoc vehicular networks. An STDMA algorithm is already in commercial use in a system called automatic identification system (AIS), where it focuses on collision avoidance between ships.

This paper analyzes the particular communication requirements introduced by traffic safety applications, namely, low-delay, reliable, real-time communications. The requirement on low delay implies the need for an ad hoc V2V network, whereas the reliability constraint poses high demands on the physical layer in terms of adaptive channel coding and modulation. The ad hoc network together with the real-time constraints requires a decentralized predictable MAC method capable of meeting real-time deadlines. We compare two MAC methods: CSMA of 802.11p and STDMA of AIS in terms of channel access delays by means of simulating a highway scenario. We have selected a data traffic scenario that is typically found in traffic safety applications: time-triggered periodic position messages having deadlines such that they expire when the next updated message arrives. The predictability in terms of channel access delays and the distance to concurrent transmitters are evaluated from the perspective of the sending node.

Related research is presented next in this paper in Section 2, followed by an introduction to real-time communication systems in Section 3 and the importance of the MAC method in Section 4. The paper continues with a performance comparison of CSMA and STDMA for real-time V2V communications by means of computer simulations in Section 5, followed by our conclusions in Section 6.

2. Related Work

The MAC schemes in the literature that are targeting VANETs can be divided into two classes: CSMA-based and TDMA-based. The CSMA-based protocols considered, for example, in [5, 6] are enhanced by providing different priority levels allowing packets with higher priorities to have shorter listening period before a channel access attempt is made. However, the channel may still be busy and when it is, a transmitter with higher priority traffic will randomize a shorter backoff time than transmitters with lower priority traffic. This type of prioritization mechanism where the delay before channel access together with the backoff time is manipulated according to packet priorities is also found in the standard IEEE 802.11e which is included in IEEE 802.11p. In [5], there is also an additional feature where a potential transmitter sends a busy tone using a reserved frequency to get the attention from the intended recipient, which then polls the busy tone sender. However, busy tones and prioritizing packets do not eliminate the problem and there is still no upper bound on when channel access can take place.

The TDMA-based protocols in [7–10] use time slots to achieve collision-free transmissions of data. The difference between these protocols lies in how they assign their time slots. In [7, 8], space division multiplexing (SDM) is used, where the road is first divided into spaces, and within each space a TDMA scheme is mapped. Each vehicle will use different time slots depending on where it is currently situated. This approach is promising but likely to be impractical in a real system. The overall network utilization will be low since many time slots are unused when the vehicle traffic is sparse. The authors of [7, 8] do propose algorithms for increasing the time slot usage, but other problems remain. For example, a spatial division of each road needs to be set up, possibly offline. In [9], the 3G radio interface UMTS terrestrial radio access time division duplex (UTRA TDD) is used as physical layer (PHY), and at the MAC level, the available time is also divided into slots. To achieve a transmission opportunity in the TDMA frame in [9, 10], a random access channel (i.e., CSMA) is deployed. The request for time slots during high utilization periods on a contention-based random access channel will face the same problem as in [5, 6]. Another drawback with almost all of the above MAC protocols [5, 6, 9, 10] proposed for the vehicular environment is that they do not incorporate the dynamics of the network and, therefore, they are still only applicable to slow moving objects and ordinary ad hoc networks.

The physical layer (PHY) of the upcoming IEEE 802.11p and its capabilities has been treated in a series of articles [11–13]. The investigation of the PHY is very important to increase the transmission reliability, but still if no channel access is possible, we will never use the PHY facilities. Enhancements to the MAC layer of 802.11p have been suggested and evaluated in [14–16], which all have in common that they want to decrease the data traffic load by, for example, prioritizing better. An attempt to avoid packet collisions by using a polling scheme is suggested in [14]. However, none of these articles clearly points out the MAC layer to be the weak part of 802.11p in order to support emerging traffic safety systems with low-delay real-time requirements. The direct communication enabled by the ad hoc mode and the prioritization does decrease the average delay, but the worst case collision scenario is still the same. In [17], a reliability analysis of the 802.11p is made from an application and a communication point of view. No enhancements are suggested, but the 802.11p together with real-world application data traffic was evaluated and found to provide sufficient reliability. However, the real-world data was collected when three vehicles in a highway scenario were communicating, which has to be regarded as a very lightly loaded system. In such a scenario with few competing nodes, almost any type of MAC method will function satisfactory. A more realistic setting with more communicating nodes is likely to stress the MAC method further. An analytical performance evaluation of 802.11p together with simulations is presented in [18]. It is concluded that 802.11p cannot ensure time-critical message dissemination and that the solution ought to be a reduction in the number of high priority messages.

3. Real-Time Communication

Real-time communication implies that the communication task has demands on timely delivery, that is, messages should reach their intended recipients before a certain deadline in time and with a certain reliability (error probability). Communicating real-time messages does not necessarily require a high transmission rate or a low delay, but it does require a predictable behavior such that the message is delivered before the deadline with the requested error probability. Therefore, real-time communication tasks are characterized by two important parameters: *deadline* and *reliability* [19]. Depending on the application, a missed deadline could potentially have severe consequences for the system user or simply lead to temporarily performance degradation. Emerging traffic safety systems based on vehicular communication are real-time systems in accordance with the above classification. Examples of real-time deadlines within traffic safety applications are lane-change warnings, rear-end collision warnings, and conveying slippery road conditions, all of which include messages which must reach the intended recipients before the event takes place.

A Voice over IP (VoIP) conversation over the Internet is an example of a real-time system that has data packets with deadlines since it is better to drop VoIP packets that are late than to introduce longer and longer delays. The antilock braking system (ABS) in a vehicle is another example of a real-time system; but contrary to the VoIP application, the requirement on error probability is significantly higher in this control application and also packets delivered shortly after the deadline could be used with diminishing returns. Consequently, applications have different requirements on the values of the parameters *deadline* and *reliability*, for example, a VoIP conversation can tolerate packet losses, implying relaxed constraints on reliability, but puts stringent demands on keeping the deadlines and in the ABS case it is almost the other way around. Vehicle safety systems, communicating to avoid or mitigate traffic accidents, are real-time systems where it is equally important that the packet loss rate is close to zero (high reliability) as it is to keep the deadlines. One way to improve the ability of the real-time communication system to meet deadlines is to prioritize the data traffic to provide classes of different importances, but obviously if all nodes in the network have traffic from the same priority class to transmit this will not have any effect.

Real-time communication systems are a mature research area within, for example, wired industrial networks and there exists a plethora of standards intended for real-time communication in industrial environments, for example, fieldbuses [2] or control networks [20], often with its own manufacturer. Since the industrial communication society has not agreed upon one common network technology, the local area network (LAN) standard Ethernet has won terrain due to its affordable equipment and the literature about the use of Ethernet in industrial environments is vast, for example, [21–23]. An attempt to make Ethernet predictable and more suitable for real-time traffic is RETHER [21], where a token ring-based protocol is used on top of the normal CSMA protocol. Despite the MAC method being CSMA, Ethernet can be used in industrial real-time applications due to the following reasons: (i) an industrial network is a controlled environment where the number of network members is known in advance, (ii) the controlled environment also implies that the data traffic including priorities is known or can be determined in the worst case, and (iii) the communication takes place via a wire implying significantly lower bit error rates than for wireless communication. These three things help the designer to either keep the network load low such that we are not operating close to what the network can handle or to introduce real-time enhancements to CSMA possible in stationary networks, such as token ring.

One of the most important parts of a real-time communication system is the MAC method. In this paper, we are investigating the ability of a sending node to get access to the channel within a finite upper bound. Therefore, we define the *MAC channel access delay* as the time it takes from when a packet arrives to the MAC from the layer above it, until the packet is delivered to the PHY layer for transmission. For brevity, we also denote the MAC channel access delay by T_{acc}. An MAC method is defined to be *deterministic* if the worst case MAC channel access delay is finite. A nondeterministic MAC method (i.e., an MAC method for which T_{acc} is not finite) is unsuitable for real-time data traffic having deadlines. The set of deterministic MAC methods includes master-slave schemes, token passing schemes, TDMA, frequency division multiple access (FDMA), and code division multiple access (CDMA). These methods are well suited for real-time data traffic but they typically require a central coordinator that can distribute channel resources among the users (i.e., allot time slots/frequency bands/spreading codes). CSMA, on the other hand, is easily deployed in decentralized, ad hoc networks but is also nondeterministic. VANET is a special case of ad hoc networks and is characterized by the fact that the nodes constituting the VANET are highly mobile and can reach very high speeds. This mobility has a great impact on the choice of MAC scheme, since it must be designed to cope with rapid changes in the network topology, where communication links constantly form and break. The problem with VANETs is threefold; (i) it is hard to foresee the number of members of the network, (ii) it is hard to predict the amount of data traffic generated by the nodes, that is, the aggregated bandwidth, and (iii) the wireless channel is stochastic and time-varying in its nature and influenced by many parameters. In a static wireless ad hoc network, (i) and (ii) could be controlled but (iii) remains a challenge. Coding and diversity schemes play a vital role to increase the data reliability and mitigate the effects of fading and interference of the channel, but before these techniques can be applied, a transmission must take place, that is, the node must get access to the channel.

4. The 802.11p and STDMA MAC Methods

In this paper, we analyze the real-time properties of two MAC methods: CSMA of 802.11p and STDMA of AIS. Since CSMA is nondeterministic, we are interested in knowing how it is affected by the network load, that is, how many deadlines are missed when the network load increases? STDMA, on the other hand, being deterministic, we are interested in knowing any potential drawbacks such as increased interference. This section describes the functionality of the two MAC methods.

4.1. The MAC method of 802.11p. Wireless access in vehicular environment (WAVE) is the protocol stack concept for the vehicular environment developed by IEEE. It contains an MAC and PHY layer derived from IEEE 802.11 [24], a new transport/network layer protocol (IEEE 1609.3), security issues specified in 1609.2, and an application protocol called 1609.1. The MAC method of the upcoming standard IEEE 802.11p is a CSMA/CA derived from the 802.11, and 802.11p will also use the quality-of-service (QoS) amendment 802.11e, Figure 1. The PHY layer of 802.11p is the 802.11a, based on orthogonal frequency division multiplexing (OFDM), with some minor changes to fit the high-speed vehicular environment. The 802.11p together with the 1609.4 standard is designed for 10 MHz wide channels instead of 20 MHz as it is in the original 802.11a. Due to this, the transfer rates will be halved in 802.11p compared to 802.11a, implying transfer rates of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps. The different transfer rates are obtained through changing modulation scheme and channel code rate. Another big difference in the 802.11p compared to the original 802.11 is that there is no difference between the nodes in the network, that is, all nodes are peers including the roadside units. There exists no access point functionality in 802.11p even though the vehicular network will contain roadside units at certain spots.

IEEE 802.11p will use enhanced distributed channel access (EDCA) from the QoS amendment IEEE 802.11e [25] as MAC method, which is an enhanced version of the basic distributed coordination function (DCF) found in 802.11. The DCF is based on CSMA/CA, meaning that the station starts by listening to the channel, and if it is free for a time period called an arbitration interframe space (AIFS), the sender can start transmitting directly. If the channel is busy or becomes occupied during the AIFS, the station must perform a backoff, that is, the node has to defer its access according to a randomized time period. In 802.11p, QoS is obtained by putting the data traffic within each node into four different priority queues. These queues have different AIFS and backoff parameters, that is, the higher priority, the shorter AIFS. The backoff procedure in 802.11 works as follows: (i) draw an integer from a uniform distribution $[0, CW]$, where *CW* refers to the current contention window, (ii) multiply this integer with the *slot time* derived from the PHY layer in use, and set this as the backoff value, (iii) decrease the backoff value only when the channel is free, (iv) upon reaching a backoff value of 0, send immediately. The MAC protocol of 802.11 is a stop-and-wait protocol and the sender will wait for an acknowledgment (ACK). If no ACK is received by the sender for some reason (that the transmitted packet never reached the recipient, the packet was incorrect at reception, or the ACK never reached the sender), a backoff procedure must also be invoked. For every attempt to send a specific packet, the size of the contention window, *CW*, will be doubled from its initial value ($CW_{\min}$) until it reaches a maximum value ($CW_{\max}$). This is done since during high utilization periods, it is convenient to distribute the nodes that want to send over a longer time period. After a successful transmission or when the packet had to be thrown away because the maximum number of channel access attempts was reached, the contention window will be set to its initial value again. In Table 1, default parameter settings for the different queues in 802.11p are found together with the *CW* setting. In a broadcast situation, the receiving nodes will not send ACKs. Therefore, a sender never knows if anyone has received the transmitted packet correctly or not. Due to this, the sender will perform at most one backoff, which occurs when the initial channel access attempt senses a busy channel. Hence, broadcast packets will never experience multiple backoffs, and the contention window will always be $CW_{\min}$. In Figure 2(a), a flow diagram presents the CSMA procedure in the broadcast situation with periodic traffic.

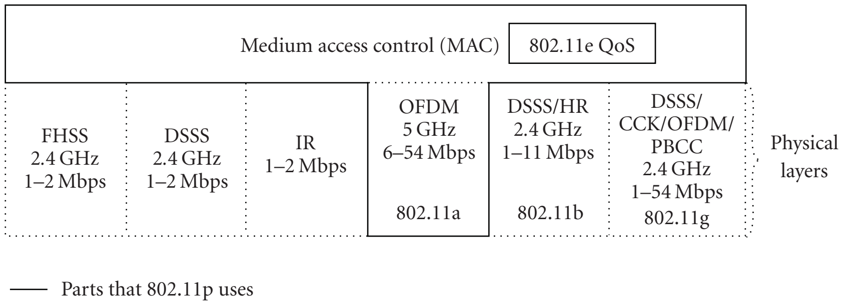

FIGURE 1: An overview of the WLAN family 802.11, showing in bold which parts that 802.11p will use and modify.

TABLE 1: Default parameter settings in 802.11p for the different queues.

	Queue no. 1	Queue no. 2	Queue no. 3	Queue no. 4
Priority	Highest	⟶		Lowest
AIFS	34 μs	34 μs	43 μs	79 μs
CW_{start}	3	7	15	15
CW_{end}	511	1023	1023	1023

4.2. Self-Organizing TDMA. The STDMA algorithm presented herein is found in a standard for the shipping industry, automatic identification system (AIS) [26]. There are international regulations saying that ships larger than 300 gross ton must use AIS, which is a transponder technique. Every ship will transmit messages containing information about its position, heading, and so on, at a predetermined heartbeat rate. The AIS system is used for identifying ships in the vicinity and it is of great help in, for example, bad weather situation since false radar images are a problem. With AIS, the ship will build its own surveillance picture about the neighborhood using the messages received from other ships. Ships all over the world can meet and track each other through this system. AIS divides the time into one minute frames where each frame contains 2250 time slots and a transfer rate of 9.6 kbps is supported. Two different frequency channels, 161 MHz and 162 MHz, are used for communication and the ships will divide its messages between these two channels (called channel A and channel B). A message is 256 bits long and it fits into one time slot.

STDMA [26] is a decentralized scheme where the network members themselves are responsible for sharing the communication channel and due to the decentralized network topology, the synchronization among the nodes is done through a global navigation satellite system such as GPS or Galileo. The algorithm is dependent on that all nodes in the network regularly send messages containing information about their own position. The STDMA algorithm will use this position information when choosing slots in the frame. All network members start by determining a report rate, that is, deciding the number of position messages that will be sent during one frame and this translates into the number of slots required in ditto. When a node is turned on, four different phases will follow: *initialization, network entry, first frame*, and *continuous operation*. During the *initialization*, the node will listen for the channel activity during one frame to determine the slot assignments, that is, listen to the position messages sent in each slot. In the *network entry* phase, the station determines its own slots to use for transmission of position messages within each frame according to the following rules: (i) calculate a nominal increment, NI, by dividing the number of time slots with the report rate, (ii) randomly select a nominal start slot (NSS) drawn from the current slot up to the NI, (iii) determine a selection interval (SI) of slots as 20% of the NI and put this around the NSS according to Figure 3, (iv) now the first actual transmission slot is determined by picking a slot randomly within SI that is not currently occupied by someone else and this will be the nominal transmission slot (NTS). If all slots within the SI are occupied, the slot used by a station located furthest away from oneself will be chosen. Upon reaching the first chosen NTS, the station will enter the *first frame* phase where the rest of the report rate decided transmission slots (NTSs) are determined (e.g., a report rate of 10 messages/frame implies 10 NTSs). An NI is added to the NSS and a new SI area is made available to choose a slot from. This is repeated until a frame has elapsed and all position messages are assigned a transmission slot, Figure 3. Every node has only one NSS and this is used to keep track of when the frame starts for this particular node, that is, all nodes keep track of its own frame and they look at it as a ring buffer with no start and no end. Modulo operations are used to avoid static numbering of slots. The parameters NSS, NS, SI, and NI are kept constant as long as the node is up running. However, if the report rate is changed during operation (increased or decreased number of position messages in the frame for some reason) then the parameters will be changed since NI is dependent on the report rate.

When all slots within one frame duration are selected, the station will enter the *continuous operation* phase, using the NTSs decided during the *first frame* phase for transmission. During the *first frame* phase, the node will draw a random integer $n \in \{3, \ldots, 8\}$ for each NTS. After the NTS has been used for the n frames, a new NTS will be allocated in the same SI as the original NTS. This procedure of changing slots after a certain number of frames is done to cater for network changes, that is, two nodes that use the same NTS which were

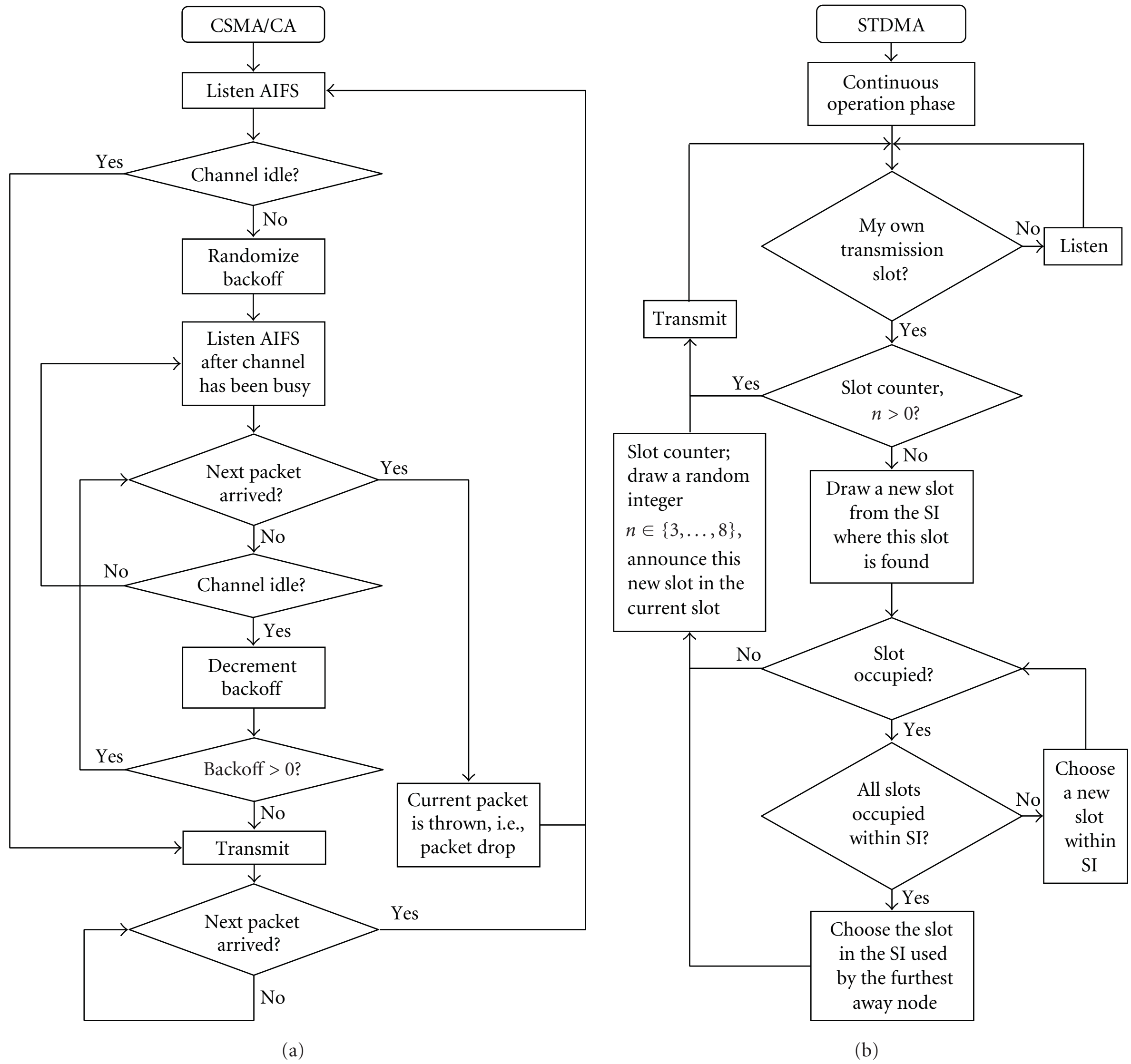

Figure 2: The two MAC procedures examined in this paper using a data traffic model with broadcasted time-driven messages at predetermined heartbeat rates, (a) the CSMA procedure according to 802.11p and (b) continuous operation phase of STDMA.

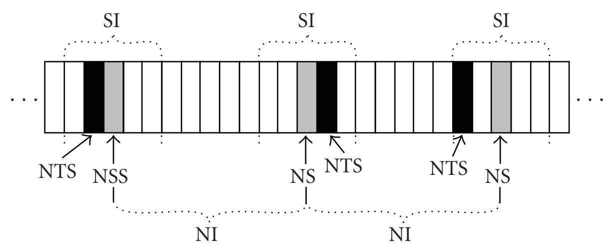

Figure 3: The frame structure for one node. The NSS and NSs are equally spaced with an interval of size NI. The SI parameter is also fixed.

not in radio range of each other when the NTS was chosen could now have come closer and will then interfere if the NTS allocation was not changed. In Figure 2(b), the continuous operation phase of STDMA is depicted.

5. Simulator

The aim of this simulator is to analyze the real-time properties of the MAC protocols described in Section 4 and especially their behavior in a typical highway scenario, Figure 4. Due to the real-time properties of the system, the interesting issue here is how the two MAC methods will influence the capability of each sending node to timely deliver data packets, that is, meeting real-time deadlines. Note that we are dealing with an uncontrolled network since the number of network nodes cannot be determined in advance as we are considering vehicles controlled by humans. On the highway, the highest relative speeds are found and this causes the network topology to change often and more rapidly. If a traffic accident occurs, many vehicles could quickly be gathered in a small geographic area implying troubles with access to the shared wireless communication channel for individual nodes. As we are studying the *MAC channel access delay* for time-driven position messages, we are not considering the reception of messages at the nodes at this time.

A promising emerging application within ITS is a cooperative awareness system such as the AIS for the ships, where the vehicles will exchange position messages with each other to build up a map of its surrounding and use this for different traffic safety and efficiency applications. In the European project SAFESPOT [27], applications that are built on this kind of message exchange are developed. Routing in highly mobile networks is also dependent on positions (i.e., geographical routing) rather than specific addresses when trying to find ways through the network. Therefore, time-driven position messages are likely to be of uttermost importance in future vehicular networks. Consequently, we have chosen to use broadcasted, time-driven position messages (the so-called heartbeat messages) as the data traffic model in the simulator. All vehicles broadcast data packets at two different heartbeat rates, 5 Hz and 10 Hz. There is no other data traffic in addition to the heartbeat messages. The highway is 10 000 meter long and contains 5 lanes in each direction, Figure 4. The vehicles are entering each lane of the highway according to the Poisson process with a mean interarrival time of 3 seconds (the 3 seconds are chosen in accordance with the Swedish 3-second rule, where vehicles should maintain a 3-second space to the vehicle in front). The speed of each vehicle is modeled as a Gaussian random variable with different mean values 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 different speeds are chosen with the speed regulations of Sweden in mind. The vehicles will have the same speed as long as they are staying on the highway and the vehicles do not overtake. The purpose of this simplistic mobility model is to achieve a realistic density of vehicles on the highway to test the communication system. It is of limited interest to use a more advanced mobility model since we are not studying applications such as lane change warning or merge assistance here. Moreover, there is no universally prevailing mobility model, and the required level of accuracy for the mobility of vehicular networks is not yet clear [28].

The channel model is a simple circular sensing range model, Figure 4, in which every node within the sensing area receives the message perfectly (i.e., without errors). Note that nodes could be exposed to two concurrent transmissions, Figure 4, where transmitters TX_1 and TX_2 are sending at the same time since the transmitters cannot hear each other: The receivers RX_1, RX_2, and RX_3 in Figure 4 will then experience collisions of the two ongoing transmissions, unless some sort of power control or multiuser detection is used. However, since the focus of this simulation is to characterize the MAC channel access delay, T_{acc}, problems such as exposed and hidden terminals are not addressed here. As soon as the nodes enter the highway, they will start to transmit after an initial random delay of between 0 and 100 milliseconds. The simulation has been carried out with three different packet lengths: $N = 100, 300$, and 500 bytes and two different sensing ranges: 500 and 1000 meters. The sensing range of 1000 meters was chosen because the PAR of 802.11p [4] states that communication ranges of up to 1000 meters must be supported and the different packet lengths are chosen because of the security issues. It is very important that heartbeat messages can be trusted since many traffic safety applications will be depending on these. One way to handle the security issue is to use a digital signature being approximately 125 bytes [29] and in worst case this signature must be included in every packet. Therefore, 500 byte packets should be the worst case length of heartbeat packets including a signature of 125 bytes, together with the header, trailer, and position data.

Table 2: Simulation parameters settings for CSMA and STDMA.

Parameter	Value
Slot time, T_{slot}	9 μs
SIFS, T_{SIFS}	16 μs
AIFS for voice, T_{AIFS}	34 μs
CW_{min}	3
CW_{max}	Will never be used due to broadcast
Backoff time, $T_{backoff}$	0, 9, 18, 27 μs
Transfer rate, R	3 Mbps
Packet sizes, N	100, 300, 500 bytes
Sensing ranges	500, 1000 meters
No. of lanes	2×5

In our CSMA simulations, all vehicles use the MAC method of 802.11p as described above, and hence each vehicle must listen before sending and backoff if the channel is busy or becomes busy during the AIFS. As explained in Section 4.1, a broadcast packet will experience at most one backoff procedure due to the lack of ACKs in a broadcast system. The contention window will never be doubled since at most one failed channel access attempt can occur. In Table 2, parameters used in the simulation of 802.11p are listed. Since all data traffic in our simulation scenario has the same priority, only the highest priority AIFS and CW_{min} have been used (Tables 1 and 2) and therefore all transmitters will have the same T_{AIFS} value (34 microseconds). The backoff time is the product of the slot time, T_{slot}, and a random integer uniformly distributed in the interval $[0, 3]$ implying four possible backoff times, $T_{backoff}$: 0, 9, 18, and 27 microseconds, respectively. In Figure 2(a), a flow diagram presents the CSMA procedure in the broadcast situation with periodic position messages from every node. The "Next packet arrived?" box tests if the new position message has arrived from the layer above the MAC layer, in which case the old packet awaiting channel access is outdated and will be dropped.

The STDMA algorithm found in AIS cannot be used right away since the dynamics of a vehicular network and a shipping network are quite different. Further, the AIS system is using lower frequencies for transmission to reach further away and the ships need to know much further ahead about ships in the vicinity to take the right decisions early on. There is a natural inertia inherent in a shipping system that is not present in the vehicular environment, that is, braking a truck

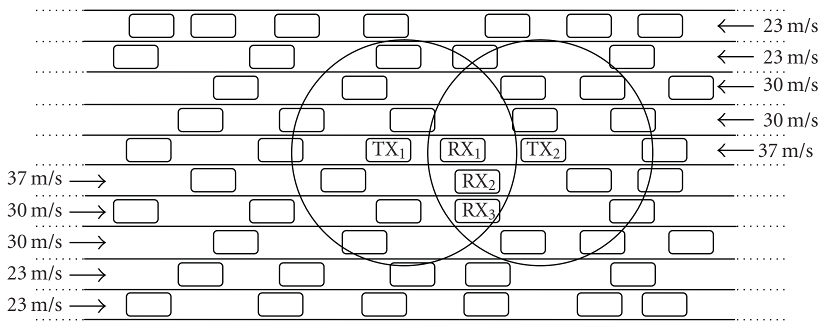

Figure 4: Simulation setup.

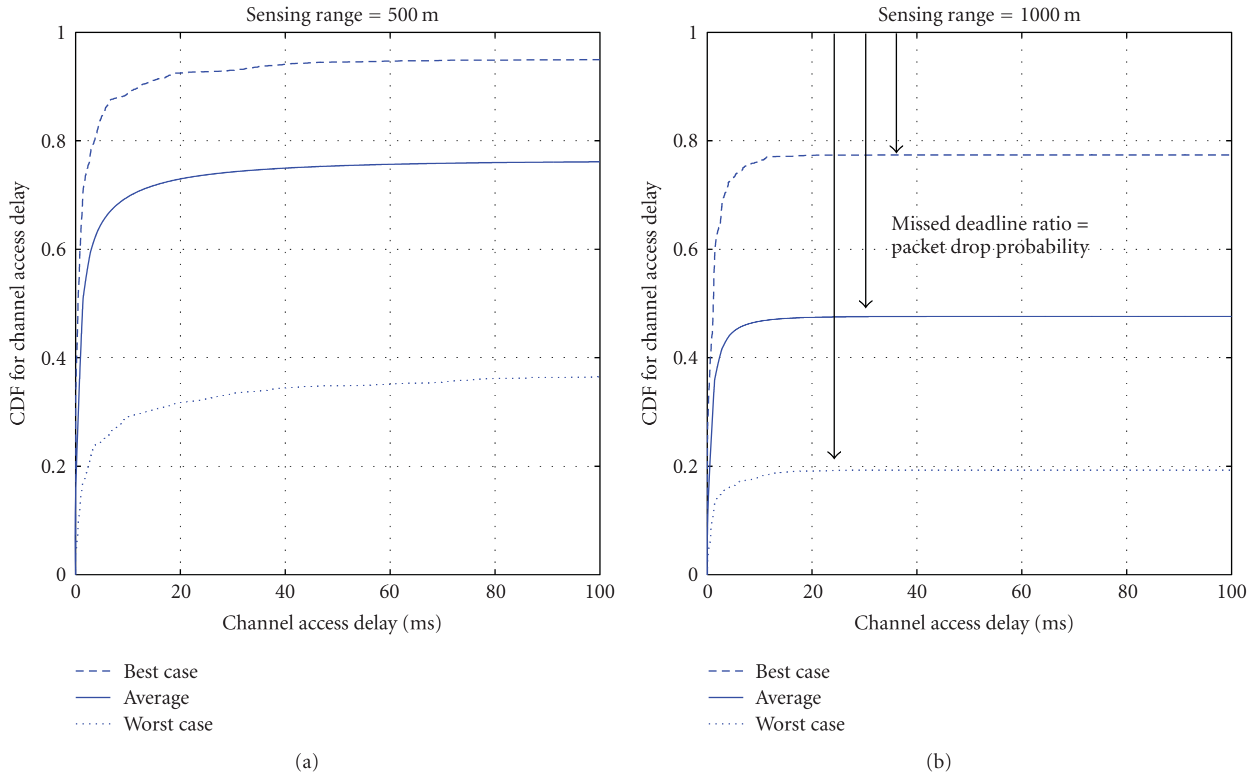

Figure 5: Cumulative distribution function of channel access delay, in a highway scenario with 10 lanes, 500 byte packets, 10 Hz heartbeat. (a) Sensing range of 500 meters and (b) sensing range of 1000 meters.

and turning a ship in an emergency situation are two very different tasks. For the most part, we have much shorter time frames to work with in the vehicular environment. Both MAC protocols used in the simulation are assumed to use the same physical layer from 802.11p. The frame duration, T_{frame}, in our simulated STDMA scheme has been set to 1 second and the number of slots is changed inside the frame to cater for different packet lengths. A transfer rate, R, of 3 Mbps has been used and this rate is available with the PHY layer of 802.11p, which has support for eight transfer rates in total where 3 Mbps is the lowest. This choice is made since the system under consideration requires high reliability rather than high throughput, and the lowest transfer rate has the most robust modulation and coding scheme.

In the STDMA simulations, the vehicles will go through three phases: *initialization, network entry*, and *first frame*, before it ends up in the *continuous operation*. The phases are described in Section 4.2, and in Figure 2(b) the continuous operation phase is depicted. The vehicle stays in the continuous phase after it has been through the other three. STDMA always guarantees channel access even when all slots are occupied within an SI, in which case a slot belonging to the node located furthest away will be selected.

Unless otherwise stated, the time parameters involved in the simulation are selected from the PHY specification of 802.11p. The CSMA transmission time, T_{CSMA}, consists of an AIFS period (listening), T_{AIFS}, of 34 microseconds, a 20 microseconds preamble, T_{preamble}, and the actual packet

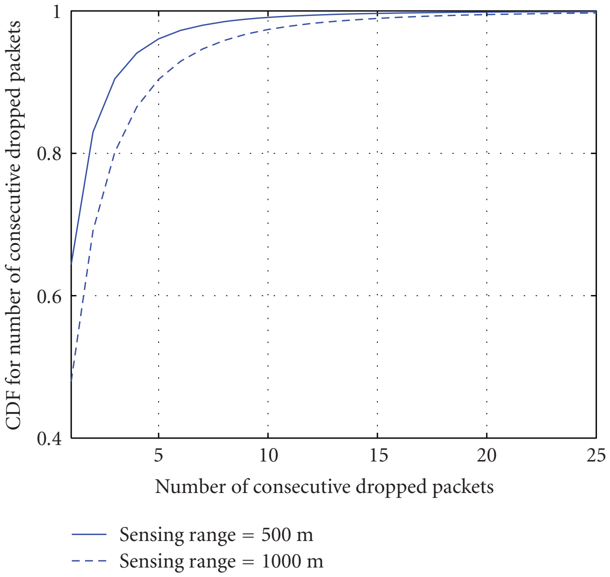

Figure 6: Number of consecutive dropped packets due to no channel access.

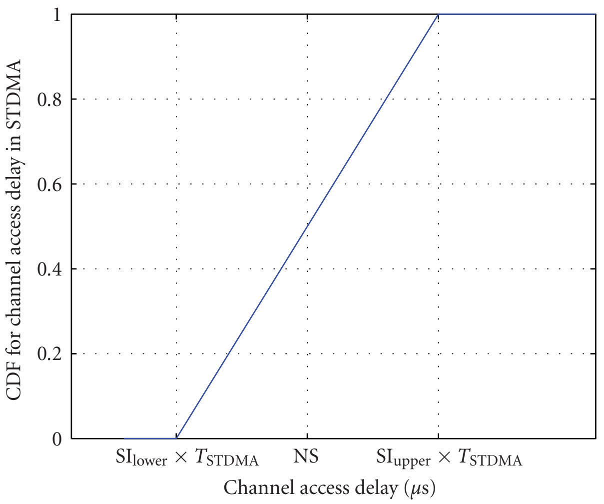

Figure 7: The CDF for channel access delay when using STDMA.

transmission, T_{packet}. The STDMA transmission time, T_{STDMA}, which is the same as the slot time, consists of two guard times, T_{GT}, of 3 microseconds each, T_{preamble}, T_{packet}, and two SIFS periods, T_{SIFS}, of 16 microseconds each derived from the PHY layer in use. SIFS stands for short interframe space and accounts for the transceiver to switch from sending to receiving state (and vice versa) plus the MAC processing delay. The total transmission time for CSMA is

$$T_{\text{CSMA}} = T_{\text{AIFS}} + T_{\text{preamble}} + T_{\text{packet}} \quad (1)$$

and the total transmission time for STDMA is

$$T_{\text{STDMA}} = 2T_{\text{GT}} + 2T_{\text{SIFS}} + T_{\text{preamble}} + T_{\text{packet}}. \quad (2)$$

In Table 3, the different timing parameters are shown for different packet lengths.

We assume that all vehicles in the system are perfectly synchronized with each other in both MAC scenarios and that in the STDMA case they are also aware of when the frame starts and how many time slots it contains.

6. Results

The simulated highway scenario described earlier has a vehicle density of approximately one vehicle every 100 meters in each lane. The vehicle density is chosen to examine the scaling performance of the two MAC layers considered in this paper. The vehicular environment is uncontrolled in terms of node density and the scalability issue, hence plays an important role when designing an MAC protocol for VANETs. Computer simulations have been carried out in MATLAB with the parameter settings in Tables 2 and 3, yielding 12 different scenarios (all combinations of three packet lengths, two sensing ranges, and two heartbeat frequencies). The most demanding case is, of course, when 500 bytes long packets are sent 10 times per second and the nodes have a sensing range of 1000 meters, since this corresponds to the largest aggregated bandwidth requirements per unit area. In this situation, an ideal MAC method (that schedules all transmissions perfectly) can handle 70 nodes that are in radio range of each other without packet collisions. However, the simulation contains situations that are overloaded and a node has around 210 neighbors within radio range when the range is 1000 meters, and consequently, we have to accept some packet drops by the transmitter or packet collisions in the air (that might also lead to packet drops at the receiver side). A packet drop at the transmitter occurs when a new position message has arrived from the layer above the MAC layer, before the old packet awaiting channel access has been transmitted.

Cumulative distribution functions (CDFs) for the channel access delay, that is, $F_{T_{\text{acc}}}(x) \triangleq \Pr\{T_{\text{acc}} < x\}$, for CSMA are shown in Figures 5(a) and 5(b) for two different sensing ranges, respectively. To avoid edge effects in the simulation, statistics were only collected from the middle part of the highway and only when the highway is filled with vehicle traffic. Dropped packets are considered to have infinite channel access delays, and the CDFs will, therefore, not reach unity at a finite delay. We can interpret $F_{T_{\text{acc}}}(1/f_h)$, where f_h is the heartbeat frequency, as the packet drop probability or, equivalently, as the missed deadline ratio (since $1/f_h$ is the deadline). The three plots in each figure represents the CDF for the node performance in the best, worst, average cases. For a sensing range of 500 meters, approximately 100 nodes are within radio range and packet drops are unavoidable. The best case node will drop 5% of its generated packets and the worst case node will drop 65% of its packets. When the sensing range is extended to 1000 meters in Figure 5(b), the situation becomes untenable and, on average, nodes will drop around 50% of their packets.

The average missed deadline ratios, average over all vehicles and all messages, for all simulated scenarios using CSMA are shown in Table 4. Hence, for a sensing range of 1000 meters and a heartbeat frequency of 10 Hz, only 47% of the packets are transmitted.

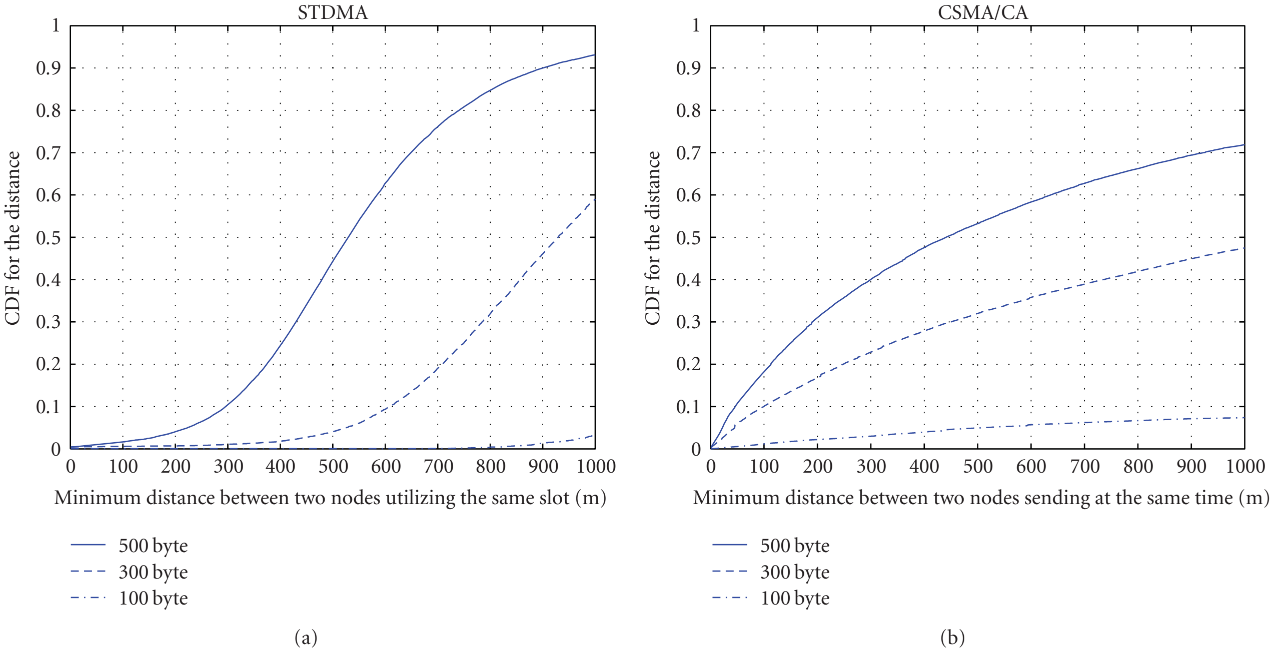

Figure 8: The CDF of the minimum distance between two nodes (a) utilizing the same time slot in STDMA and (b) sending at the same time in CSMA/CA, using 500 byte packets, heartbeat of 10 Hz, sensing range of 1000 m.

Table 3: The transmission times for CSMA and STDMA, respectively, together with packet sizes and number of slots per frame in STDMA.

Packet length N (byte)	T_{packet} (μs)	T_{CSMA} (μs)	T_{STDMA} (μs)	No. of slots
100	267	321	325	3076
300	800	854	858	1165
500	1333	1387	1391	718

The distribution of packet errors over time for a certain node is also of interest. Clearly, it is undesirable to lose many consecutive packets since this will make the node invisible to the surrounding vehicles for a period of time. The CDF for the number of consecutive packet drops is shown in Figure 6 for two different sensing ranges. In the worst case, a node experienced over 100 consecutive packet drops, implying invisibility for over 10 seconds. However, in more than 90% of the cases, fewer than 5 consecutive packets were dropped.

The STDMA algorithm always grants packets channel access since slots are reused if all slots are currently occupied within the selection interval of a node. When a node is forced to reuse a slot, it will choose the slot that is used by a node located furthest away. Hence, there will be no packet drops at the sending side when using STDMA and the channel access delay is always bounded and relatively small. In Figure 7, the CDF for the channel access delay for STDMA is depicted and as can be seen, all nodes will choose a slot for transmission during their selection interval. Therefore, the CDF for T_{acc} in STDMA is ending at unity after a finite delay as compared to the CDF for T_{acc} in CSMA according to Figures 5(a) and 5(b).

This finite upper bound on T_{acc} in STDMA does, however, come at the expense of increased interference on the channel (i.e., more packet collisions in the air will occur) as compared with CSMA. The intentional slot reuse probability is a parameter that can be used to indicate the interference level and thereby the reception performance of an STDMA system. In Table 5, the intentional slot reuse probability is tabulated for the different data traffic settings. The worst case is found when the nodes are transmitting 500 bytes long packets having a heartbeat of 10 Hz and a sensing range of 1000 meters, and then 50% of the slots are intentionally reused.

In Figure 8(a), the CDF for the minimum distance between nodes intentionally utilizing the same slot within sensing range is depicted for different packet lengths. With a smaller packet size, more nodes can be handled by the network since smaller packets imply that every node keeps the channel occupied during a shorter time period. When long packets are used, the distance between two nodes intentionally reusing the same slot is reduced. In the CSMA/CA case, all channel requests did not make it to a channel access and then the nodes started to drop packets. However, in the CSMA/CA case when a node gets a channel access, there is always a risk that someone else sends at the same time, that is, a collision in the air. This is due to the fact that nodes can experience the channel idle at the same time, either because the channel actually is idle or because ongoing transmissions are not detected (see Figure 2). In

Table 4: Probability of packets drop averaged over nodes in a network using CSMA.

CSMA		Sensing range			
		500 meters		1000 meters	
		5 Hz	10 Hz	5 Hz	10 Hz
Packet length	100 bytes	0%	0%	0%	0%
	300 bytes	0%	0%	0%	35%
	500 bytes	0%	22%	33%	53%

Table 5: The intentional reuse of slots within sensing range for different data traffic scenarios in the STDMA case.

STDMA		Sensing range			
		500 meters		1000 meters	
		5 Hz	10 Hz	5 Hz	10 Hz
Packet length	100 bytes	0%	0%	0%	0%
	300 bytes	0%	0%	0%	34%
	500 bytes	0%	22%	15%	50%

Figure 8(b), the CDF for the minimum distance between two nodes in the CSMA/CA scenario sending at the same time for three different packet lengths is depicted. The minimum distance can be interpreted as the distance between the nodes whose packets will, on the average, interfere the most with each other. In the 500 bytes, 1000 meters sensing range scenario, about 47% of the channel requests were granted (see Table 4), and, from Figure 8(b), we conclude that the transmitted packets will be interfered by another transmission within 500 meters in approximately 53% of the cases.

7. Conclusions

The new emerging cooperative traffic safety systems can be classified as real-time communication systems, and they are characterized by two important parameters: *deadline* and *reliability* (error probability). At the PHY layer, the reliability could be increased by using tailored channel coding and diversity techniques to overcome the impairments of the wireless channel, but first and foremost a timely channel access must be granted. Otherwise, the PHY layer techniques are irrelevant. To meet real-time deadlines, the MAC scheme must be predictable so that it can provide some sort of finite *channel access delay*, T_{acc}, to guarantee that communication tasks meet their deadlines, that is, the MAC scheme must be deterministic (T_{acc} is finite).

The upcoming standard IEEE 802.11p intended for VANET used for safety traffic applications with real-time communication demands will use CSMA as its MAC method despite its two well-known drawbacks: unbounded channel access delays as well as collisions on the wireless channel. When the node density increases, CSMA has huge troubles with solving all channel access requests into channel access. We have proposed to use STDMA as a remedy to the CSMA scaling problems. STDMA is a decentralized, predictable MAC method with a finite channel access delay, making it suitable for real-time ad hoc vehicular networks. An STDMA algorithm is already in commercial use in a system called automatic identification system (AIS) where it focuses on collision avoidance between ships.

We have analyzed the particular communication requirements introduced by traffic safety applications, namely, low-delay, reliable, real-time communications. The requirement on low delay favors the use of an ad hoc V2V network, whereas the reliability constraint poses high demands on the physical layer in terms of adaptive channel coding and modulation. The ad hoc network together with the real-time constraints requires a decentralized predictable MAC method capable of meeting real-time deadlines. We have, therefore, compared the real-time properties of two decentralized MAC methods, CSMA of 802.11p and STDMA of AIS, in terms of channel access delays and interference (due to packet collisions in the air), by simulating a highway scenario with periodic broadcast traffic, where the packets contain information about the sending node, such as position and speed. The deadline in this case is simply the time between consecutive packets.

As an example, the results revealed that on a 10-lane highway where nodes send 500 bytes long packets every 100 milliseconds and the sensing range is 1000 meters, a node with the CSMA MAC layer can drop up to 80% of the packets in the worst case (i.e., channel access was not granted during the 100 milliseconds between two consecutive packets). Moreover, in this scenario, a vehicle can experience up to 100 *consecutive* heartbeat packet drops, implying that the vehicle will become invisible to the surrounding nodes during as long as 10 seconds. The STDMA algorithm, on the other hand, always grants packets channel access since slots are reused if all slots are currently occupied within the selection interval of a node. When a node is forced to reuse a slot, it will choose the slot that is used by a node located further away. Hence, there will be no packet drops at the sending side when using STDMA and the channel access delay is always bounded and relatively small.

Packet collisions in the air will occur in both CSMA (unintentionally) and STDMA networks (intentionally and unintentionally). We have shown that small distances between the closest interfering nodes are more probable for CSMA compared to STDMA, indicating, somewhat counter-intuitively, that the packet collision problem is actually worse in CSMA compared to STDMA.

Acknowledgment

This work was funded in part by the Knowledge Foundation, http://www.kks.se/.

References

[1] J. J. Blum, A. Eskandarian, and L. J. Huffman, "Challenges of intervehicle ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 347–351, 2004.

[2] K. Bilstrup, E. Uhlemann, and E. G. Ström, "Medium access control in vehicular networks based on the upcoming IEEE 802.11p standard," in *Proceedings of the 15th World Congress on Intelligent Transport Systems (ITS '08)*, pp. 1–12, New York, NY, USA, November 2008.

[3] K. Bilstrup, E. Uhlemann, E. G. Ström, and U. Bilstrup, "Evaluation of the IEEE 802.11p MAC method for vehicle-to-cehicle communication," in *Proceedings of the 68th IEEE Vehicular Technology Conference (VTC '08)*, pp. 1–5, Calgary, Canada, September 2008.

[4] The latest version of the PAR for IEEE 802.11p, http://standards.ieee.org/board/nes/projects/802-11p.pdf.

[5] S. Yang, H. H. Refai, and X. Ma, "CSMA based inter-vehicle communication using distributed and polling coordination," in *Proceedings of the 8th International Conference on Intelligent Transportation Systems (ITSC '05)*, pp. 167–171, Vienna, Austria, September 2005.

[6] A. Pal, A. Dogan, F. Özgüner, and Ü. Özgüner, "A MAC layer protocol for real-time inter-vehicle communication," in *Proceedings of the IEEE 5th International Conference on Intelligent Transportation Systems (ITSC '02)*, pp. 353–358, Singapore, September 2002.

[7] S. V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust ad hoc vehicle communication networks," in *Proceedings of the IEEE International Conference on Intelligent Transportation Systems (ITSC '01)*, pp. 962–967, Oakland, Calif, USA, August 2001.

[8] J. J. Blum and A. Eskandarian, "A reliable link-layer protocol for robust and scalable intervehicle communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 8, no. 1, pp. 4–12, 2007.

[9] M. Lott, R. Halfmann, E. Schulz, and M. Radimirsch, "Medium access and radio resource management for ad hoc networks based on UTRA TDD," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '01)*, pp. 76–86, Long Beach, Calif, USA, October 2001.

[10] F. Borgonovo, L. Campelli, M. Cesana, and L. Coletti, "MAC for ad-hoc inter-vehicle network: services and performance," in *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03)*, vol. 5, pp. 2789–2793, Orlando, Fla, USA, October 2003.

[11] L. Stibor, Y. Zang, and H.-J. Reumerman, "Evaluation of communication distance of broadcast messages in a vehicular ad-hoc network using IEEE 802.11p," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '07)*, pp. 254–257, Kowloon, China, March 2007.

[12] M. Wellens, B. Westphal, and P. Mähönen, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios," in *Proceedings of the 65th IEEE Vehicular Technology Conference (VTC '07)*, pp. 1167–1171, Dublin, Ireland, April 2007.

[13] W. Xiang, P. Richardson, and J. Guo, "Introduction and preliminary experimental results of wireless access for vehicular environments (WAVE) systems," in *Proceedings 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous*, pp. 1–8, San Jose, Calif, USA, July 2006.

[14] N. Choi, S. Choi, Y. Seok, T. Kwon, and Y. Choi, "A solicitation-based IEEE 802.11p MAC protocol for roadside to vehicular networks," in *Proceedings of the Mobile Networking for Vehicular Environments (MOVE '07)*, pp. 91–96, Anchorage, Alaska, USA, May 2007.

[15] C. Suthaputehakun and A. Ganz, "Priority based inter-vehicle communication in vehicular ad-hoc networks using IEEE 802.11e," in *Proceedings of the 65th IEEE Vehicular Technology Conference (VTC '07)*, pp. 2595–2599, Dublin, Ireland, April 2007.

[16] S. Shankar and A. Yedla, "MAC layer extensions for improved QoS in 802.11 based vehicular ad hoc networks," in *Proceedings of IEEE International Conference on Vehicular Electronics and Safety (ICVES '07)*, pp. 1–6, Beijing, China, December 2007.

[17] F. Bai and H. Krishnan, "Reliability analysis of DSRC wireless communication for vehicle safety applications," in *Proceedings of IEEE Intelligent Transportation Systems Conference (ITSC '06)*, pp. 355–362, Toronto, Canada, September 2006.

[18] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proceedings of the 66th IEEE Vehicular Technology Conference (VTC '07)*, pp. 2199–2203, Baltimore, Md, USA, September-October 2007.

[19] E. Uhlemann, T. M. Aulin, L. K. Rasmussen, and P.-A. Wiberg, "Deadline dependent coding—a framework for wireless real-time communication," in *Proceedings of the 7th International Conference on Real-Time Systems and Applications (RTCSA '00)*, pp. 135–142, Cheju Island, Korea, December 2000.

[20] D. Caro, *Automation Network Selection*, ISA, Research Triangle Park, NC, USA, 2004.

[21] C. Venkatramani and T. Chiueh, "Supporting real-time traffic on the Ethernet," in *Proceedings of the IEEE Real-Time Systems Symposium*, pp. 282–286, San Juan, Puerto Rico, USA, December 1994.

[22] S. Rüping, E. Vonnahme, and J. Jaspernite, "Analysis of switched Ethernet networks with different topologies used in automation systems," in *Proceedings of the Fieldbus Technology Conference (FeT '99)*, pp. 351–358, Springer, Magdeburg, Germany, September 1999.

[23] P. S. Marshall and J. S. Rinaldi, *Industrial Ethernet*, ISA, Research Triangle Park, NC, USA, 2005.

[24] "IEEE P802.11p/D3.0, Part 11: Wireless LAN Medium Access Contrl (MAC) and Physical Layer (PHY) Specifications: Amendment: Wireless Access in Vehicular Environments (WAVE)," Draft 3.0, July 2007.

[25] "IEEE Std. 802.11e-2005, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," 2005.

[26] Recommendations ITU-R M.1371-1, "Technical characteristics for universal shipborne automatic identification system using time division multiple access in the VHF maritime mobile band".

[27] "Safespot project," http://www.safespot-eu.org.
[28] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.
[29] J. J. Blum, A. Tararakin, and A. Eskandarian, "Efficient certificate distribution for vehicle heartbeat messages," in *Proceedings of the 68th IEEE Vehicular Technology Conference (VTC '08)*, pp. 1–5, Calgary, Canada, September 2008.

Paper B

Katrin Bilstrup, Elisabeth Uhlemann, Erik G. Ström, and Urban Bilstrup

On the ability of the 802.11p and STDMA to provide predictable channel access

Proceedings of the 16th World Congress on ITS

Stockholm, Sweden, September 2009

ON THE ABILITY OF IEEE 802.11P AND STDMA TO PROVIDE PREDICTABLE CHANNEL ACCESS

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

[†]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, urban.bilstrup}@hh.se, erik.strom@chalmers.se

ABSTRACT

Emerging traffic safety applications requiring low delay communications will need vehicle ad-hoc networks. The only communication standard currently supporting this is IEEE 802.11p. However, 802.11p uses the medium access method CSMA/CA, which has a major drawback: *unbounded worst case channel access delay*. We therefore propose an algorithm already in commercial use in the shipping industry: STDMA. With STDMA, nodes always get predictable channel access regardless of the number of competing nodes and the maximum delay is deterministic. In this paper we elaborated with different parameter settings for the two protocols with the aim of improving performance without altering the standards.

KEYWORDS: IEEE 802.11p, MAC, V2V, vehicular communications, STDMA

INTRODUCTION

One of many emerging applications intended for enhancing traffic safety is the cooperative awareness system, where vehicles periodically broadcast position messages containing information about their own speed, heading, etc. The EU project SAFESPOT [1] are developing a facility called Local Dynamic Map (LDM) that will rely upon the reception of position messages called Cooperative Awareness Messages (CAM). This facility will dynamically build up an advanced map of its local surroundings containing information about moving objects, traffic signs etc. The IEEE 802.11p will be the first standard supporting broadcast in vehicular ad hoc networks (VANET), i.e. direct communication between vehicles without relying on any kind of communications infrastructure. ISO and ETSI are also using 802.11p as the basis for their work on producing vehicular communication standards. However, a major drawback with 802.11p is its medium access control (MAC) procedure, which determines how the common wireless radio channel is shared among the users. 802.11p inherits the MAC procedure found in 802.11, namely carrier sense multiple access with collision avoidance (CSMA/CA) where nodes start by sensing the channel and if it becomes busy (i.e. a transmission starts within the node's reception range) during the sensing period, the node must await a random time before attempting to send again. This MAC method is not predictable and nodes can experience unbounded channel access delay when the network load increases due to increased data traffic or when many nodes are within radio range of each other.

Automatic Identification System (AIS) is a surveillance system similar to the LDM that is already in commercial use within the shipping industry [2]. Every ship larger then 300 gross ton must carry a transponder that periodically broadcasts messages containing the ship's size, direction, speed etc., and the captain on the bridge can easily follow other ships in the vicinity

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.

and their intentions. The system was developed to overcome the shortcomings of radar in bad weather situations and to enable communication where no line of sight is possible. Like IEEE 802.11p, the AIS system supports direct ad hoc communication between ships but it has a completely different MAC method, where the available time is divided into slots and the nodes choose their slots according to an algorithm called self-organizing time division multiple access (STDMA). One transmission fits into one slot. The algorithm relies upon the existence of CAMs in the system. When the network load increases due to increased data traffic or many participating members, the nodes will start to pinch slots from each other based on the available position information, i.e. slots are pinched from nodes currently situated furthest away from the pinching node. This algorithm is predictable implying that all nodes always get a timely channel access regardless of the number of competing nodes.

Since the CAMs will be of utmost importance in emerging traffic safety systems, the probability that these messages are properly received by especially the nodes closest to the transmitting node should be made as high as possible. The MAC must therefore be deterministic such that the time between channel access request to actual channel access is upper bounded. In [4] it was shown that the MAC method used in 802.11p does not fulfill this criterion and is therefore unsuitable for CAMs. STDMA, on the other hand, is deterministic and performs remarkably well for the LDM facility, thus providing a really interesting alternative to 802.11p. *In this paper our aim is to enhance the performance of both MAC protocols as much as possible, without altering the original standards. We do this by elaborating with different parameter settings used in the standards.* For example, the 802.11p provides the possibility to assign different priorities to the data packets, which implies different listening/sensing periods and different backoff times (the time before a new channel access is possible). In the evaluation made in [4], all data traffic had the highest priority resulting in short initial listening periods, but also few discrete backoff values to choose from. This implies that the probability of collisions occurring due to the fact that several nodes choose the same discrete random backoff value, is fairly high. In this work, we use our simulator to determine whether the performance of CSMA/CA, when used for broadcasting CAM messages, can increase by using the other available priority classes. The question is whether the potential drawback of increasing the initial listening periods is compensated by increasing the number of discrete random backoff value and thereby reducing the number of collisions. In addition, for CSMA/CA we try to mitigate the problem with several consecutive packet drops found in [4] by introducing an algorithm that changes the priority class on a packet per packet basis depending on if the previous channel access attempt was successful or not. Since channel access with STDMA is always granted regardless of the number of competing nodes, we instead focus on how the nodes are pinching slots from each other, when the wireless channel becomes crowded. In order to improve STDMA we therefore improve how the pinched slot is selected and for how long it is kept. We also make a numerical evaluation on the probability of two nodes using STDMA, interfering with each other by selecting the same time slot. This loosely corresponds to collisions due to the same random backoff value with CSMA/CA, even if the distance between the two concurrently transmitting nodes is likely to be longer in STDMA since the pinching of time slots is carefully orchestrated. Finally, we elaborate on the synchronization issues implied by STDMA.

CSMA/CA OF IEEE 802.11p

The MAC method CSMA/CA that is used by 802.11p [5] is derived from 802.11 [6] where it is referred to as distributed coordination function (DCF). In a scenario where the nodes employ CSMA/CA, they first listen to the wireless channel for a predetermined listening period and if the channel is or becomes busy during this period, the node must perform a backoff procedure. If, however, the channel is sensed free for the entire listening period, the node can transmit directly. In a unicast transmission each transmitting node awaits an acknowledgment (ACK) in return from its destination node. If this is not received successfully for some reason, the sending node must also perform a backoff procedure, retransmit and again await an ACK. In contrast, a broadcast situation implies that a node will perform at most one backoff procedure since no ACKs are employed nor expected.

The backoff procedure in 802.11 works as follows: (*i*) draw an integer from a uniform distribution [0, *CW*], where *CW* refers to current contention window, (*ii*) multiply this integer with the *slot time* derived from the physical layer in use, and set this as the backoff value, (*iii*) decrement the backoff value only when the channel is sensed free and (*iv*) upon reaching a value of 0, send immediately. Note that a node is only allowed to decrement its backoff value while the channel is free and that after the channel has been sensed busy, a listening period must elapse before the countdown can be resumed. Every unsuccessful channel access attempt for a specific packet will result in a doubling of the *CW* size up to a maximum number, determined by the physical layer in use. *In a broadcast situation when the nodes perform only one backoff procedure, the mechanism with increasing the backoff window during high utilization periods and thereby spreading the transmissions in time to reduce collisions will never occur.* By spreading the backoff times, nodes will experience a longer average delay but the probability that two transmitters within radio range transmit at the same time decreases.

802.11p will also use the physical layer supplement 802.11a and the Quality of Service (QoS) amendment 802.11e [7] to prioritize the data traffic within each node. In 802.11e there are four different priority levels called access categories (AC), i.e., queues. The different ACs have different listening periods and *CW* settings. In Table 1 the different priorities with their corresponding listening periods and backoff settings are found. P1 is the highest priority and P4 is the lowest. The values are taken from the default settings found within 802.11e together with the physical layer attributes in 802.11a. The highest priority results in shortest listening period and the fewest, but lowest backoff values. When a node with a data packet with high priority, *P1*, starts to listen to the channel at exactly the same time as a node with a data packet with priority *P3*, the first node with *P1* will win the race and access the channel. This is due to the fact that the *P3* node will experience that the medium becomes busy during its listening period (43 μs) and must then perform the above described backoff procedure.

Table 1. The different listening periods and backoff values within 802.11p.

Priority	Listening period [μs]	Backoff values [μs]
P1	34	{0, 9, 18, 27}
P2	34	{0, 9, 18, 27, 36, 45, 54, 63}
P3	43	{0, 9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99, 108, 117, 126, 135}
P4	79	{0, 9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99, 108, 117, 126, 135}

With this type of QoS mechanism, nodes can prioritize the traffic internally within the node but still there can be priority inversion between competing nodes. Therefore there are no guarantees of first-in-first-out (FIFO) services for messages that arrive at different nodes with the same priority. Similarly, since the backoff times are random, there is a possibility that a lower priority message is sent before a high priority message within a node even if the lower priority message arrives earlier since the backoff intervals all contain the lower values.

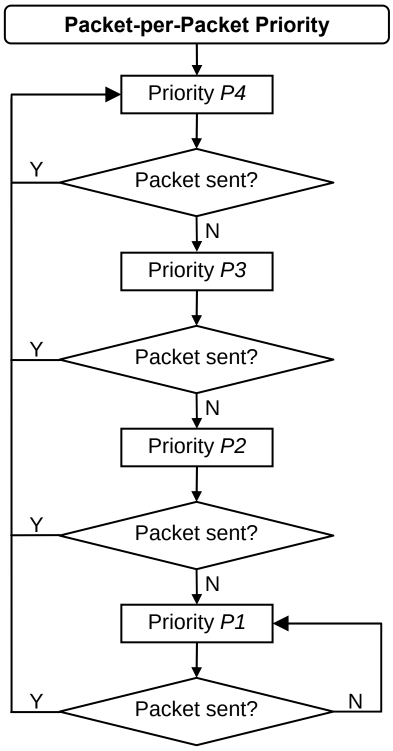

Figure 1. New algorithm for changing the priority on a packet-per-packet basis.

In this work, we investigate if the lower priority classes are better suited for broadcasted CAM, since a higher number of backoff values to choose from lowers the probability of collisions even if the initial listening period is increased.

Proposal of a new packet-per-packet change of priorities in CSMA/CA

When CSMA/CA is used to broadcast periodic CAM, in order to save bandwidth, it is better to discard packets that have not yet been sent if a newer version of the same CAM becomes available. Thus, a packet that has not been granted channel access when the next periodic message arrives should be dropped. In [4] it was shown that using CSMA/CA for high network loads, the number of consecutive packets that were dropped could be as a high as 100. This implies that a sending node did not get channel access for over 10 seconds and thus no position messages was transmitted by this node, resulting in invisibility to the surroundings for more than 10 seconds. In this work we therefore propose an algorithm that increases the priority of the current message if the previous message was dropped. All nodes start with the lowest priority, *P4* as shown in Table 1, i.e. listening period of 79 µs and 16 different backoff values. If a packet was sent successfully with these values the node will maintain its priority. Otherwise the next packet will get a higher priority, i.e. *P3* in this case. Once the node experience a successful transmission, the next packet will again get the lowest priority, *P4*. In Figure 1 the procedure of this packet-per-packet change of priority is depicted.

STDMA

STDMA [2] is a deterministic MAC method where all messages always will be granted channel access despite the number of competing nodes. STDMA is also decentralized and the network members themselves are responsible for sharing the communication channel. Nodes utilizing this algorithm, will broadcast periodic data messages containing information about their position. The algorithm thus relies on the nodes being equipped with GPS receivers.

Time is divided into frames as in a TDMA system. These frames are further divided into slots, which typically corresponds to one packet duration. All nodes will randomly select among free slots, a number of slots within each frame to transmit in. However, when there are more nodes within radio range than available slots, the nodes will start to pinch slots from each other. However, the pinching is done in a controlled manner where the node pinching will select a slot occupied by someone that is situated furthest away from it. Since positioning messages are sent periodically, this is easily determined and hence unlike other TDMA algorithms, STDMA contains no random slot assignment or contention-based periods to self-organize.

All network members start by determining a report rate, i.e., how many CAMs that will be sent during one frame (corresponding to how many slots that needs to be reserved in each frame). Then follows four different phases; *initialization, network entry, first frame,* and *continuous operation*. During the *initialization,* a node will listen to the channel activity during one frame length to determine the slot assignments (i.e., which slots are occupied and what the position is of the node using it). In the *network entry* phase, the node determines its own transmission slots within each frame according to the following rules: (*i*) calculate a nominal increment (*NI*) by dividing the number of slots with the report rate, (*ii*) randomly select a nominal start slot (NSS) drawn from the current slot up to *NI* (this slot will be the start of the frame for the node and therefore each node has its own NSS), (*iii*) determine a selection interval (SI) of slots as 20% of *NI* and put this interval around the NSS according to Figure 2, (*iv)* now the first actual slot to be used for transmission is determined by picking a slot randomly within the interval SI around NSS and this slot is denoted nominal transmission slot (NTS), Figure 2. If the randomly chosen NTS is occupied, then the closest free slot within SI is chosen. If all slots within the SI are occupied, the slot used by a node furthest away from oneself will be chosen.

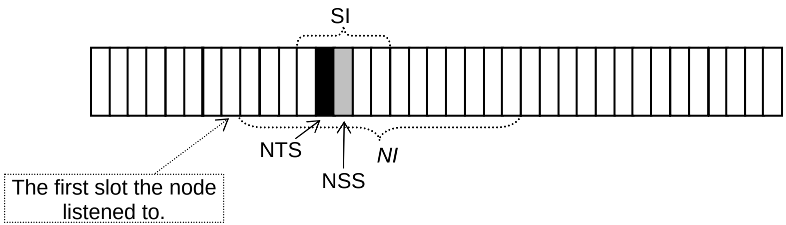

Figure 2. The STDMA algorithm in the network entry phase.

When the first NTS is selected, the node will enter the third phase called the *first frame*. Here the next slot transmission is decided by first assigning a nominal slot (NS) by adding *NI* to NSS. Thereafter the interval SI is placed around NS and the procedure of determining the next NTS will start over again. This procedure will be repeated as many times as decided by the report rate (i.e., the number of slots each node uses within each frame), Figure 3. For each NTS that is selected during the *first frame* phase, the node draws a random integer $n \in \{3,...,8\}$ which determines how long this particular NTS should be maintained. When one of the node's NTS has been used during its assigned *n* frames, a new NTS will be selected within the same SI as the original NTS. This procedure of changing slots after a certain number of frames is adopted to cater for network changes, e.g., two nodes using the same NTS which were not in radio range of each other when the NTS was chosen could have come closer and will then interfere. Note that since each NTS has its own *n*, not all slots in the frame are reassigned at the same time, and this further enhances the algorithm since the assignment will then depend on instantaneous channel conditions.

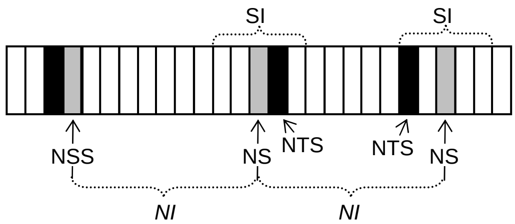

Figure 3. The STDMA algorithm in the first frame phase.

After the first frame phase when all NTS have been selected (which lasts for one frame), the station will enter the *continuous operation* phase. This phase, starting with the NSS, is when the node first starts using the selected NTSs for transmission.

Fine tuning of the slot assignment procedure in STDMA

The chosen NTS, i.e. the actual transmission slot, is kept for a number of consecutive frames. When a node uses a transmission slot, it also sends information about how many times it will continue to use this particular slot. In the original AIS standard [2] the number of times, *n*, a NTS is kept is decided by a uniform distribution, $n \in \{3,...,8\}$. A particular slot is hence kept at least three consecutive frames and at maximum eight frames. In our vehicular simulation scenario the frame is chosen to be one second, implying that a slot could be kept for eight seconds. Since the vehicular network scenario rapidly changes, this window of randomized numbers could become too large to cater for network topology changes with the result that two nodes could come really close to each other and still use the same slot. Therefore, choosing a different size of the window could be advisable for vehicular environments. We have run simulations using $n \in \{2,3,4\}$ which implies that an NTS kept for two up to four times.

SIMULATION STUDY OF THE TWO PROPOSED MAC METHODS

Our simulator is based on a highway scenario with 10 lanes, 5 lanes in each direction, where vehicles appear Poisson distributed with a mean inter-arrival time of 3 seconds. Vehicle speeds are modelled as Gaussian random variables with mean values for each lane, 23 m/s, 23 m/s, 30 m/s, 30 m/s and 37 m/s, the standard deviation being 1 m/s. All vehicles start sending periodic positioning messages of 500 byte every 100 ms with a transfer rate of 3 Mbps when they enter the highway. Since we evaluate the performance on the transmitter side, the channel model is circular and all nodes within a given sensing range of 1000 meters sense and receive the message perfectly. More details about the simulator can be found in [2]. The highway scenario appears to be the most challenging scenario for the MAC procedure since it should be able to cope with high relative speeds, rapidly changing network topology and dense vehicle traffic.

SIMULATION RESULTS

We evaluate the performance of CSMA/CA and STDMA from the sending nodes' perspective in terms of Channel Access Delay or, for periodic messages, Percent Packet Drops, Number of Consecutive Packet Drops, and Distance between Two Concurrently Transmitting Nodes.

We have run several simulations to evaluate the different priority classes in 802.11p. The priorities *P1* and *P2* have the shortest listening period, but randomize between two different sets of backoff values, see Table 1. For a simulation with a particular priority, all nodes in our system are using the same priority during the entire simulation, i.e., there are no nodes with higher/lower priority than the others. The packet-per-packet priority changing algorithm as described above has also been simulated and in Figure 4 the cumulative distribution function (CDF) for the channel access delay is shown for the five different schemes. The channel access delay is defined as the time it takes before a node is allowed to send its packet after a channel request. However, if a channel access request was never resolved into an actual channel access before a new periodic packet arrived, the old packet will be thrown away, i.e., the packet is dropped at the sending node. This explains why the CDFs found in Figure 4 never reach 1. Figure 4(a) shows the best case for an individual node, Figure 4(b) the average case for all nodes and 4(c) the worst case for a single node in the network. With a sensing range of 1000 meter as in Figure 4, there are approximately 230 nodes within sensing and interfering range. Since every node has a bandwidth requirement of 40 kbps (500 byte packets sent every 100 ms at a transfer rate of 3 Mbps) the network is overloaded. No node in the network is able to resolve all channel access requests into actual channel access.

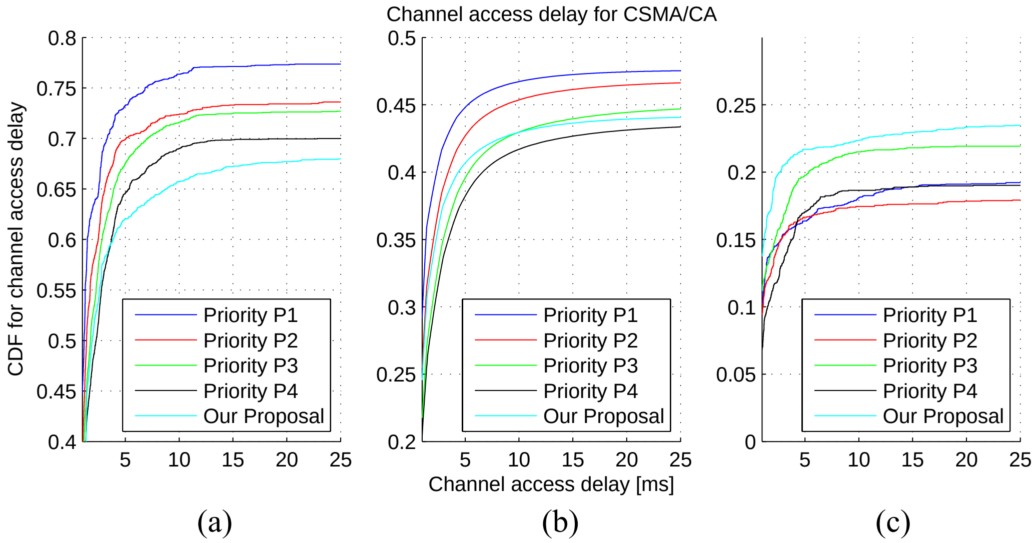

Figure 4. CDF for the channel access delay in CSMA/CA for the different priorities and our proposed packet-per-packet priority change. (a) Best case for an individual node, (b) average case for all nodes and (c) worst case for an individual node.

As can be seen in Figure 4, the different priorities do not significantly impact the channel access delay. In the average case, Figure 4b, only 50% of the generated CAMs will actually be sent. However, our proposed packet-per-packet priority changing algorithm decreases the difference between the best and the worse case nodes in the system, i.e., it is able to improve the network fairness since the priority of the next CAM is increased whenever a node was previously mistreated. When it comes to the performance measure “distance between two concurrently transmitting nodes”, the priorities have a bigger impact since the size of the different backoff windows now comes into play. Nodes that have more discrete random backoff values to choose from will have transmissions that are more spread in time. Consequently, the probability of two closely located nodes having chosen the same backoff value decreases, and thereby the collision effects are mitigated.

In the STDMA scenario simulations have been run to see what impact the factor *n* has, i.e., the number of times a specific slot is kept. In the original AIS standard, a specific NTS is kept for three to eight times. In Figure 5, the NTS is instead kept for two to four times. Figure 5 illustrates the CDF for the distance between two concurrently transmitting nodes using STDMA. Three different packet lengths; 100, 300 and 500 byte, and the transfer rate 3 Mbps have been used. The sensing range is 1000 m and there are approximately 230 nodes within this range. The frame size is one second and the number of available slots within the frame is altered depending on the packet size; 100 byte = 3076 slots, 300 byte = 1168 slots, and 500 byte = 718 slots. Every node is using 10 transmission slots, as decided by the report rate of the STDMA algorithm. In the case with 500 byte packets, the system has a requirement of approximately 2300 slots within every frame with the sensing range of 1000 m and there are 718 available slots implying an overload situation of 300%. The dotted lines in Figure 5 represent simulations run with the reduced window size (i.e., our suggested procedure) and it can be seen that the performance is indeed increased.

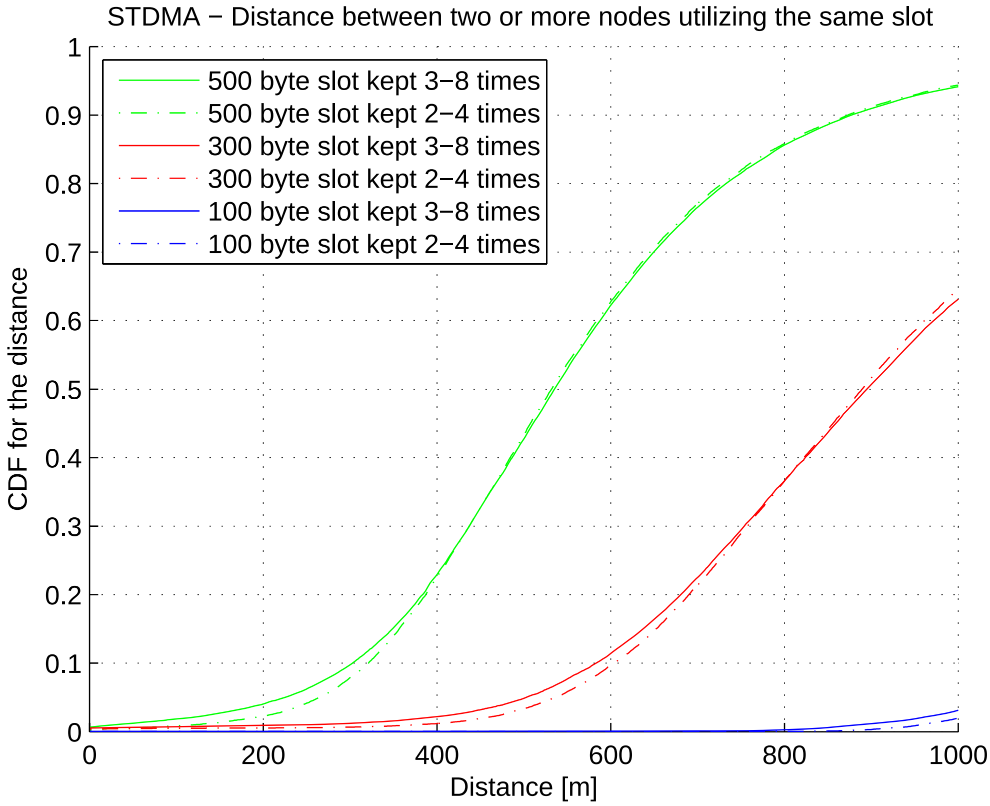

Figure 5. STDMA: CDF for distance between two or more nodes using the same slot.

DISCUSSION

The CSMA/CA approach has many advantages. It has support for arbitrary packet sizes and does not need synchronization among the nodes. The CSMA/CA is suitable for event-driven data traffic, especially when there is data traffic with variable packet sizes. In STDMA the packet size is fixed and should fit into one slot. If a packet is longer than one time slot, it must be fragmented and more slots allocated.

STDMA is very suitable for time-triggered positioning messages such as the CAMs that constitute the LDM since then the overhead messages required for self-organization is included naturally in the payload. Synchronization in STDMA is a requirement and this is done through a Global Navigation Satellite System (GNSS). In today's GPS system, the time resolution is on a nanosecond level, which fortunately is enough for synchronizing STDMA nodes in a vehicular environment. If no GNSS signal is available, the STDMA system can fall back to become a CSMA/CA system. Note however, that if there is no GNSS signal available, there will no longer be any position information available in the vehicle, and thus applications relying on CAMs may breakdown anyway. It is important to note that STDMA, unlike many other self-organizing TDMA schemes does not need any random access channel to allocate time slots. Instead it uses available positioning information at the MAC layer and the overhead introduced by the self-organizing mechanism is negligible in an STDMA system using

CAM, since the CAM messages themselves constitute the required positioning messages. In STDMA the worst case in terms of concurrently transmitting nodes is the probability that two or more nodes have totally overlapping selection intervals, *SI*, and therefore have the opportunity of choosing among the same set of transmission slots. If the two nodes with overlapping *SI* are really close to each other, they will also have the same information about allocated slots by neighbouring nodes in their respective frames. However, the probability that they have chosen exactly the same transmission slot in all of their *SI* in the superframe is low and can be calculated according to [8]. The probability of *l* consecutive transmission conflicts is

$$P(l) = \frac{1}{(N_{frame} - N_{SI})(N_{SI})^{l}}, \qquad \text{Eq. 1}$$

where N_{frame} is the total number of slots in the frame and N_{SI} is the number of slots in the *SI*. If there are 718 slots in the frame, the *SI* will be fourteen slots and every node would want to send ten times in each frame. The probability that two nodes within radio range of each other has chosen the same slots for ten consecutive transmissions within the same superframe is tabulated in Table 2. The probability of two approaching nodes not being aware of each other is consequently very low.

Table 2. The probability of *l* consecutive transmission conflicts between two nodes with totally overlapping *SI* having a frame size of 718 slots and a *SI* of 14 slots.

l	P(*l*)
1	1×10^{-4}
2	7×10^{-6}
3	5×10^{-7}
4	1×10^{-8}
5	3×10^{-9}
6	1×10^{-10}
7	1×10^{-11}
8	1×10^{-12}
9	1×10^{-14}
10	1×10^{-15}

The STDMA algorithm is very suitable for vehicular ad hoc networks with periodic heartbeat messages such as CAMs. Up to now the algorithm has been evaluated using the parameter settings of the AIS specification. However, STDMA could be further tuned and adopted to the conditions in a vehicular ad hoc network. The procedure for pinching slots can be made more sophisticated, e.g., it could be advantageous to pinch a slot from a vehicle moving away, in the opposite direction even if this node is not currently the one situated furthest away. Our initial simulations show that being able to choose freely the node situated furthest away among all nodes within range is better than to only be allowed to chose among the nodes in the opposite direction. This result will of course be influenced by relative vehicle speeds and report rate, as well as how many more times a particular slot will be occupied. Thus there are still several opportunities to enhance the performance of STDMA.

CONCLUSION

Since there cannot be any restrictions on the number of participating stations in a VANET, the MAC method must be able to handle overloaded situations. CSMA/CA becomes unfair when the network load increases and thus unbounded access delays and thereby packet drops become more frequent. Given our CAM based data traffic model, some nodes in the CSMA/CA system were forced to drop several consecutive packets, resulting in invisibility to the environment for very long periods of time. The results in this paper show that using the priorities available in 802.11p (through 802.11e) will not significantly enhance the probability of channel access for CAMs in overloaded situations. Our proposed packet-per-packet priority change algorithm, where the priority is changed depending on previous successful/unsuccessful channel access attempts, did enhance the overall performance of CSMA/CA, i.e., it decreases the difference between the worst affected node and the most favoured node in the system (the variance was decreased). Power control and restrictions on amount of data traffic seem to be the only efficient tools for proper system function with CSMA/CA.

STDMA, on the other hand, is predictable in the sense that a node always will get channel access within a bounded time upon request. By decreasing the number of times a specific slot is kept, an increase in system performance was noted. The pinching of slots in STDMA could also be combined with efficient power control to increase the overall capacity in the network. There are further possibilities to develop and adapt STDMA in order to enhance the performance when used in vehicular ad hoc networks.

To conclude, both CSMA/CA and STDMA have benefits and drawbacks which all must be considered carefully when developing traffic safety applications.

REFERENCES

[1] SAFESPOT, http://www.safespot-eu.org.

[2] Recommendations ITU-R M.1371-1, “Technical characteristics for universal shipborne automatic identification system using time division multiple access in the VHF maritime mobile band”.

[3] The latest version of the PAR for IEEE 802.11p, http://standards.ieee.org/board/nes/projects/802-11p.pdf

[4] 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 communication,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 902414, 13 pages, 2009. doi:10.1155/2009/902414.

[5] IEEE P802.11p/D3.0, *Part 11: Wireless LAN Medium Access Contrl (MAC) and Physical Layer (PHY) Specifications: Amendment: Wireless Access in Vehicular Environments (WAVE)*, Draft 3.0, July 2007.

[6] IEEE Std. 802. 11-1999, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.

[7] IEEE Std. 802.11e-2005, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*, 2005.

[8] R. Kjellberg, *Capacity and Throughput Using a Self Organized Time Division Multiple Access VHF Data Link in Surveillance Applications*, Master Thesis, The Royal Institute of Technology, Sweden, April 1998.

Paper C

Katrin Sjöberg Bilstrup, Elisabeth Uhlemann, and Erik G. Ström

Scalability issues for the MAC methods STDMA and CSMA/CA of IEEE 802.11p when used in VANETS

Submitted to IEEE International Conference on Communications (ICC2010)

Cape Town, South Africa, May 2010

Scalability issues of the MAC methods STDMA and CSMA/CA of IEEE 802.11p When Used in VANETs

Katrin Sjöberg-Bilstrup[†,§], 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 – **Heartbeat messages will be the foundation for many emerging traffic safety applications based on wireless communications. These messages contain information about the vehicle's position, speed, direction, etc. and are broadcasted periodically by each vehicle. The upcoming IEEE 802.11p standard, intended for vehicle *ad hoc* networks (VANETs) has flaws caused by the unpredictable behavior of its medium access control (MAC) scheme, which imply that traffic safety applications cannot be supported satisfactory. The IEEE 802.11p MAC is carrier sense multiple access (CSMA), which was originally designed for lightly loaded networks with bursty data traffic. CSMA provides high throughput and good average performance. However, traditional performance measures are not relevant when it comes to periodic heartbeat messages. Instead, network fairness and predictable channel access delays are more important measures. In this paper we study the MAC mechanism within IEEE 802.11p and compare it with a self-organizing time division multiple access (STDMA) scheme when used for broadcasting periodic heartbeat messages. We investigate the scalability in terms of the number of vehicles that the VANET can support using metrics such as worst case channel access delay, number of concurrent transmissions and distance between concurrent transmissions. The results show that STDMA outperforms CSMA of 802.11p even at not saturated networks.**

I. INTRODUCTION

The main motivation for using vehicular communications to form cooperative systems is to decrease the number of traffic accidents by introducing traffic safety applications, but also to reduce congestion, travel-time and pollution through traffic efficiency applications. In addition, other types of services may be offered to facilitate system introduction and provide sustainable business and operation models. Mainly three types of applications are considered: *traffic safety*, *traffic efficiency* and *value-added services*. These applications will use different wireless access technologies to meet the diverse set of communication requirements. The main focus of this article is traffic safety applications since the communication requirements of these applications notably differ from those of most existing applications relying on wireless communications.

Many of the traffic safety applications being proposed both in the US and in Europe will rely on *ad hoc* communications, i.e., direct vehicle-to-vehicle communications, using the upcoming IEEE 802.11p standard [1]. A typical vehicular *ad hoc* network (VANET) is a spontaneous network with no central mechanism controlling the network resources [2]. This is advantageous for traffic safety applications, since it eliminates the need for coverage by access points or base stations. The VANET, as specified in 802.11p, must self-organize, have support for distributed channel access, use a common frequency channel for communication, and have support for all nodes within radio range. Position messages, broadcasted periodically by every vehicle, will be the foundation for many traffic safety applications in Europe. These messages have strict timing requirements, i.e., they must be delivered before a specific deadline (the next updated position message) otherwise they are of no use. This implies that all vehicles need fair access to the channel to transmit their position message in to avoid becoming invisible to the surrounding vehicles.

In a VANET the medium access control (MAC) procedure must be decentralized to fit the *ad hoc* structure, but it also needs to cope with the rapid topology changes without collapsing, i.e., it should handle overloaded network situations without becoming unpredictable or unfair. An overloaded situation could arise from the node density increasing drastically within a geographical area or the injected data traffic from nodes in the vicinity increasing. IEEE 802.11p uses the MAC method carrier sense multiple access (CSMA), which has good support for variable packet sizes as well as nodes entering and leaving the network. The complexity is low and no synchronization is required. The IEEE 802.11p for VANETs has been evaluated through simulations previously, but from an average performance viewpoint [3, 4]. However, when considering traffic safety applications the worst case aspects are more important. The authors have shown that CSMA has problems with unbounded channel access delay and consecutive packet drops [5]. This implies that the CSMA has problems with predictability and fairness and is therefore unsuitable for traffic safety applications based on periodic heartbeat messages. Due to these problems the authors have proposed to use a self-organizing time division multiple access (STDMA) scheme, which is particularly suitable for time-triggered data traffic. STDMA is predictable, i.e., a node knows when it will be allowed to send since the maximum channel access delay is upper bounded. STDMA is fair and the predictable behavior and the fairness remain even during heavily loaded periods [5]. However, synchronization is needed

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.

and the self-organizing mechanism requires periodic heartbeat messages to be present in the system.

In this paper we evaluate the scalability of the two MAC methods; STDMA and CSMA of IEEE 802.11p for periodic heartbeat messages. Rather than focusing on average behavior, we consider performance metrics such as the worst case channel access delay, the probability that two or more nodes within radio range transmit concurrently and the distance between two concurrently transmitting nodes. These performance measures are relevant to evaluate the scalability, but also the predictability and the fairness of the MAC methods CSMA and STDMA when used for traffic safety applications based on periodic positioning messages.

II. Requirements and performance measures

Cooperative ITS applications have diverse communication requirements, especially regarding *reliability* and *delay*. Reliability is coupled with the packet error probability. Existing wireless technologies such as 2G/3G and WLAN have been designed with specific applications in mind and thus also to meet specific application requirements. 2G/3G was originally intended for voice indicating a delay sensitive application that can tolerate a lower data reliability, whereas WLAN is designed for data communication where reliability and throughput are more important than delay. Traffic safety applications, however, differ from most existing applications using wireless communications since *reliability* and *predictable delay* are required concurrently. By predictable delay is meant that a message needs to be delivered to the receiver before a predefined deadline. Traditional performance measures generally found in networking, such as throughput, are of less importance in traffic safety applications. Instead *worst case behavior* is sought for and therefore the *deadline miss ratio* is a central performance measure. A missed deadline in a wireless broadcast communication system as seen from the MAC layer perspective can mainly be caused by two things – the packet was never transmitted or the packet was not received correctly. Therefore, the deadline miss ratio is closely coupled to the *channel access delay*, i.e., the time it takes from channel access request to actual channel access at the MAC layer. The *worst case channel access delay* is essential and should not exceed the message deadline. The interference in the wireless systems is one reason for not receiving a packet successfully. The MAC scheme is responsible for scheduling the transmissions to minimize the interference and therefore the *distance between concurrently transmitting nodes* is an important performance measure. The closer two concurrently transmitting nodes are in space, the higher the interference in that area.

The periodic heartbeat messages will be of utmost importance for a range of different traffic safety applications. If a channel access request for a heartbeat messages never results in actual channel access before the next heartbeat messages is generated, the former heartbeat messages should be thrown away since more recent information is available, i.e., it is dropped at the sending node, and we say that the deadline is missed. Missing a heartbeat messages deadline does not necessarily have severe consequences for the application, but merely implies temporary performance degradation. However, if the same node is forced to drop many consecutive packets due to continuously being denied channel access, this can turn into a huge problem. When there are few ITS equipped vehicles, there will be many "inherently invisible" vehicles, but as the penetration increases, invisibility due to packet drops turns into a problem. The distributed algorithm that provides channel access therefore needs to be fair, so that potential packet drops affect all network members evenly.

Many traffic safety applications will rely on a VANET and thereby IEEE 802.11p. Currently, 802.11p does not have any restrictions on the number of nodes constituting the VANET and since many nodes could be or come into radio range good *scalability* is vital. *Fairness*, *predictability* and *scalability* are thus central performance measures in a VANET.

III. CSMA and STDMA

CSMA is the proposed MAC method in the upcoming vehicular communication standard IEEE 802.11p and it is the only standard supporting VANETs. In CSMA of 802.11p the node starts to listen to the channel, i.e. carrier sense, for a predetermined listening/sensing period called arbitration interframe space (AIFS). If the sensing is successful, i.e., no channel activity is detected, the node starts transmitting directly. If the channel becomes occupied during the sensing period, the node must perform a backoff procedure, i.e., the node has to defer its access according to a randomized time period. The backoff procedure works as follows: (*i*) draw an integer from a uniform distribution [0, *CW*], where *CW* refers to the current contention window, (*ii*) multiply this integer with the *slot time* derived from the physical layer in use, and set this as the backoff value, (*iii*) decrease the backoff value only when the channel is free, (*iv*) upon reaching a backoff value of 0, send immediately. After a busy channel all nodes must perform a sensing period (AIFS) before the decrementation of the backoff value can resume. During high utilization periods nodes using CSMA can experience unbounded channel access delays due to the channel always being or becoming busy during the sensing period.

STDMA [6] is a decentralized MAC scheme where the network members themselves are responsible for sharing the communication channel and due to the network topology being decentralized the synchronization among the nodes is done through a global navigation satellite system such as GPS or Galileo. STDMA is already in commercial use in a system called automatic identification system (AIS), where it focuses on collision avoidance between ships [7]. The algorithm is dependent on that all nodes in the network regularly send messages containing information about their own position. The STDMA algorithm uses this position information when choosing time slots in the frame. All network members start by determining a report rate, i.e., how many position messages that will be sent during one frame, which translates into the number of slots required during one frame. When a node is turned on, it will follow four different phases; *initialization, network entry, first frame,* and *continuous operation*. During the *initialization,* the node will listen for the channel activity during one frame to determine the existing slot assignments, i.e., listen to the messages sent in each slot, which contains the sending node's position and future slot assignment. In the *network entry* phase, the node determines its own slot assignment. In the *network entry* phase, the station determines its own slots to use for transmission of position messages within each frame. If all slots are occupied, the node will select an occupied slot based on its knowledge of positions, namely the slot used by the node located furthest away from itself. This way channel access is always granted and the distance between two concurrently transmitting nodes is maximized. When all slots within one frame duration are selected the station will enter the *continuous operation* phase, using the slots decided during the *first frame* phase for transmission. However, during the *first frame* phase, the node will also draw a random integer for each slot which determines for how many consecutive frames the slot will be used. This procedure of changing slots after a certain number of frames is done to cater for network changes, i.e., two nodes that use the same slots which were not in radio range of each other when the slots was chosen could now have come closer and will then interfere.

IV. Performance Evaluation

We have evaluated the scalability of CSMA and STDMA by means of computer simulation using periodic heartbeat messages as data traffic model. Depending on the transfer rate, the packet size and the frequency of the heartbeat messages, the VANET can support a certain number of vehicles within radio range without being overloaded. The maximum number of *packets* that can be sent during one second in a broadcast scenario using CSMA of IEEE 802.11 is given by:

$$N_{CSMA} = \left\lfloor \frac{1}{B \times 8 / R + T} \right\rfloor, \quad (1)$$

where B is the packet size in bytes, R is the transfer rate and T is the listening period in seconds. For STDMA the maximum number of packets per second is:

$$N_{STDMA} = \left\lfloor \frac{1}{B \times 8 / R} \right\rfloor, \quad (2)$$

since no carrier sense is needed. By knowledge of the heartbeat periodicity and the maximum number of packets per second, we can calculate the maximum number of *vehicles* within transmission range that the two MAC protocols can support. Note however, that this number is an upper bound and applies only if the arrival rate of the packets is perfectly evenly distributed. The channel would then be fully loaded and completely filled with packets, i.e., a network load of 100%. In Table 1 the theoretical numbers of packets during one second, vehicles supported and throughput are tabulated when a transfer rate of 6 Mbps, update rate 2 Hz, and 800 byte packets have been used, together with the shortest listening period (AIFS of 58 µs) from 802.11p. In Table 2 the corresponding calculations are shown for 10 Hz and 300 byte packets. The throughput for CSMA decreases when shorter packets are used due to the need for more listening periods. The two different packet lengths and heartbeat frequencies that have been tabulated are selected based on the discussions in Europe within ETSI as well as in the US within IEEE. In Europe a packet length of 800 byte together with an update rate of 2 Hz is proposed and in the US much shorter packet lengths in the order of 100-300 byte are proposed with a heartbeat of 10 Hz.

Table 1. Theoretical number of vehicles supported within transmission range with a heartbeat of 2 Hz and 800 byte packets.

	CSMA	STDMA
Number of packets/s	889	937
Number of vehicles	444	468
Throughput [Mbps]	5.69	6

Table 2. Theoretical number of vehicles supported within transmission range with a heartbeat of 10 Hz and 300 byte packets.

	CSMA	STDMA
Number of packets/s	2183	2500
Number of vehicles	218	250
Throughput [Mbps]	5.24	6

Note also that even if STDMA does not need listening periods between packets, guard intervals between slots may be necessary and thereby the number of supported vehicles is slightly reduced. The differences between STDMA and CSMA lie in how far away from the ideal case (as tabulated above) the two schemes are when used in practice. When we increase the number of vehicles within communication range beyond the maximum number that can be supported (e.g., 120%), it has different effects in CSMA/CA and STDMA. When the network becomes overloaded in CSMA, the transmitters will start to drop packets before they are sent, since a new packet with updated periodic information will have arrived at the MAC layer, i.e., the deadline of the previous packet was missed. When the network becomes overloaded in STDMA, all packets are sent, but the distance between concurrent transmissions is reduced, thereby increasing the interference. Further, the *message arrival distribution* plays an important role when considering the number of supported vehicles. In the best case, the message arrival distribution is uniform. In the worst case, all vehicles want to transmit their periodic heartbeat message at the same time instant. In CSMA this would result in all vehicles sensing the channel, determining that it is free and then all vehicles would transmit at the same time, and the distance between concurrent transmissions is minimized. Another equally bad situation for CSMA is that one vehicle have started to transmit its heartbeat message while all remaining vehicles want to sent, senses the channel, determine that it is busy, randomize a backoff value and then collisions occur evenly distributed among the discrete back off

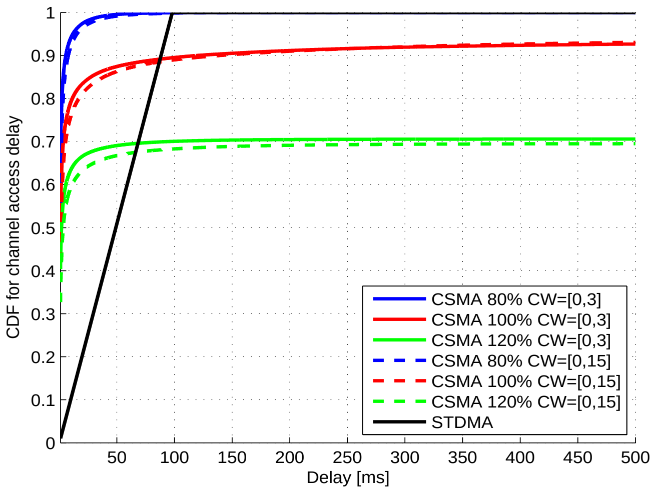

Figure 1. The CDF for channel access delay for CSMA and STDMA for 2 Hz and 800 byte at different traffic loads – 80%, 100% and 120%. The CSMA has also two different *CW* setting.

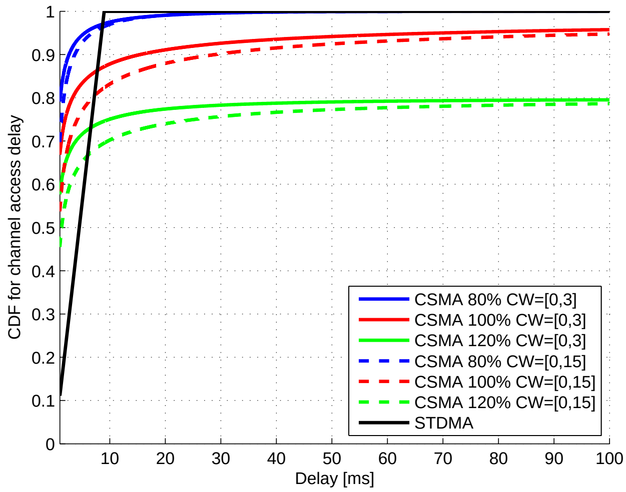

Figure 2. The CDF for channel access delay for CSMA and STDMA for 10 Hz and 300 byte at different traffic loads – 80%, 100% and 120%. The CSMA has also two different *CW* setting.

values. For STDMA these two situations entail no problems since all vehicles have to wait for their timeslot regardless of when a message arrives. In between the best and the worst case are many messages arrival distributions, so in order to get a realistic one, we used the following simulation.

We consider a highway scenario with five lanes in each direction. The vehicles arrive at the highway entrance according to a Poisson distribution. The inter-vehicle arrival rate is 1/3 Hz, which reflects dense traffic. The data traffic is periodic with independent and random starting times. This way we have obtained a random but realistic message arrival distribution. A speed is randomized for each vehicle, which they maintain as long as they are on the highway. In [5] more details about the simulator are found. All vehicles broadcast position messages at a predetermined periodicity with two different packet lengths and heartbeat frequencies – 800 byte, 2 Hz and 300 byte, 10 Hz. Simulations have been conducted with three different network loads; 80%, 100% and 120% (note that each MAC scheme is loaded with the respective number of vehicles that constitutes its 100%, see Table 1 and 2). The network loads have been achieved by altering the communication range for the nodes and thereby different numbers of nodes comes within range. CSMA simulations have been run with two different sizes of the contention window, *CW*=[0, 3] and *CW*=[0, 15]. The transmitting side has been evaluated in terms of packet drops (occurs only for CSMA), channel access delay, the probability that two or more nodes within communication range transmit concurrently together with the distance between concurrently transmitting nodes.

In Figure 1, the *cumulative distribution function (CDF) for channel access delay* for CSMA and STDMA is depicted for a packet size of 800 byte and a heartbeat frequency of 2 Hz. In STDMA the CDF always ends at 1 because all channel access request result in channel access, i.e., the ideal case is equal to the real case for this performance measure. However, at a load of 100% in CSMA, the nodes do not transmit all generated packets since some deadlines are missed and the corresponding packet is then discarded/dropped (recall that 100% indicates a network load that should be possible to support in the ideal case). By convention, a dropped packet is considered to have infinite channel access. The results show that no packet drops occur with CSMA for a network load of 80% but for 120% almost 30% of all generated packets averaged over all nodes are dropped. The *CW* setting for CSMA shows that a few more packets are dropped when the *CW* is increased due to the backoff values on average being longer, resulting in more deadlines expiring. In Figure 2 the channel access delay for CSMA and STDMA is depicted for a packet size of 300 byte and an update frequency of 10 Hz. On average there is fewer packet drops for this CSMA settings since the packet size is shorter and therefore every node keeps the channel occupied a shorter time.

In Figure 3 the *probability that two or more nodes transmit at the same time* is depicted for the setting of 2 Hz and 800 byte packets at a network load of 80%. The probability is almost the same for STDMA as for CSMA with *CW*=[0,15], slightly above 2%. The larger *CW* results in nodes being spread more in time, thereby reducing the probability of concurrent transmission but at the same time increasing the probability of dropped packets, as seen in Figure 1. However, the probability that two nodes transmit at the same time for *CW*=[0,3] is 8%, which is quite high for a network load of 80% (recall that 80% is low enough so that no nodes should have to transmit concurrently).

In Figure 4 the *CDF for the distance between nodes sending concurrently* is shown for 2 Hz and 800 byte packets. The probability of CSMA nodes sending at the same time is almost the same regardless of the *CW* setting and the load. However, there is a huge difference between CSMA and STDMA. In

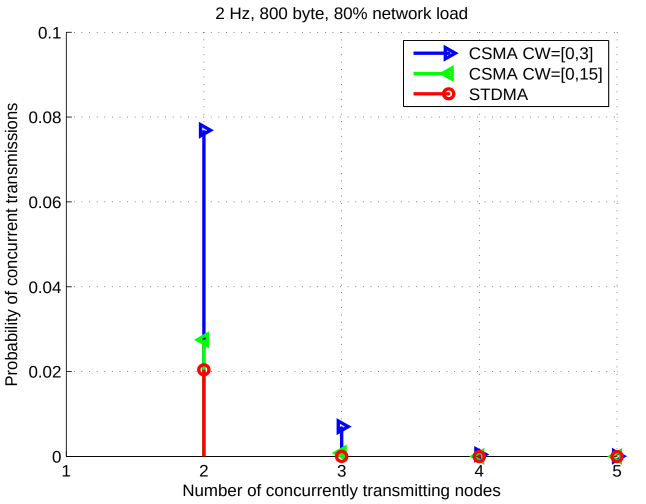

Figure 3. The probability that nodes transmit concurrently out of the number of *successful channel access requests* for 2 Hz and 800 byte at a network load of 80%.

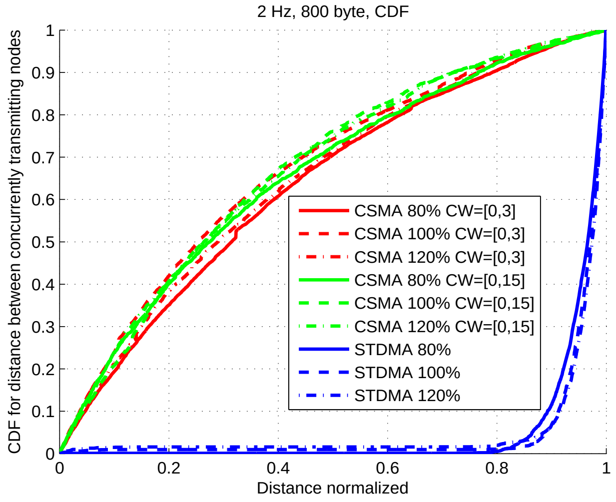

Figure 4. The CDF for the distance between concurrently transmitting nodes for 2 Hz and 800 byte packets.

STDMA the nodes use the position information to schedule the transmissions so the distance between two concurrently transmitting nodes is as long as possible. In CSMA (not using this side information) the randomness of the protocol plays an important role. Two nodes close to each other can start to sense the channel at the same time and thereby transmit at the same time. A second reason is that the discrete random backoff values are too few, also causing transmissions to start at the same time instant. Note also from Figure 4 that concurrent transmissions between nodes within communication range occur at a network load of 80% for both MAC methods even though they should be able to support this. Part of the reason for this has to do with the dynamics of the vehicular network, i.e., nodes moving in and out of communication range.

V. Conclusions

The first generation of traffic safety systems based on VANET will use IEEE 802.11p. This is unfortunate since even with not saturated networks, CSMA has a very high probability that nodes sending at the same time are located close to each other. This is due to nodes starting to listen at the same time and thereby also transmitting at the same time or nodes choosing the same backoff value. The main tasks of the MAC scheme are to provide access to the channel in a fair manner and to schedule transmission so that interference is minimized. In STDMA the nodes closest to a sender are better protected when the load increases since concurrent transmissions are scheduled to be as far apart as possible. Consequently, considering the performance measure *the distance between concurrently transmitting nodes* STDMA outperforms CSMA even at not saturated networks. To reduce the amount of concurrently transmitting nodes in CSMA simulations have been conducted with an increased backoff window. This results in slightly more packet drops at the sending side but fewer concurrent transmissions. However, the distance between concurrently transmitting nodes in CSMA is independent on the *CW* setting. In a not saturated network fewer packets are dropped with CSMA and there is almost the same amount of transmissions in the air for both the CSMA and STDMA. However, the main difference between them is *where in space the transmissions take place* – in CSMA it is randomly selected and in STDMA it is scheduled using the side information from the position messages. Consequently, STDMA provides *fairness*, a *predictable delay*, good *scalability* and also an increased *reliability* compared to CSMA since the nodes sending at the same time are located as far away as possible to reduce the interference for the nodes situated closest to the senders. Intuitively, the nodes situated closest to the transmitters are most interested in receiving information from the transmitter.

References

[1] IEEE 802.11p/D7.0, *Part11: Wireless LAN Medium Access Control (MAC) and the Physical Layer (PHY) Specifications: Amendment 7: Wireless Access in Vehicular Environment*, Draft 7.0, May 2009.

[2] H. Hartenstein and K. P. Lamberteaux, "A tutorial survey on vehicular ad hoc networks," in *IEEE Communications Magazine*, vol. 46, no. 6, June 2008, pp. 164-171.

[3] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proc. Of the 66th IEEE Vehicular Technology Conference*, pp. 2199-2203, Baltimore, MD, US, Sept-Oct. 2007.

[4] M. Torrento-Moreno, *Inter-vehicle Communications Achieving Safety in a Distributed Wireless Environment*, PhD dissertation, University of Karlsruhe, Germany, 2007.

[5] 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 communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, article id 902414, 2009.

[6] R. Kjellberg, *Capacity and Throughput Using a Self Organized Time Division Multiple Access VHF Data Link in Surveillance Applications*, Master Thesis, The Royal Institute of Technology, Stockholm, Sweden, Apr. 1998.

[7] Recommendations ITU-R M.1371-1, "Technical characteristics for universal shipborne automatic identification system using time division multiple access in the VHF maritime mobile band.